Monografías 137

Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario

Escuela de Altos Estudios de la Defensa

MINISTERIO DE DEFENSA

Monografías 137

Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario

Escuela de Altos Estudios de la Defensa

Septiembre 2013

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://publicacionesoficiales.boe.es/

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

www.bibliotecavirtualdefensa.es

NIPO: 083-13-178-0 (edición papel)
ISBN: 978-84-9781-862-9 (edición papel)
Depósito Legal: M-21101-2013
Imprime: Imprenta Ministerio de Defensa
Fecha de edición: abril 2013

NIPO: 083-13-179-6 (edición libro-e)
ISBN: 978-84-9781-863-6 (edición libro-e)

En esta edición se ha utilizado papel 100% reciclado libre de cloro.

ÍNDICE

¿Por qué una conciencia nacional de *ciberseguridad*? 9

Bibliografía 27

Capítulo primero

Principios de una conciencia nacional de *ciberseguridad* 35

Por José Tomás Hidalgo Tarrero

Guerra total, guerra asimétrica y *ciberguerra* 35

Antecedentes de conciencia nacional de *ciberseguridad* 38

Principios en los que se debe basar la conciencia nacional de *ciberseguridad* 42

Conocimiento de las amenazas y los riesgos y asumirlos 42

Notificación por los usuarios de los errores e incidencias sufridos 44

Información por los responsables de seguridad de los sistemas informáticos de los ISP, de las instituciones y empresas a los usuarios, miembros, empleados y clientes 46

Formación de todos, cada uno en el nivel que corresponda, en ciberseguridad 47

Adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio 49

La base de los principios de conciencia nacional de «ciberseguridad» ... 50

Requisitos necesarios para poderlo hacer 52

Participación de las instituciones de la sociedad civil 61

Conclusiones 67

Bibliografía 69

Capítulo segundo

Conciencia ciudadana de *ciberseguridad* 71

Por José Manuel Roldán Tudela

Introducción 71

El ciberespacio y la persona 73

El ciberespacio 73

Existencia 73

Modelo 74

Página

La persona 77
Datos personales 77
Identidad digital 80
Ciudadano digital 83

Los riesgos 84
Análisis centrado en los riesgos 84
Atacantes 87

Víctimas 92
Activos 93
Amenazas 97
Disminución del riesgo 114

Conciencia de *ciberseguridad* 118
Grados 118
Los sujetos 120
Los actores 121
El objeto 122
Los medios 124

Conclusiones 127

Bibliografía 132

Capítulo tercero
Concienciación en las administraciones públicas 137
Por Luis Jiménez Muñoz

Toma de conciencia y percepción del riesgo 137
Las vulnerabilidades 143
El nuevo enfoque en la gestión de riesgos 146

Toma de conciencia de lo que hay que proteger 148
Las políticas de seguridad de la información 148
Principios de seguridad 149
El Esquema Nacional de Seguridad 152

Las responsabilidades básicas del personal de la Administración 158
La organización de seguridad 159
Las responsabilidades y los riesgos 164

Las normas y los procedimientos 166
Ejemplo del contenido de una norma general de utilización de los recursos y sistemas de información de un organismo de la Administración 169

Información y concienciación 171

La formación del personal de la Administración 173
Instituto Nacional de Administración Pública 175
Federación Española de Municipios y Provincias 178
Centro Criptológico Nacional 178
Contenido de la oferta formativa del CCN en 2011-2012 181

Bibliografía 182

Capítulo cuarto
La conciencia de *ciberseguridad* en las empresas 185
Por Oscar Pastor Acosta

Introducción 185
Contenido 187

Las empresas en el ciberespacio 188
Activos de las empresas en el ciberespacio 188
Activos intangibles: propiedad intelectual, reputación y marca 188

Página

Infraestructuras críticas 194
Los servicios esenciales y las infraestructuras críticas 194
Ciberdependencia de las infraestructuras críticas 196
Amenazas a las empresas desde el ciberespacio 198
Amenazas a la propiedad intelectual 198
Amenazas a la reputación y marca 203
Amenazas a las infraestructuras críticas 209
Principales vulnerabilidades para las empresas de las tecnologías del ciberespacio 212
Cloud computing 212
Principales vulnerabilidades de la computación en la nube 215
Big data 219
Principales vulnerabilidades del *big data* 220
«Consumerización» y BYOD 222
Principales vulnerabilidades del BYOD 224
Redes sociales 225
Principales vulnerabilidades de las redes sociales 226
Vulnerabilidades asociadas a la presencia corporativa en redes sociales 227
Vulnerabilidades asociadas al uso por parte de los empleados de las redes sociales 228
Buenas prácticas de seguridad para las empresas en el ciberespacio 229
Uso de productos certificados 229
La norma «Common Criteria» 229
Aspectos evaluados en un proceso de certificación «Common Criteria» 230
Consumo de productos certificados CC 233
La norma CC en la cadena de suministro 236
Buenas prácticas para la gestión de la seguridad de la información 237
ISO 27000: Sistemas de gestión de la seguridad de la información 237
«20 Critical Security Controls» 239

La concienciación de *ciberseguridad* en las empresas 242
Programas de formación y concienciación 242

Bibliografía 246

Capítulo quinto
Cooperación internacional en temas de ciberseguridad 255
Por Emilio Sánchez de Rojas Díaz

Introducción 255

Comienza la amenaza transfronteriza 256
Dominios conectados globalmente 257
Spamhaus 261
El tratamiento de la «ciberdefensa» en las políticas de defensa 261

Los principales actores nacionales 262
Posición respecto a la cooperación internacional 264
Alemania 264
EE. UU. 265
Rusia 265
Francia 267
China 268
Unión Europea 270

Página

El papel de las organizaciones internacionales 271
ONU 271
Antecedentes 271
La seguridad de la información en la ONU 273
OTAN 276
Consejo de Europa 280
OSCE 281
Caso de análisis: la Unión Europea 284
Caso de análisis: los EE. UU. 289
Conclusiones 300
Bibliografía 301

Conclusiones de una conciencia de *ciberseguridad* y *ciberdefensa* 307
Bibliografía 331

Composición del grupo de trabajo 335

Relación de Monografías del CESEDEN 337

¿Por qué una conciencia nacional de *ciberseguridad*?

«La implantación de una cultura de *ciberseguridad* sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.» Estrategia de Seguridad Nacional.

«España está expuesta a los *ciberataques,* que no solo generan elevados costes económicos sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.» Estrategia de Seguridad Nacional.

Bajo la pregunta: «¿Por qué una conciencia nacional de *ciberseguridad*?» se desarrolla una monografía que lleva como título: «Necesidad de una conciencia nacional de *ciberseguridad*. La *ciberdefensa*: un reto prioritario», y donde hemos intentado responder a una pregunta que, cuando nos la formulábamos el primer día de nuestro trabajo, suscitaba interrogantes, pero, sobre todo, entusiasmo que solo rivalizaba con la amplitud y vigencia del proyecto que teníamos frente a nosotros.

Cuando comenzamos el estudio no se había publicado la Estrategia de Seguridad Nacional y esperábamos que antes de la finalización del presente trabajo pudiéramos contar con dicha estrategia y con la Estrategia Nacional de Ciberseguridad. La segunda aún no ha sido publicada pero la primera ya hace una especial mención a la *ciberseguridad*.

El tercer capítulo de la Estrategia de Seguridad Nacional, «Los riesgos y amenazas para la Seguridad Nacional», describe los riesgos y amenazas que afectan singularmente a la seguridad nacional: los conflictos armados, el terrorismo, las amenazas cibernéticas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las infraestructuras críticas y los servicios esenciales. También se contemplan factores potenciadores como el cambio climático, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos o la generalización del uso nocivo de las nuevas tecnologías que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos.

El cuarto capítulo, «Líneas de acción estratégicas», expone en el área de seguridad cibernética un objetivo: garantizar un uso seguro de las redes y sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y reacción frente a los ataques cibernéticos. Para ello, traza las siguientes líneas de acción estratégicas:

- Incremento de la capacidad de prevención, detección, investigación y respuesta ante las *ciberamenazas*, con apoyo en un marco jurídico operativo y eficaz. Se mejorarán los procedimientos y se impulsarán los recursos necesarios con especial énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés nacional.
- Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Se finalizará la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio, mediante el refuerzo de las capacidades de detección y la mejora de la defensa de los sistemas clasificados. Se fortalecerá la seguridad de los sistemas de información y las redes de comunicaciones que soportan las infraestructuras críticas. Se impulsará la normativa sobre protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.
- Mejora de la seguridad y resiliencia de las tecnologías de la información y la comunicación (TIC) en el sector privado a través del uso de las capacidades de los poderes públicos. Se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.
- Promoción de la capacitación de profesionales en *ciberseguridad* e impulso a la industria española a través de un plan de I+D+i.

– Implantación de una cultura de *ciberseguridad* sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.

– Intensificación de la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable. En todo momento se salvaguardarán los intereses nacionales.

Ha sido un trabajo de altísimo nivel profesional, acorde con los miembros del Comité que he tenido el placer y orgullo de presidir. Este equipo lo han constituido José Manuel Roldán Tudela, Luis Jiménez, Óscar Pastor Acosta, Emilio Sánchez de Rojas y José Tomás Hidalgo Tarrero. Los capítulos que han configurado esta monografía son los siguientes:

Capítulo 1: Principios de una conciencia nacional de *ciberseguridad*.
Capítulo 2: Concienciar a los particulares.
Capítulo 3: Concienciar a la Administración.
Capítulo 4: Concienciar a las empresas.
Capítulo 5: La cooperación internacional en *ciberseguridad*.

Entender la realidad social en nuestros días pasa ineludiblemente por analizar las circunstancias que rodean a los ciudadanos, tanto en su comportamiento individual como colectivo, y tanto en su concepto de personas físicas como en su forma de agrupamientos jurídicos, siendo empresas, fundaciones, asociaciones u organismos públicos. En este análisis, forma parte sustancial el ecosistema donde la vida se realiza. Dicho ecosistema se compone de elementos físicos y de otros elementos que, aun siendo físicos, no son tangibles como ciertos elementos naturales o algunos creados por el hombre. Dentro de estos últimos se encuentran las tecnologías de las comunicaciones que han evolucionado en estos últimos años de una forma vertiginosa, posibilitando el cambio social aun antes de que la sociedad haya tomado conciencia de su desarrollo. Siendo la tecnología, una vez más, un disparador de esta modificación sustancial de las reglas del juego social, modificando los modelos de relación desde un punto de vista antropológico.

La emergencia de Internet –después de haber sido durante años en sus fases incipientes un instrumento de comunicaciones militares– y su difusión y proliferación han servido de base para acelerar procesos de cambio social de una forma distinta a la que venía produciéndose tradicionalmente, pues ha roto dos dimensiones: el espacio y el tiempo.

Si algo define a Internet es la «democratización» de la información, favoreciendo movimientos a escala planetaria como la globalización y posibilitando también aquellas reacciones organizadas transnacionalmente

como son las corrientes antiglobalización. Elementos como la inmediatez de las acciones en el espacio virtual se trasladan a elementos visibles en cuestión de segundos, y la posibilidad de la acción social directa cambia la capacidad de obtener resultados que en otro tiempo se veían más lejanos.

A la hora de abordar este trabajo, mantuvimos la primera aproximación de estructurar las distintas ponencias basándonos en los actores de esta aproximación, a saber, las personas, las organizaciones privadas, los organismos públicos y la cooperación internacional. Ningún aspecto ha quedado sin considerar, desde los entornos jurídicos a las amenazas y los riesgos que afectan a cada uno de los colectivos sujetos del estudio.

La necesidad de una concienciación pasa por una definición del término «conciencia», que es, según la Real Academia Española: «(Del lat. *conscientĭa, y del gr. συνείδησις*) Propiedad del espíritu humano de reconocerse en sus atributos esenciales y en todas las modificaciones que en sí mismo experimenta. Acto psíquico por el que un sujeto se percibe a sí mismo en el mundo». Y concienciar: «Hacer que alguien sea consciente de algo. Adquirir conciencia de algo».

Para empezar podemos hablar de la aproximación a una nueva era organizativa donde los esquemas tradicionales tanto de comportamiento como de influencia se han visto modificados. Observando estas transformaciones podemos llegar a concluir que los paradigmas clásicos de comprensión de la estructura social han sido reemplazados por esquemas mucho más dinámicos en los que los acontecimientos se suceden a velocidades hasta ahora jamás experimentadas por las sociedades en las que tradicionalmente hemos vivido.

Pero los seres humanos intentamos entender las diferencias desde nuestros esquemas históricos de pensamiento. Según Lévi-Strauss, «estas uniformidades surgen de la estructura del cerebro humano y del proceso de pensamiento inconsciente. La característica estructural más importante de la mente humana es la tendencia a *dicotomizar,* o a pensar en términos de oposiciones binarias, y después intentar mediar esta oposición mediante un tercer concepto, que puede servir como base para otra oposición. Una oposición recurrente presente en muchos mitos, por ejemplo, es cultura/naturaleza. Desde el punto de vista estructural, cuanto más cambien las culturas más permanecerán siendo las mismas, puesto que simplemente constituyen variaciones del tema de las oposiciones recurrentes y sus resoluciones». Este esquema de pensamiento nos ha servido para la tradicional distinción bueno-malo, aliado-enemigo, pero el entendimiento de la realidad no es lineal; lo mismo sucede con Internet, un elemento donde la democratización aparente de la información es un continuo, donde la *anonimización* es prácticamente omnipresente, un espacio de comunicación interpersonal sin barreras de espacio donde

la velocidad, la inmediatez transforma nuestra percepción de nuestra vivencia como ser humano, como ser social.

Dentro de este esquema, las relaciones sociales cambian, los modelos productivos se ven modificados, aparecen nuevos negocios, desaparecen empresas, la relación entre los administrados y su administración varía sustancialmente, la cual se vuelve más participativa y para ello necesita nuevos canales de expresión. Por todo ello, Internet es un fenómeno de revolución social que posibilita cambios y fuerza la acomodación de estructuras tanto jurídicas como políticas, educativas, formativas, de negocios, delincuenciales, de protección y seguridad. Todo bajo el prisma de la comprensión y de la adecuación, incluida, como no podía ser de otra forma, la seguridad personal y estatal donde aparecen nuevos riesgos, amenazas, oportunidades... Internet y su medio «natural», el ciberespacio, se convierten en un nuevo ecosistema donde todos hemos empezado a convivir. La convivencia exige adaptación a unas nuevas reglas, a la comprensión de los modelos nuevos sobre formas de relación tradicionales, es por ello que la necesidad de una concienciación sobre este nuevo entorno es fundamental. No se excluyen de este modelo ningún fenómeno de relación social ni interindividual ni colectiva ni familiar ni empresarial ni las relaciones entre estados.

Estamos ante un nuevo modelo cultural, entre otras características, fascinante que permite al observador inquieto observar más allá de los fenómenos aparentes. Una oportunidad para el desarrollo de nuevos campos formativos, de desarrollo tecnológico, de nuevas formas de relación, de nuevas formas de modelos productivos, de nuevos pesos de los estados en el panorama internacional. Todos estamos desarrollando nuevas herramientas para acomodarnos a este nuevo ecosistema, la evolución del ser social está ante nosotros y en nosotros.

En el libro VII de *República* Platón presenta su mito más importante y conocido, el mito de la caverna, donde dice expresamente que el mito quiere ser una metáfora «de nuestra naturaleza respecto de su educación y de su falta de educación», es decir, sirve para ilustrar cuestiones relativas a la teoría del conocimiento. El mito describe nuestra situación respecto del conocimiento: al igual que los prisioneros de la caverna que solo ven las sombras de los objetos, nosotros vivimos en la ignorancia cuando nuestras preocupaciones se refieren al mundo que se ofrece a los sentidos. Solo la reflexión puede liberarnos y permitirnos salir de la caverna e incorporarnos al mundo verdadero o Mundo de las Ideas.

En este sentido, Internet se convierte en un escenario donde todo cobra un nuevo sentido. Un espacio donde la persona expresa y comunica espacios de su personalidad que, de otra forma, le serían difíciles de transmitir. Este espacio genera nuevas formas de comportamiento, nuevas relaciones; desde esta monografía hemos abordado una faceta de esta relación, la de profundizar en la necesidad de un desarrollo de una con-

ciencia de *ciberseguridad*. Faceta que se convierte en vertebral ya que la seguridad es una sensación que permite al ser humano y a las organizaciones desarrollar de una forma estable sus relaciones.

Las relaciones sociales se desarrollan en marcos conceptuales definidos, en los que la seguridad jurídica y el cumplimiento de la ley y de las normas establecidas permiten una ordenación definida. Pero cuando los espacios donde esas relaciones no están aún regulados porque la velocidad del cambio es sustancialmente superior al de su marco establecido, se generan tensiones que han de ser suavizadas por un esfuerzo en la formación de las personas para adecuar su acción ante estos nuevos retos. Los nativos en Internet no encuentran razonables determinadas limitaciones que son reclamadas por aquellos que hemos visto el nacimiento de este nuevo modelo de interacción social.

Las iniciativas sobre materias de *ciberseguridad* que están siendo desarrolladas en todos los países ante este entorno de cambio y en el ciberespacio configuran un reto de entendimiento de este «nuevo mundo». Un mundo que permite grandes oportunidades y presenta grandes retos, una experiencia fascinante para el investigador social donde, transformado en analista de inteligencia, debe interpretar los datos, ver más allá de lo evidente y concluir que, desde un punto de vista interpretativo y otro prospectivo, el papel que desarrollan los individuos, las empresas, las organizaciones públicas y los Estados está sometido a cambios y revisión.

En el presente estudio comenzaremos por la definición de los principios de una conciencia nacional de *ciberseguridad;* para ello, el coronel José Tomás Hidalgo Tarrero nos hablará sobre el concepto de *ciberguerra* comparándolo con otros paradigmas conocidos históricamente:

> *El paradigma de la «ciberguerra» es en todo similar a los paradigmas de la guerra asimétrica y de la guerra total; fundamento esta aseveración en lo siguiente:*

- *Los efectos pueden alcanzar a todos los ciudadanos, administraciones, instituciones y empresas del Estado aunque no estén conectados al ciberespacio (paradigma de la guerra total).*
- *Involucra, voluntaria o involuntariamente, a todos los ciudadanos, administraciones, instituciones y empresas del Estado (paradigma de la guerra total).*
- *La relación entre eficacia y coste es muy alta, posiblemente la más alta, ya que puede inutilizar sistemas básicos y críticos de un país con un coste para el atacante extraordinariamente bajo (paradigma de la guerra asimétrica).*
- *No necesita de una infraestructura grande y costosa como la industria de armamento clásico –terrestre, naval, aéreo y NBQR– (paradigma de la guerra asimétrica).*

– *Solo necesita personas con muy buena formación en ingeniería informática y en psicología.*

– *En la ciberdefensa pasiva deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su nivel y con sus medios (paradigmas de la guerra total y de la guerra asimétrica).*

– *La ciberdefensa activa es, o debe ser, función exclusiva, a nivel dirección, del Gobierno de la nación.*

  Es muy difícil probar fehacientemente la autoría de un ataque a menos que el atacante quiera que se sepa, lo que proporciona un nivel de anonimato muy grande y convierte a la «ciberguerra» en una guerra pérfida (paradigma de la guerra asimétrica).

Una vez hecha esta apreciación, el coronel Hidalgo Tarrero profundizará sobre el concepto de conciencia de defensa cibernética, haciendo una mención especial al concepto de:

> *...la conciencia nacional de ciberseguridad y hay que utilizar ambos significados porque es necesario ser conscientes de las amenazas y es necesario conocer nuestros deberes como individuos, como miembros de diversas organizaciones y de la administración e instituciones y como directivos, en su caso, de ellas; debemos ser conscientes de nuestras responsabilidades tanto individuales como colectivas en el campo de la ciberseguridad; estas responsabilidades son, como en el texto transcrito, personales, ciudadanas, éticas y políticas.*
>
> *La conciencia nacional de ciberseguridad, para que sea nacional, debe incluir a todos los ciudadanos y todas las instituciones, empresas y organizaciones pues de lo contrario presentará carencias y flancos débiles que serán usados, sin ninguna duda, por los atacantes.*

La concienciación en la protección frente a las amenazas «debe cubrir todos los aspectos de los sistemas informáticos y de las comunicaciones, empezando por el eslabón débil en todos ellos: el ser humano que los construye, los mantiene y los usa».

En España, al igual que en otros países, es necesario desarrollar esta cultura de concienciación en *ciberseguridad*, pero, como todo proceso cultural, necesita tiempo, recursos y convicción para llevar a cabo una política y una estrategia en esta materia. El coronel Hidalgo Tarrero hace especial referencia en este aspecto al informe del Spanish Cyber Security Institute (SCSI) titulado *La ciberseguridad nacional, un compromiso de todos*, donde queda reflejado el bajo nivel de concienciación en *ciberseguridad* de la sociedad civil, resaltando las siguientes causas:

> *Escaso protagonismo de los actores privados en materia de «ciberseguridad». La ciberseguridad nacional, hoy en día, es un sistema cerrado*

y exclusivo de los actores gubernamentales. En la actualidad, más del 80% de las infraestructuras críticas de nuestro país son propiedad, están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales). Por tanto, la aportación del sector privado al proceso de construcción de la «ciberseguridad» nacional resulta esencial.

Ausencia de una política estatal en materia de «ciberconcienciación» y «cibereducación». Muchos países de nuestro entorno están desarrollando ambiciosas políticas en materia de «ciberconcienciación» y «ciberseguridad» como eje fundamental para la creación de una cultura de «ciberseguridad». Estas políticas han sido desarrolladas e impulsadas, en primera instancia, por el sector privado y, posteriormente, han recibido un fuerte apoyo gubernamental.

En este caso, cabe destacar una doble función, por un lado, concienciar y educar al conjunto de la ciudadanía de los riesgos del ciberespacio y, por otro, identificar futuros talentos en el campo de la «ciberseguridad» dentro de la comunidad escolar y universitaria.

En España, INTECO y el CCN disponen de programas de «ciberconcienciación» y «ciberseguridad». Desde el sector privado, organismos como el ISMS Forum Spain han lanzado su propia campaña de «ciberconcienciación» bajo la denominación protegetuinformacion.com. De momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil.

Ausencia de políticas específicas para el I+D+i nacional en materia de «ciberseguridad». No existen políticas, programas o iniciativas para el I+D+i de ámbito nacional que promuevan y faciliten actividades en materia de «ciberseguridad», lo que contrasta con el gran protagonismo que a nivel europeo el nuevo marco de trabajo del Horizonte 2020 (continuación del 7.º Programa Marco) otorga a la «ciberseguridad».

Con la nueva Estrategia de Seguridad Nacional y con la inminente Estrategia Nacional de Ciberseguridad se desarrollará una actividad de concienciación por parte de la organización del Estado pero es imprescindible tener en cuenta que ha de desarrollarse una acción conjunta por parte de todos los organismos implicados en la sociedad civil.

En el capítulo segundo, el general Roldán Tudela aborda el problema de la concienciación de los particulares. Empezará por reflejar las relaciones entre el ciberespacio y la persona. Para ello, estructurará su reflexión en tres partes: una definición del ciberespacio, la adopción de un modelo y una descripción del mismo, para posteriormente centrarse en la persona y su relación con el ciberespacio: sus datos personales, la identidad digital y la evolución hacia el nuevo «ciudadano digital».

Una vez sentadas las bases de la relación de las personas con el ciberespacio, se realizará un análisis basado en el riesgo para poner de mani-

fiesto qué es lo que deben temer las personas al actuar en el ciberespacio y cómo se pueden defender contra ello. Se analizarán los orígenes de los ataques en el ciberespacio, las víctimas de estos ataques, los activos o bienes que corren peligro, las amenazas y las medidas para disminuir el riesgo.

La tercera parte resulta la más significativa puesto que se refiere a la creación de la conciencia de seguridad cibernética, basada en los análisis de los apartados anteriores. Se hablará de los grados de conciencia de seguridad cibernética a alcanzar, de los sujetos a los que se les va a imbuir esta conciencia, de los actores que participan activamente en estas actividades, de las materias objeto de concienciación y de las vías y los medios a emplear.

> *Hay muchas definiciones de ciberespacio. El Cuaderno de Estrategia núm. 149 (1) del IEEE (pág. 51), recoge varias, de las que nos quedamos, como más conveniente, con la del Departamento de Defensa de los EE. UU. El ciberespacio es «un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores».*

Nos hablará el general sobre los distintos modelos para describir este nuevo dominio, el ciberespacio, para la acción humana, distinguiendo entre este e Internet, ya que Internet es una parte de aquel. Posteriormente, profundizará en la persona como objeto fundamental del estudio en este capítulo y sus principales activos que aportan información, datos, elementos que, en su crecimiento exponencial tanto en cantidad como en calidad, aportan un enorme valor para la economía global. Estos datos son objeto de «monetización». Las personas han comprendido el valor que los datos personales tienen para las administraciones y las corporaciones y quieren aprovecharlo en su beneficio.

> *Este valor está creciendo continuamente, ya que cuantos más datos hay, más valor posee, al contrario que otras mercancías, como el oro. La estabilidad depende de la disposición de las personas para comunicar sus datos, que se ve mermada si sienten amenazada su privacidad. Resulta necesario por tanto que las empresas y administraciones sean capaces de crear y mantener la confianza que hace fluir los datos. La protección de datos personales y la posibilidad de usarlos en un contexto económico deben alcanzar un equilibrio en el que la persona pueda decidir libremente si comunica o comparte sus datos y en qué grado.*

En definitiva, podemos decir que una regulación adecuada de la protección de datos personales, la creación de un clima de confianza, la educación de las personas en relación con el control de su privacidad y una

compensación equitativa pueden hacer sumamente provechosas las aplicaciones de los datos personales.

El control de la privacidad de los datos, objeto en estos momentos de especial controversia, puede ser ejercido, en general, a través del proceso de la anonimización que permite desconectar entre sí los datos que forman la identidad digital. Por otra parte, el proceso de garantizar la identidad de la persona depende del enlace existente entre la identidad digital y la identidad real, es decir, el proceso de «autenticación» puede ser más o menos fuerte. Frente a estas prevenciones veremos quiénes son los atacantes, desde dónde atacan y qué motivaciones les mueven a actuar, sean políticas, de lucro o satisfacciones personales (conductas desviadas), entre otras. Y veremos quiénes son las víctimas, haciendo el general una distinción fundamental por su riesgo y alarma social entre los menores y el resto de los ciudadanos, resaltando que «por motivos legales y morales, el Estado, la sociedad y todos sus integrantes tienen un imperativo que obliga a la protección de los menores».

El factor humano es el eslabón más débil de la cadena de seguridad y del que se pueden explotar tres rasgos presentes en el ser humano: el miedo, la confianza y la inconsciencia (o inadvertencia). Se utilizarán tres vías principalmente para crear una conciencia nacional de *ciberseguridad*: la educación, la enseñanza y la concienciación. La conciencia de *ciberseguridad* se alcanza paulatinamente, según ciertos grados; no todas las personas pueden llegar a alcanzar el mismo grado. La edad también influye: cada grado de madurez de la persona permite alcanzar un grado de conciencia de *ciberseguridad*. Podemos establecer cuatro grados, de los que los tres primeros podrían ser alcanzados por una parte significativa de la población. Desde el nivel más básico al más avanzado se pueden establecer los siguientes grados: *ciberhigiene, ciberconciencia, ciberciudadanía* y *ciberespecialistas cibernéticos*. Siendo los sujetos primarios los que deben crear conciencia de *ciberseguridad* en los sujetos últimos, es decir, en la población.

En el tercer capítulo, Luis Jiménez nos hablará sobre la necesidad de una concienciación en la Administración sobre los riesgos asociados al uso de las tecnologías de la información por parte del personal de las Administraciones Públicas, así como la importancia de su gestión en los marcos regulatorios del funcionamiento de la Administración.

> *Haciendo especial hincapié en la necesidad de comunicación y conocimiento (toma de conciencia), que es mayor en los niveles jerárquicos superiores del personal de las Administraciones Públicas, incluido el nivel político, pues la toma de decisiones en relación con la seguridad cibernética debe tener una buena ubicación para que las prioridades puedan ser adecuadas y el eterno equilibrio entre seguridad y eficacia pueda ser alcanzado.*

Para ello, la Administración en su conjunto no puede ser ajena al escenario de riesgos, amenazas y vulnerabilidades y, en función de sus responsabilidades, debe asumir que el desarrollo, la adquisición, conservación y utilización segura de las TIC debe ser considerado como algo imprescindible para garantizar el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales. Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad. En algunos entornos, especialmente en los dedicados a la administración electrónica, interesan, además, otros aspectos muy importantes de las transacciones *on line* como son la autenticidad o la trazabilidad.

Todos los empleados públicos, de todos los niveles, tienen la obligación legal de conocer y cumplir las políticas de seguridad de la información y la normativa de seguridad. Normas de seguridad (*security standards*), guías de seguridad (*security guides*) y procedimientos de seguridad (*security procedures*). La concienciación de los empleados públicos en materia de seguridad es una tarea imprescindible para el cumplimiento de esta obligación.

A la hora de abordar el apartado de vulnerabilidades, Luis Jiménez desarrolla los distintos elementos que lo componen haciendo mención a los servicios en la nube, que en estos momentos se están desplegando de una forma masiva. Nos enfrentamos a fugas de información y dispositivos no controlados en las organizaciones –el fenómeno del *bring your own device* provoca grandes riesgos ante las vulnerabilidades que aportan unos dispositivos no normalizados dentro de las políticas de seguridad de las organizaciones–. Las políticas de seguridad han de ser seguidas con especial cuidado y su plan de acción ha de ser rigurosamente monitorizado y, para ello, es fundamental el proceso de concienciación y de formación en estos procedimientos, ya que muchas organizaciones no los tienen en cuenta.

Las normas de seguridad en la información, como la SGSI, la ISO 27001 o la protección de los servicios de la administración electrónica (Esquema Nacional de Seguridad, Real Decreto 3/2010), son obligadas si queremos cumplir escrupulosamente la normativa. Pero nos enfrentamos a un mundo dinámico donde los riesgos evolucionan, mutan a una velocidad impensable para muchos, y aquellos que tienen la responsabilidad de gestionar estos riesgos y ven diariamente los ataques por parte de los atacantes exigen un análisis de riesgos que incorpore una gestión preventiva. Los análisis de riesgos tradicionales confeccionados desde un despacho no se adecuan a la realidad actual. Por ello necesitamos un análisis dinámico y preventivo de las medidas de protección adecuadas y proporcionadas al valor de lo protegido frente a una caracterización del entorno hostil en que se encuentra, sea por incidentes externos, ataques deliberados o vulnerabilidades propias del sistema de información.

La necesidad de una capacidad de reacción ante un ataque, una respuesta adecuada a dicho ataque en tiempo real, nos obliga a aumentar nuestras capacidades y nuestro presupuesto. En estas situaciones se requiere revisar el análisis de riesgos del nuevo escenario y tomar rápidamente decisiones correctivas que mitiguen el impacto y permitan salir lo antes posible del escenario de crisis, recuperando el control de la situación.

Los aspectos de concienciación sobre los riesgos y de formación en seguridad pueden verse reflejados en los principios de conducta que establece la Ley 7/2007 relativos a la actuación diligente, eficaz, responsable, etc. Sin embargo, se echa de menos una expresión explícita a la observancia de las normas de seguridad informática tal como hace con las normas de seguridad y salud laboral. La necesidad de concienciación en materias de seguridad viene recogida expresamente en la ley y obliga al funcionario de la Administración a ser cumplidor estricto de las normativas que se aplican.

La responsabilidad del éxito de una organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades y la política de seguridad del organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas. En una organización pueden coexistir diferentes informaciones y servicios, debiendo identificarse al responsable (o propietario) de cada uno de ellos, pues una misma persona puede aunar varias responsabilidades. Por ejemplo, en el ENS dos figuras son especialmente relevantes:

- El responsable de la información que establece las necesidades de seguridad de la información que se maneja.
- El responsable del servicio que establece las necesidades de seguridad del servicio que se presta.
- Una campaña de concienciación orientada a los empleados debe tener presente los diferentes aspectos del problema de la *ciberseguridad*. Aunque cualquier acción es positiva, es realmente necesario que se planifiquen y detallen los objetivos a conseguir.
- Los programas de «concienciación» no solo deben concienciar a las personas sino también formarlas y mostrar suficientes casos prácticos en los que se pueda apreciar la realidad.
- El fin último de dichos programas es que el empleado público sepa identificar las situaciones de riesgo en el uso de las TIC y que adquiera hábitos de uso seguro de las mismas. Para ello será imprescindible que alcance un cierto nivel de conocimiento sobre los motivos para llevar a cabo dichas conductas.

– Los mensajes de concienciación de seguridad necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes y que se han recibido y entendido, se deben tener en cuenta las particularidades de cada organización y su entorno de trabajo. Aumentar la concienciación no es un ejercicio único, es un proceso continuo que provoca un cambio cultural que con el tiempo se irá integrando en el día a día del organismo.

La necesidad de formación en materias de seguridad en la Administración ha de ser continuada y se deben aumentar los esfuerzos en tiempo e intensidad.

Tras el tercer capítulo, Óscar Pastor nos hablará de la necesidad de una concienciación de *ciberseguridad* en las empresas, sometidas en estos momentos a todo tipo de ataques, incluidos los provenientes del *ciberespionaje.* El presente capítulo abordará los aspectos más importantes que las empresas deben considerar para alcanzar una adecuada concienciación de su seguridad cibernética. Para ello, se revisarán cada uno de los grupos conceptuales que todo buen análisis de riesgos debe abordar, esto es: los activos de las empresas, como elementos que aportan valor a las mismas; sus amenazas y vulnerabilidades, que pueden ocasionar impactos negativos en los anteriores, y las salvaguardas, que pueden reducir el riesgo de que dichos impactos negativos se materialicen finalmente.

Revisar con detenimiento aquellos elementos que son de especial significación para la *ciberseguridad* de las empresas es de capital importancia a la hora de abordar los principales activos que las empresas exponen en el ciberespacio, analizando sus activos intangibles, como son la propiedad intelectual, la reputación o la imagen de marca, y el creciente valor que estos elementos están tomando en el conjunto de activos de las empresas frente a los activos materiales tradicionales como son edificios, materiales, existencias de productos, etc. También se revisarán las infraestructuras críticas, como activos cuya propiedad recae mayoritariamente en empresas privadas pero cuya protección se ha convertido en una cuestión de Seguridad Nacional, dado que un impacto negativo sobre los mismos podría afectar no solo a la empresa que los operan sino a la sociedad en su conjunto.

A continuación, se abordarán las amenazas provenientes del ciberespacio a las que se enfrentan los activos de las empresas previamente analizados. Se revisarán los ataques reales o potenciales de los que son o pueden ser objeto los citados elementos, su finalidad y sus principales características, pues solo así las empresas pueden alcanzar una conciencia de su *cibersituación* que les permita mejorar su *ciberseguridad*.

También se examinarán las principales vulnerabilidades que las tecnologías más avanzadas del ciberespacio suponen para las empresas. Las organizaciones del siglo XXI, si quieren garantizar su eficiencia y perdu-

rar en el tiempo, no pueden prescindir de los servicios y funcionalidades que estas tecnologías proporcionan. Sin embargo, deben implementarlas con el conocimiento suficiente de los riesgos intrínsecos que conllevan para mejor gestionar su exposición a los mismos. En este capítulo, se abordará el análisis de nuevas funcionalidades y servicios como el *cloud computing* y el *big data,* la «consumerización» de los terminales de usuario y su movilidad en las redes empresariales, o lo que se ha denominado con el acrónimo anglosajón «BYOD»; así como las redes sociales, en las que la presencia empresarial como lugar donde hacer negocios es cada vez mayor.

Vistos los elementos que conjuntamente colaboran a conformar los riesgos a los que las empresas se enfrentan en el ciberespacio, posteriormente se analizarán las principales herramientas de que disponen las empresas para gestionar dichos riesgos hasta limitarlos a niveles aceptables. En este apartado se revisarán las buenas prácticas de ciberseguridad, entre las que se incluyen el uso de productos certificados y el establecimiento de sistemas de gestión de la seguridad de la información.

Por último, para concluir el presente capítulo, se analizará cómo se podría abordar en las empresas un adecuado programa de concienciación de *ciberseguridad* como herramienta mediante la que difundir a lo largo de la organización los conceptos de ciberseguridad analizados en el presente capítulo, asegurando que los diferentes miembros disponen del conocimiento adecuado, según su rol y responsabilidad, para asegurar una adecuada conciencia de la situación de la empresa en el ciberespacio y que permita a esta garantizar su éxito en este nuevo medio.

Las empresas están sometidas a continuos cambios, entre ellos, el peso en su valor de los activos intangibles frente a los tangibles. Las necesidades de protección frente a ataques deliberados vienen acompañadas de una concienciación por parte de la alta dirección de las empresas para que los medios necesarios para su protección se desarrollen y se implanten como una cultura empresarial; es un modelo de gestión estratégica. Los países occidentales, en especial Estados Unidos y los miembros de la Unión Europea, se enfrentan a un grave desafío para su seguridad y estabilidad económica debido al incremento progresivo de los *ciberataques* recibidos.

Los ataques son diversos desde las APT (las amenazas persistentes avanzadas), los ataques de denegación de servicio distribuido (DDoS), la ingeniería social, el *defacement* (modificación de las páginas web), uso de vulnerabilidades *zero-day,* etc. Los objetivos tradicionales habían sido los bancos pero en estos momentos los ataques van dirigidos a todos los sectores. La protección de las infraestructuras críticas se ha considerado una prioridad a nivel mundial, siendo traspuestas las obligaciones normativas europeas a nuestra legislación a través de la Ley de Infraestruc-

turas Críticas, donde se integran los aspectos de seguridad física y lógica en la preservación de la integridad de la seguridad de las infraestructuras estratégicas.

La seguridad es un proceso de mejora continua y es necesario adoptar una cultura estratégica que permita desarrollar dicho proceso, siendo su elemento clave el Ciclo de *Deming* o PDCA (*Plan Do Check Act*). Adoptando normas internacionales como las ISO 27000 y 27001 y las normas que afectan directamente a los denominados «20 controles críticos de seguridad para una ciberdefensa efectiva», que son el resultado de un consenso alcanzado por el consorcio auspiciado por el CSIS *(Center for Strategic and International Studies)* de Estados Unidos a través del organismo de control que es el *SANS Institute*; desde aquí se desarrolla un conjunto de medidas de seguridad cuyo objetivo es servir como elemento de apoyo a la decisión, proporcionando una guía que permita a las organizaciones priorizar sus inversiones en materia de seguridad y garantizando que las medidas que se implantan son aquellas cuya efectividad ha quedado acreditada por la experiencia real. De esta forma, se busca maximizar el retorno de la inversión realizada para la implantación de medidas de seguridad.

Óscar Pastor acaba su capítulo abundando en la necesidad de reforzar el eslabón más débil de la cadena de la seguridad, el individuo, y, para ello, hace especial hincapié en la necesidad de redoblar los esfuerzos en materias de formación, educación y concienciación en *ciberseguridad*.

El quinto capítulo, desarrollado por el coronel Emilio Sánchez de Rojas, aborda la cooperación internacional en *ciberseguridad*. Desde una perspectiva global provista de un profundo conocimiento del mundo internacional en materias de seguridad, defensa y ciberdefensa, el coronel Sánchez de Rojas traza un recorrido en el que aparecen los claroscuros de la voluntad de colaboración en estas materias y la realidad que, muchas veces, nos hace replantearnos si alguna vez se conseguirán los objetivos que se han diseñado como inspiradores de esta estrategia de colaboración, al estar presentes los intereses legítimos de los actores intervinientes es este teatro de operaciones.

Comienza la exposición con una cita al discurso del presidente Obama realizado a principios de 2013 y que, en estos días del mes de junio, toman una especial notoriedad:

> *EE. UU. también debe hacerle frente a la amenaza real y creciente de «ciberataques». Sabemos que los piratas informáticos roban las identidades de personas y se infiltran en correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos. Y nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones financieras, y nuestros sistemas de control del tráfico aéreo.*

> *No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía (...). Es por eso que hoy, más temprano, firmé un nuevo decreto ejecutivo que fortalecerá nuestras defensas cibernéticas aumentando el intercambio de información y desarrollando normas que protejan nuestra seguridad nacional, nuestros empleos y nuestra privacidad. Ahora bien, el Congreso también debe actuar, aprobando las leyes que otorguen a nuestro Gobierno una mayor capacidad para proteger nuestras redes y disuadir los ataques. (2)*
>
> *Barack Obama*

La defensa de los intereses estratégicos marca una línea a seguir en la política de defensa de un Estado impulsado por su legítimo interés de defensa de su soberanía. Los escenarios cambian y el ciberespacio permite la conexión global de dominios donde se desarrollan los enfrentamientos entre actores estatales y no estatales. La *ciberamenaza* es transnacional y se acrecienta debido a la falta de normativas internacionales, la dificultad de asignar la atribución real de los ataques y una asimetría entre el atacante y el atacado.

La configuración de un ciberespacio seguro dependerá de la capacidad de colaboración entre las distintas agencias gubernamentales, los actores internacionales –tanto públicos como privados–, el desarrollo de nuevas tecnologías para prevenir y reaccionar ante dichas amenazas y la capacitación suficiente para afrontarlas. El establecimiento de medidas de persecución real y efectiva de los actores maliciosos es urgente y se ha convertido en un objetivo de todas las organizaciones nacionales e internacionales en la lucha contra este tipo de ataques. Pongamos como ejemplo el informe de la OCDE *Reducción del riesgo sistémico en «ciberseguridad»*, que afirma que la cooperación internacional es una de las claves para reducir los riesgos de *ciberseguridad*. El Convenio sobre la *ciberdelincuencia* firmado en Budapest en 2001 necesita ser ratificado por todos los estados para una adecuada persecución de los delitos.

Según el coronel Sánchez de Rojas,

> *...nos encontramos con que existen en estos momentos tres cosmovisiones básicas de la ciberseguridad: la ciberliberal defensiva representada por la UE y compartida por casi todos los países europeos, la ciberliberal-ofensiva representada por los EUA y la cibernacionalista-aislacionista representada por China y Rusia. A ellas hay que añadir las que, como Irán o Corea del Norte, sin disponer de la sofistificación de las grandes potencias disponen de unas capacidades ofensivas que están dispuestas a emplear directamente o indirectamente.*

Entre las prioridades de todos los estados en su Estrategia de Seguridad figuran:

> *Acciones de mitigación proactivas, preventivas y reactivas para alcanzar y neutralizar las fuentes de problemas y el apoyo a la creación de un ecosistema global de seguridad, incluidos los acuerdos de colaboración público-privada, el intercambio de información, bilaterales y acuerdos multilaterales con los CERT en el extranjero, los organismos de seguridad y los proveedores de seguridad...*

En el plano internacional, la inclusión de una serie de conceptos (la guerra de información, seguridad de la información, las armas de la información, el terrorismo en el ciberespacio) hace que se observe la preservación de la soberanía del Estado sobre su espacio de información, así como las disposiciones relativas a la acción en el ciberespacio a fin de socavar el sistema político, económico y social de otro Estado, el tratamiento psicológico de la población o la desestabilización de la sociedad. El derecho internacional ha de modificarse con el objetivo de desarrollar un marco legal en el que se circunscriban todas las materias a tratar. Con esta intención, la OSCE se centra en la confianza, mientras que el Grupo de las Naciones Unidas de Expertos Gubernamentales (GEG) 2012 se ha comprometido a la construcción de un consenso internacional. Desde esta perspectiva, se estudian los casos de las principales organizaciones internacionales, como la ONU, la OTAN, el Consejo de Europa y la OSCE.

Pero los distintos países muestran sus visiones sobre la configuración de estos escenarios que se reflejan en sus políticas de seguridad: países como China, Rusia, Estados Unidos o la Unión Europea plantean distintas aproximaciones. Para ejemplificar este punto de vista, el coronel Sánchez de Rojas se centra en dos casos de análisis: la Unión Europea y los Estados Unidos.

La UE propone esta estrategia una visión articulada en cinco prioridades estratégicas:

1. Lograr la *ciberresiliencia*.
2. Reducir drásticamente la *ciberdelincuencia*.
3. El desarrollo de la política de *ciberdefensa* y las capacidades relacionadas con la Política Común de Seguridad y Defensa (PCSD).
4. Desarrollar los recursos industriales y tecnológicos para la *ciberseguridad*.
5. Establecer una política internacional coherente para la Unión Europea en el ciberespacio y promover valores esenciales de la UE.

En febrero de 2013 la Unión Europea (UE) ha aprobado el documento *Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto, seguro y protegido.*

Como puede apreciarse deja bien sentada su prioridad: ciberespacio abierto y libre; pero para cualquiera que esté familiarizado con las negociaciones en el marco de la UE sabe que la sustancia viene después del «but»...:

«Pero la libertad en línea requiere también protección y seguridad. El ciberespacio debe ser protegido de los incidentes, las actividades maliciosas y mal uso; y los Gobiernos tienen un papel importante para garantizar un ciberespacio libre y seguro».

Y reserva las tareas más importantes para los Gobiernos:

«Los Gobiernos tienen varias tareas: para salvaguardar el acceso y apertura, de respeto y protección de los derechos fundamentales en línea y para mantener la fiabilidad y la interoperabilidad de Internet. Sin embargo, el sector privado posee y opera una parte significativa del ciberespacio, por lo que cualquier iniciativa que pretenda tener éxito en esta área tiene que reconocer su papel de liderazgo (3)».

Sin embargo, es en el punto 5 donde la UE puede ser más proactiva y eficaz: *preservar el ciberespacio abierto, libre y seguro es un desafío global, que la UE debe abordar junto con los interlocutores pertinentes y organizaciones internacionales, el sector privado y la sociedad civil.* La Comisión, el alto representante y los estados miembros deberían articular una política internacional coherente de la UE sobre el ciberespacio que se dirija a una mayor participación y fortalecimiento de las relaciones con los principales socios internacionales y las organizaciones, así como con la sociedad civil y el sector privado (3 pág. 15).

En el caso de Estados Unidos, La Estrategia Nacional para asegurar el Ciberespacio del presidente George W. Bush fue publicada en 2003. Posteriormente, publicó en 2006 el Plan Nacional de Protección de Infraestructuras, que designa 17 (ahora 18) sectores clave de infraestructura que requieren planes de protección individual. También publicó la Iniciativa Nacional Integral de *ciberseguridad* en 2008. La Administración Obama inició sus esfuerzos en *ciberseguridad* con el *Los 60 días de examen de las políticas sobre el ciberespacio,* publicado en mayo de 2009, que presenta una revisión sólida de dónde estaba el gobierno en relación con la *ciberseguridad*, pero ofrecía poco de su visión de la forma de llegar a su destino. La principal recomendación fue que el presidente debería nombrar a un solo coordinador central de los esfuerzos nacionales y del Gobierno para las políticas de *ciberseguridad*.

En cuanto a los posicionamientos de los dos partidos en Estados Unidos, tanto republicanos como demócratas convergen en el reconocimiento de que existe una importante amenaza de naturaleza *ciber* contra la seguridad nacional y en la necesidad de la cooperación público-privada y del intercambio de información.

El presidente Obama ha declarado que la «amenaza cibernética es una de los más graves desafíos de la seguridad económica y nacional al que nos enfrentamos como nación» y que «la prosperidad económica de EE. UU. en el siglo XXI dependerá de la seguridad cibernética». Y en su ánimo está ampliar la cooperación ciberespacial con aliados y socios para aumentar la seguridad colectiva e iniciar diálogos para intercambiar las mejores prácticas en áreas como la forense, el desarrollo de la capacidades, participación en ejercicios y alianzas público-privadas.

Termina el capítulo con una llamada de atención:

> *En cualquier caso, no debemos perder la esperanza de que las grandes ciberpotencias lleguen a un acuerdo que permita fomentar la confianza y aumentar la transparencia reduciendo los crecientes riesgos asociados con los cada vez más numerosos y cada vez más complejos ciberataques. En unos años podría alcanzarse un acuerdo... ¡O no!*

Como el lector ha podido comprobar, nuestros panelistas le despertarán la curiosidad y satisfarán no solo la curiosidad ante una situación de candente actualidad sino también el conocimiento en esta materia, por el trabajo cuidadoso y extraordinariamente bien conducido y documentado que han llevado a cabo.

Disfruten de su lectura tanto como yo he disfrutado en su dirección.

Bibliografía

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *Information systems defence and security - France's strategy*. 2011

1. JOYANES AGUILAR, Luis, y otros. *Cuadernos de Estrategia 149: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid: Ministerio de Defensa, 2010. Instituto Español de Estudios Estratégicos. ISBN 978-84-9781-622-9.
2. OBAMA, Barak. *Discurso sobre el estado de la Unión de Barack Obama.* Washington: The White House, 2013.
3. UE. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruselas: European Commission & High Representative of the European Union for Foreign Affairs and Security Policy, 2013.
4. United States Army Training and Doctrine Command. *TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe, VA: TRADOC Publications, 2010.
5. LIBICKI, Martin C. *Cyberdeterrence and cyberwar.* Santa Monica, CA: RAND Corporation, 2009. ISBN 978-0-8330-4734-2.

6. World Economic Forum y The Boston Consulting Group. *Rethinking personal data: Strengthening trust.* Ginebra (Suiza): World Economic Forum, 2012.
7. DUDMAN, Jane. «Data is the new raw material of the 21st century». *The Guardian.* Electrónica, 18 de abril de 2012 [consultada el 11 de abril de 2013]. <www.guardian.co.uk/public-leaders-network/2012/apr/18/francis-maude-data-raw-material>.
8. REDING, Viviane. Press conference: «Commission proposes a comprehensive reform of EU data protection rules». *European Commission Audiovisual Services.* s. l.: vídeo en web, 25 de enero de 2012. <http://ec.europa.eu/avservices/video/player.cfm?ref=82655&sitelang=en>.
9. ABELSON, Hal y LESSIG, Lawrence. «Digital Identity in Cyberspace», White Paper Submitted for 6.805/Law of Cyberspace: Social Protocols. *MIT's Computer Science and Artificial Intelligence Laboratory.* [En línea] 10 de diciembre de 1998 [citado el: 17 de febrero de 2013]. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/linked-white-paper.html.
10. ROUNDS, M. y PENDGRAFT, N. *Diversity in Network Attacker Motivation: A Literature Review.* Computational Science and Engineering, agosto de 2009. CSE'09 International Conference, vol. 3, págs. 319-323.
11. Spanish Cyber Security Institute. *La ciberseguridad nacional, un compromiso de todos.* Junio de 2012.
12. FEDORENKO, Andrei. «The fight over the draft UN Convention on International Information Security». *Regulatory Cyber Security: The FISMA Focus IPD.* [En línea] 15 de julio de 2012 [citado el: 12 de mayo de 2013]. http://www.thecre.com/fisma/?p=2173.
13. NEWMEYER, Kevin P. *Who should lead U.S. Cyber Security efforts?* 2012, PRISM 3, n.º 2, págs. 115-126.
14. EGUILLOR, Marcos. *Social media.* n.º 185, 2011, Bit, págs. 68-71.
15. EFE. «Un nuevo caso de 'ciberacoso' se lleva por delante la vida de una chica de 15 años». *ABC.* 18 de octubre de 2012.
16. HEARN, Alison. *Structuring feeling: Web 2.0, online ranking and rating, and the digital «reputation» economy.* Ephemera, 2010, págs. 421-438.
17. SHELDON, John. «State of the Art: Attackers and Targets in Cyberspace». 2012, *Journal of Military and Strategic Studies,* vol. 14, n.º 2.
18. MUIR, Lawrence L. «The Case Against an International Cyber Warfare convention». *Wake Forest Law Review.* Winston-Salem, NC., EE. UU.: Wake Forest University School of Law, diciembre de 2011, vols. 2, n.º 5.
19. VAN HEERDEN, R. P., IRWIN, B. y BURKE, I. D. *Classifying network attack scenarios using an ontology.* Seattle: University of Washington, 2012. Proceedings of the 7th International Conference on Information Warfare and Security, 22-23 de mazo de 2012, págs. 311-324.

20. DESFORGUES, Alix. «Cyberterrorisme: quel périmètre?» *Fiche de l'Irsem n.° 11.* [En línea] diciembre de 2011 [citado el: 24 de febrero de 2013]. http://www.irsem.defense.gouv.fr.
21. GOLDSTEIN, Emmanuel. *The Best of 2600, Collector's Edition: A Hacker Odyssey.* Indianapolis, IN: Wiley Publishing Inc., 2009. ISBN 97-0-470-45853-2.
22. MIZRACH, Steven. «Is there a Hacker Ethic for 90s Hackers?» *Old and New Hacker Ethics.* [En línea] 1997 [citado el: 25 de febrero de 2013]. http://www2.fiu.edu/~mizrachs/hackethic.html.
23. MIRÓ LLINARES, Fernando. *El cibercrimen.* Madrid: Marcial Pons, 2012.
24. MITNICK, Kevin D. y SIMON, William L. *The art of Deception.* [Ed.] Carol Long. Indianapolis, IN: Wiley Publishing Inc., 2002. ISBN 0-471-23712-4.
25. Government Accountability Office. *Cyber Threats Facilitate Ability to Vommit Economic Espionage.* Government Accountability Office. Washington: s. n., 2012. Testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives. GAO-12-876T.
26. POSTEL, J. RFC 801. *NCP/TCP Transition Plan.* [Electrónico] s.l.: Network Working Group, noviembre de 1981.
27. FALLIERE, Nicolas, MURCHU, Liam O. y CHIEN, Eric. *W32. Stuxnet Dossier. Version 1.4.* Symantec Coporation, 2011.
28. ZETTER, Kim. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.* [En línea], Wired.com, 11 de julio de 2011 [citado el 24 de marzo de 2013]. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/.
29. ETSI. *TR 101 771V1.1.1. Service Independent Requirements Definition: Threat Analysis.* Sophia Antipolis, Francia: European Telecommunications Standards Institute, 2001-2004. Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).
30. Department of Defense (DoD). MIL-STD-882E. *Standard Practice. System Safety .* s.l., EE. UU.: Department of Defense (DoD), 11 de mayo de 2012.
31. Ponemon Institute. *The Human Factor in Data Protection.* Ponemon Institute LLC, 2012. Patrocinado por Trend Micro.
32. LYNN, William J. [*Defending a New Domain. The Pentagon's Cyberstrategy.* [En línea]: Council on Foreign Relations, Foreign Affairs, 1 de septiembre de 2010, [citado el 26 de marzo de 2013]. <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
33. CIALDINI, Robert B. *The Science of Persuasion.* Edición especial enero de 2004, Scientific American special edition, vol. 14, n.º 1, págs. 70-77.

34. CIALDINI, Robert B. *Influence.* [Ed.] Carolyn Merryll. Needham Heights, MA: Allynn & Bacon, 2001. ISBN 0-321-01147-3.
35. NIST. *Special Publication 800-30. Guide for conducting risk assessments.* Gaithersburg, MD: National Institute of Standards and Technology, 2012.
36. ISO. *ISO/IEC 27005: 2011 Information technology-Security techniques-Information security risk management.* ISO/IEC, 2011.
37. OIKARINEN, J. y REED, D. RFC 1459. *Internet Relay Chat Protocol.* [Electrónico] Network Working Group, mayo de 1993.
38. *Symantec Intelligence Report: February 2013.* Symantec Corporation, 2013. <http://www.symanteccloud.com/es/es/mlireport/SYMCINT_2013_02_February_ES.pdf>.
39. MARINO, Louis y SFAKIANAKIS, Andreas. *ENISA Threat Landscape. Responding to the Evolving Threat Environment.* European Network and Information Security Agency (ENISA). 2012.
40. KRAMER, Simon y BRADFIELD, Julian C. «A general definition of malware». Springer-Verlag, 2010, *Journal in Computer Virology,* vol. 6, n.º 2, págs. 105-114. Online ISSN 1772-9904.
41. KRYSIUK, Piotr y DOHERTY, Stephen. *The World of Financial Trojans.* Symantec Security Response. Mountain View, CA (EE.UU): Symantec Corporation, 2013 [citado el 7 de abril de 2013]. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_world_of_financial_trojans.pdf>.
42. DANG, Hiep. «The origins of social Engineering». *McAfee Security Journal.* Otoño de 2008. Santa Clara, CA (EE. UU.): McAfee Inc., 2008.
43. SHAH, Jimmy. «Los riesgos contra los datos confidenciales de los dispositivos móviles en el origen de las amenazas futuras». *McAfee Security Journal,* n.º 7. Santa Clara, CA (EE. UU.): McAfee Inc., 2011.
44. ISTTF. *Enhancing child safety and online technologies: final report of the Internet Safety Technical Task Force to the Multi-state Working Group on Social Networking of State Attorneys General of the United States.* Berkman Center for Internet & Society at Harvard University, 2008.
45. Equipo de Estudios del ONTSI. *Perfil sociodemográfico de los internautas, análisis de datos INE 2012.* Observatorio Nacional de las Tecnologías y de la Sociedad de la Información, 2013. ISSN 2172-9212.
46. The Boston Consulting Group, Inc. *The value of our digital identity.* Liberty Global Inc., 2012 [documento electrónico]. <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>.
47. RICHARDS, Reshan. «Digital Ctizenship and Web 2.0 tools». [En línea] Merlot, junio de 2010, *Journal of Online Learning and Teaching,* vol. 6, n.º 2. <http://jolt.merlot.org/vol6no2/richards_0610.htm>.

48. Blue Coat Systems. *2012 Web Security Report.* Blue Coat Systems Inc., 2013. <http://www.bluecoat.com/sites/default/files/documents/files/BC_2012_Security_Report-v1i-optimized.pdf>.
49. RIBBLE, Mike. *Digital Citizenship in Schools.* 2.ª ed. International Society for Technology in Education (ISTE), 2011. ISBN: 978-1564843012.
50. Kindsight. *Kindsight Security Labs Malware Report - Q4 2012.* [En línea]. Kindsight Inc., 2012. <http://www.kindsight.net/sites/default/files/Kindsight_Security_Labs-Q412_Malware_Report-final.pdf>.
51. Damballa. *Damballa Threat Report - First Half 2011.* [En línea]. Damballa Inc., 2011. <https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf>.
52. NAO. *The UK cyber security strategy: Landscape review.* Reino Unido: National Audit Office, 2013.
53. MAIALEN, Garmendia y otros. *Riesgos y seguridad en Internet: los menores españoles en el contexto europeo.* Universidad del País Vasco. Bilbao: EU Kids Online, 2011.
54. AGRE, P. E. y ROTENBERG, M. *Technology and privacy: The new landscape.* Cambridge (MA): MIT Press, 1998. ISBN: 9780262511018.
55. *MAGERIT versión 3.* Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.
56. «New firewall to safeguard against medical-device hacking». *Purdue University.* [En línea] 12 de abril de 2012 [citado el 14 de abril de 2013]. http://www.purdue.edu/newsroom/research/2012/120412RaghunathanHacking.html.
57. BUZAI, Gustavo D. «El ciberespacio desde la geografía. Nuevos espacios de vigilancia y control global». *Meridiano. Revista de Geografía.* [En línea] 2012, n.º 1 [citado el 25 de febrero de 2013]. http://www.revistameridiano.org/.
58. EUA, Joint Chief of Staff. *Estrategia nacional militar de los Estados Unidos de América .* Washington: Joint Chief of Staff EUA, 2011.
59. OCDE. *Future Global Shocks. Improving Risk Governance.* París: OCDE, 2011.
60. SOMMER, Peter y BROWN, Ian. *Reducing Systemic Cybersecurity Risk.* Informe: OCDE, 2011.
61. OSCE_MC.DEC/7/06. *DECISION No. 7/06: Countering the Use of the Internet for Terrorist Purposes.* Brussels: OSCE, 2006.
62. KAGAN, Robert. *Paradise and Power: America and Europe in the New World Order.* Londres: Atlantic Books, 2004.
63. WEGENER, Henning. *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence Building Measures.* [En línea] 23 de agosto de 2012 [citado el 29 de marzo de 2013]. http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Wegener publication.docx.

64. BAILEY, Eric. *«Nothing Can Justify Torture»: An interview with Noam Chomsky on Obama's human rights record.* [En línea] 12 de diciembre de 2012 [citado el 30 de marzo de 2013]. http://chomsky.info/interviews/20121212.htm.
65. The White House. *Cyberspace Policy Review.* Washington: The White House, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
66. The_White_House2. *International Strategy for Cyberspace.* Washington: The White House, 2011.
67. BIDEN, Joseph R. *VP's Remarks to London Cyberspace Conference.* Londres: The White House, 2011.
68. CLAPPER, James R. *Worldwide Threat Assessment of the US Intelligence Community 2013.* Washington DC: Office of the Director of National Intelligence, 12 de marzo de 2013.
69. ALEXANDER, Keith B. *Statement of general Keith B. Alexander Commander United States Cyber Command before the Senate Committee on armed services.* Washington: United States Cyber Command, 2013.
70. PELLERIN, Cheryl. *American Forces Press Service. Cybercom Builds Teams for Offense, Defense in Cyberspace.* [En línea] 12 de marzo de 2013 [citado el: 30 de marzo de 2013]. http://www.defense.gov/news/newsarticle.aspx?id=119506.
71. KEHLER, C. R. *Statement of general C. R. Kehler Commander United States Strategic Command before the Senate Committee on Armed Services.* Washington: United States Strategic Command, 12 de marzo de 2013.
72. LEWIS, James Andrew. *Critical Questions for 2013: Global Challenges. What's Next in Cybersecurity?* Center for Strategic and International Studies. [En línea] 25 de enero de 2013 [citado el: 30 de marzo de 2013]. http://csis.org/publication/critical-questions-2013-global-challenges.
73. BUMILLER, Elisabeth. «Pentagon to Beef Up Cybersecurity Force to Counter Attacks». *The new York Times*. [En línea] 29 de marzo de 2013 [citado el 31 de marzo de 2013]. www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html.
74. GEERS, Kenneth. *Cyberspace and the changing nature of warfare.* [En línea] 27 de agosto de 2008 [citado el 31 de marzo de 2013]. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.
75. HEALEY, Jason y BOCHOVEN, Leendert van. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington: The Atlantic Council of the United States, 2011.
76. PRINCE, Matthew. «The DDoS that Almost Broke the Internet». *Cloud Flare.* [En línea] 27 de marzo de 2013 [citado el 28 de marzo de 2013]. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet.

77. TIKK, Eneken. *Comprehensive legal approach to cyber security 2011*. Tarfu, Estonia: Faculty of Law, University of Tartu, 2011.
78. Unión Europea. «Council Framework Decision 2005/222/JHA». *Official Journal of the European Union.* [En línea] 16 de marzo de 2005 [citado el 31 de marzo de 2013]. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.
79. FROOMKIN, Michael. «Cybercrime Treaty Goes Live». *Discourse.net.* [En línea] 19 de marzo de 2004 [citado el 31 de marzo de 2013]. http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html.
80. ARCHICK, Kristin. *CRS Report for Congress. Cybercrime: The Council of Europe Convention.* Washington: Congressional Research Service, 2004.
81. SCHJØLBERG, Stein y GHERNAOUTI-HÉLIE, Solange. *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace,* segunda edición. Oslo: AiTOslo, 2011.
82. EUA_OSCE. [En línea] 16 de octubre de 2009 [citado el 31 de marzo de 2013]. https://dazzlepod.com/cable/09STATE107552/.
83. SCHNEIDER, Deborah. *United States Mission to the OSCE Cyber Security Keynote Address by Dr. Deborah Schneider, U.S. Department of State as delivered to the Joint FSC/PC.* Viena: OSCE, 2010.
84. SAFIRE, William. «The Farewell Dossier». *The New York Times.* [En línea] 2 de febrero de 2004 [citado el 2 de enero de 2013]. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsaire.
85. BROWN, Gary y POELLET, Keira. *The Customary International Law of Cyberspace.* IV, Strategic Studies Quarterly, otoño de 2012, vol. 6, págs. 126-145.
86. STEPHENS, Bret. «The limits of Stuxnet». *The Wall Street Journal.* [En línea] 18 de enero de 2011 [citado el 2 de enero de 2013]. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.
87. PERTERMANN, Kerstin. *Conference Report: Challenges in Cybersecurity, Risks, Strategies, and Confidence Building International Conference.* Hamburgo: Institute for Peace Research and Security Policy at the University of Hamburg, 2011.
88. VENTRE, Daniel. *La politique de cyberdéfense peut-elle être a-politique?* Paris: Ministère de la défense Délégation aux Affaires Stratégiques, 2013.
89. EES. *Estrategia Española de Seguridad.* Madrid: Gobierno de España, 2011.
90. PÉREZ, Jesús. «Cómo Cyberbunker atacó a Spamhaus y casi se llevó a medio Internet por delante». *Security By Default.* [En línea] 28 de

marzo de 2013 [citado el 12 de mayo de 2013]. http://www.security-bydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.

91. VENTRE, Daniel. *Japon: stratégies de cyberdéfense, Multi-System and Internet Security Cookbook.* MISC, n.° 64, 2012, págs. 65-73.
92. BAGCHI, Sohini. «India needs more warriors in the cyber space». *Cxotoday.com.* [En línea] 3 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.cxotoday.com/story/india-needs-more-warriors-in-the-cyber-space/.
93. ZORZ, Zeljka. «India has a new National Cyber Security Policy». *Help net security organization.* [En línea] 10 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.net-security.org/secworld.php?id=14891.

Principios de una conciencia nacional de *ciberseguridad*

Por José Tomás Hidalgo Tarrero

Sé extremadamente sutil, discreto, hasta el punto de no tener forma. Sé completamente misterioso y confidencial, hasta el punto de ser silencioso. De esta manera podrás dirigir el destino de tus adversarios. (Sun Tzu, El arte de la guerra, 550-500 a.C.).

Guerra total, guerra asimétrica y *ciberguerra*

En primer lugar quería hacer una disquisición sobre los paradigmas de la guerra total, la guerra asimétrica y la guerra cibernética. El paradigma de la *ciberguerra* es algo totalmente novedoso y es necesario compararlo con otros paradigmas que ya conozcamos para poder establecer un marco conceptual.

Según Carl Schmitt en su gran obra *El concepto de lo político* (1):

La llamada guerra total cancela la distinción entre combatientes y no combatientes y conoce, junto a la guerra militar, otra no militar (guerra económica, propagandística, etc.) como emanación de la hostilidad. Pero aquí la cancelación de la distinción entre combatientes y no combatientes es una superación dialéctica. No significa pues que, por ejemplo, los que antes no eran combatientes se hayan convertido pura y simplemente en combatientes de los de antaño. Son las dos partes las que cambian, y la guerra se hace ahora en un plano nue-

> *vo, intensificado, como activación ya no solo militar de la hostilidad. El carácter total consiste aquí en que ámbitos de la realidad de suyo no militares (economía, propaganda, energías psíquicas y morales de los que no combaten) se ven involucrados en la confrontación hostil. El paso más allá de lo puramente militar no representa tan solo una expansión cuantitativa; es también un incremento cualitativo. Por eso no supone una atenuación sino una intensificación de la hostilidad. La mera posibilidad de este incremento de intensidad hace que también los conceptos de amigo y enemigo se transformen de nuevo y por sí mismos en políticos y que, incluso allí donde su carácter político había palidecido por completo, se aparten de la esfera de las expresiones privadas y psicológicas.*

De la anterior definición se extrae que la guerra total abarca todos los ámbitos del Estado y cancela la distinción de combatiente y no combatiente porque todos los ciudadanos participan, voluntaria o involuntariamente, en el esfuerzo de guerra y todos sufren los efectos de la guerra. El Estado tiene que subordinar todo al esfuerzo de guerra porque de lo contrario será él mismo sometido.

Antonio Cabrerizo Calatrava, en su ponencia *El conflicto asimétrico* en el Congreso Nacional de Estudios de Seguridad, Universidad de Granada, 21-25 de octubre de 2002, (2) definió el conflicto armado asimétrico como:

> *...el que se produce entre varios contendientes de capacidades militares normalmente distintas y con diferencias básicas en su modelo estratégico. Alguno de ellos buscará vencer utilizando el recurso militar de forma abierta en un espacio de tiempo y lugar determinados y ateniéndose a las restricciones legales y éticas tradicionales. Su oponente u oponentes tratarán de desgastar, debilitar y obtener ventajas actuando de forma no convencional mediante éxitos puntuales de gran trascendencia en la opinión pública, agotamiento de su adversario por prolongación del conflicto, recurso a métodos alejados de las leyes y usos de la guerra o empleo de armas de destrucción masiva. Todo ello con el objetivo principal de influir en la opinión pública y en las decisiones políticas del adversario.*

De la definición de Antonio Cabrerizo se concluye que en la guerra asimétrica uno de los bandos se aparta del cumplimiento de las leyes y usos de la guerra, aunque exige a su oponente dicho cumplimiento; los medios usados por la parte «débil» son económicos porque no tiene la capacidad de obtener y emplear medios a la altura del oponente «fuerte». La guerra asimétrica también ha sido llamada guerra sin restricciones por algunos autores, en especial los dos coroneles del Ejército popular chino Qiao Liang y Wang Xiangsui, que acuñaron el término en su obra *Guerra sin restricciones* (3). Los coroneles Liang y Xiangsui son muy explícitos en

el apartarse del cumplimiento de las leyes y usos de la guerra y señalan, con cierta insistencia, el uso de las *ciberarmas* contra sistemas críticos del enemigo, no solo como parte de una guerra asimétrica entre estados sino también como parte de lo que llamamos terrorismo.

Otro aspecto que introducen los coroneles Liang y Xiangsui es involucrar, al menos de forma anímica, a todos los ciudadanos del país opositor, la parte «fuerte» o «poderosa», y ponerlos en contra de las autoridades para que obliguen a las mismas a aceptar los postulados, a ser posible en su totalidad, de la parte «débil» de la guerra.

Los principios establecidos en *Guerra sin restricciones* están en consonancia conceptual con los establecidos por el general chino Sun Tzu en *El arte de la guerra* (4), escrito hace más de 2.500 años. Las frases del inicio de este capítulo, sacadas de esta obra maestra de la estrategia, parecen hablar de la *ciberguerra* cuando no se conocía ni la electricidad. Eso es así porque hay una serie de principios o axiomas de la guerra que no cambian aunque cambien los medios con los que se libran las batallas.

Hay otros autores han apuntado que en el siglo XXI la guerra se civilizará, en el sentido de que no será el monopolio de los militares debido al uso generalizado de *ciberarmas* que estarán al alcance de cualquier persona incluso sin grandes conocimientos de informática.

El paradigma de la *ciberguerra* es en todo similar a los paradigmas de la guerra asimétrica y de la guerra total; fundamento esta aseveración en lo siguiente:

- Los efectos pueden alcanzar a todos los ciudadanos, administraciones, instituciones y empresas del Estado aunque no estén conectados al ciberespacio (paradigma de la guerra total).
- Involucra, voluntaria o involuntariamente, a todos los ciudadanos, administraciones, instituciones y empresas del Estado (paradigma de la guerra total).
- La relación entre eficacia y coste es muy alta, posiblemente la más alta, ya que puede inutilizar sistemas básicos y críticos de un país con un coste para el atacante extraordinariamente bajo (paradigma de la guerra asimétrica).
- No necesita de una infraestructura grande y costosa como la industria de armamento clásico –terrestre, naval, aéreo y NBQR– (paradigma de la guerra asimétrica).
- Solo necesita personas con muy buena formación en ingeniería informática y en psicología.
- En la *ciberdefensa* pasiva deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su

nivel y con sus medios (paradigmas de la guerra total y de la guerra asimétrica).

- La *ciberdefensa* activa es, o debe ser, función exclusiva, a nivel dirección, del Gobierno de la nación.
- Es muy difícil probar fehacientemente la autoría de un ataque a menos que el atacante quiera que se sepa, lo que proporciona un nivel de anonimato muy grande y convierte a la *ciberguerra* en una guerra pérfida (paradigma de la guerra asimétrica).

Como se ha visto, el paradigma de la *ciberguerra* es una mezcla de los paradigmas de la guerra total y de la guerra asimétrica que convierten a la *ciberguerra* en muy peligrosa por sus posibles efectos y por su perfidia. Además, crea un marco conceptual nuevo, la *ciberseguridad*, para el cual es necesario crear conciencia en todos los ciudadanos como individuos y como Estado.

Los efectos de que la cibernética pueda ser empleada como el arma pérfida del siglo XXI son que las amenazas son reales pero se perciben por el común de los mortales de manera difusa, cuando se perciben. Como no hay un conocimiento adecuado de los daños que puede producir un ataque informático, más allá de que puedan publicarse datos o fotos nuestros sin nuestro consentimiento o de que suframos un fraude informático, los usuarios de sistemas informáticos tienen grandes dificultades para percibir claramente la amenaza cibernética, lo que dificulta mucho la concienciación. En muchos casos, y a todos los niveles, se considera que los posibles efectos catastróficos, comparables en todo a los de algunas armas de destrucción masiva, son cosa de ciencia ficción y solo se pueden dar en las películas y novelas de dicho género.

Hay quienes distinguen entre seguridad informática y seguridad de la información. Podría considerarse que la *ciberseguridad* engloba ambos conceptos.

La seguridad informática, o de los sistemas de información, parece dirigirse más al ámbito de los sistemas informáticos, mientras que la seguridad de la información parece orientarse más por la seguridad de los datos transmitidos. Estas son disquisiciones académicas que el concepto de *ciberseguridad* debería superar al dirigirse a todo el conjunto de los sistemas informáticos y de la información tanto dentro de dichos sistemas como transmitida por cualquier medio físico o radioeléctrico.

Antecedentes de conciencia nacional de *ciberseguridad*

Antes de buscar y definir los principios de la conciencia nacional de *ciberseguridad,* quisiera mostrar una definición de lo que es conciencia. Para ello, creo que el *Cuaderno de Estrategia* n.º 155 del Instituto Español de

Estudios Estratégicos (5), más concretamente el inicio del segundo capítulo, página 68, escrito por D. José Antonio Marina Torres, es extremadamente didáctico y no me resisto a transcribirlo:

> *La palabra «conciencia» tiene dos significados. El primero, darse cuenta, percatarse de algo. En nuestro caso, de la importancia, dificultades, complejidades que tiene la seguridad y defensa de una nación. El segundo significado equivale a «conciencia moral», y hace referencia a los deberes, responsabilidades y al modo de cumplirlos. Una persona dormida, anestesiada o en coma no tiene conciencia en el primer sentido. Un criminal, un psicópata, no tiene conciencia en el segundo. Hago esta reflexión lingüística porque en el caso de la «conciencia de defensa» hay que utilizar ambos significados. Se trata de conocer la importancia, las dificultades, los problemas que plantea, y, también, la responsabilidad personal, ciudadana, ética y política.*

También en el caso de la conciencia nacional de *ciberseguridad* hay que utilizar ambos significados porque es necesario ser conscientes de las amenazas y es necesario conocer nuestros deberes como individuos, como miembros de diversas organizaciones, de la Administración y de instituciones y como directivos, en su caso, de ellas; debemos ser conscientes de nuestras responsabilidades tanto individuales como colectivas en el campo de la *ciberseguridad*; estas responsabilidades son, como en el texto transcrito, personales, ciudadanas, éticas y políticas.

La conciencia nacional de *ciberseguridad*, para que sea nacional, debe incluir a todos los ciudadanos y todas las instituciones, empresas y organizaciones pues de lo contrario presentará carencias y flancos débiles que serán usados, sin ninguna duda, por los atacantes.

Si la *ciberguerra* alcanza a todos los ciudadanos tanto en sus efectos como en sus medios, parece lógico que los ciudadanos, que ya están involucrados voluntaria o involuntariamente, tomen conciencia de ello y participen en la defensa. Pero no solo la *ciberguerra* alcanza a todos los ciudadanos; también el *cibercrimen*, que utiliza los mismos medios o parecidos pero con otros fines, tiene como objetivo a cualquier ciudadano. Por esto la conciencia de *ciberseguridad* debe ser nacional pues de otra manera siempre habrá puertas abiertas para que los atacantes, sean *ciberguerreros* o *cibercriminales*, tengan más probabilidades de éxito al no ofrecer un frente, una muralla sólida y completa.

La conciencia de *ciberseguridad*, de acuerdo con el paradigma de la *ciberguerra*, debe cubrir todos los aspectos de los sistemas informáticos y de las comunicaciones, empezando por el eslabón débil en todos ellos: el ser humano que los construye, los mantiene y los usa. El uso de los sistemas informáticos como armas, aunque no estuvieran ni remotamente pensados para ser usados como tales armas, implica que deben ser diseñados, construidos y mantenidos pensando en que sí pueden ser em-

pleados como armas por terceras personas y, sobre todo, como objetivos de las mismas.

Para ver contexto de conciencia de seguridad en el que nos encontramos en España creo que es conveniente resaltar algunos resultados del estudio n.º 2912 del Centro de Investigaciones Sociológicas (CIS) (6):

- En la pregunta 1 del estudio se constata que el 52,2% de la población califica la profesión de militar con una nota mínima de 7.
- Las respuestas a las preguntas 7 y 7a del estudio revelan que solo el 19,68% de la población se sacrificaría por salvar a su patria, su nación, su país.
- De las respuestas a la pregunta 8 se infiere que solo el 40,4% estaría dispuesto a participar voluntariamente en la defensa del país.
- Sin embargo, de las respuestas a la pregunta 9 se ve claramente que el 66,3 % justificaría que el Gobierno de la nación ordenase una acción militar en caso de invasión del territorio nacional.
- Las respuestas a la pregunta n.º 14 son reveladoras del nivel de conciencia nacional de seguridad y defensa: el 62,3% de los encuestados siguen con poco o nulo interés las informaciones relativas a la defensa nacional o las Fuerzas Armadas.

De lo expuesto del estudio del CIS se desprende que se considera la seguridad y defensa nacional como algo que pertenece al ámbito exclusivo de lo militar y que los ciudadanos no militares tienden a no involucrarse en la misma. Esto es algo conocido y tratado en muy diversos foros.

De lo anterior se deduce que no hay conciencia de seguridad pues falta, en el mejor de los casos y lo demuestra con mucha claridad la encuesta del CIS ya mencionada, la segunda parte de la definición de conciencia: la de los deberes y obligaciones. En general, tendemos a creer que la seguridad es algo que, cual maná, cae del cielo y no tenemos que preocuparnos de ello por lo que no es necesario hacer sacrificios para obtenerlo.

Pues si el nivel de conciencia nacional de seguridad y defensa es poco alto, el nivel de conciencia nacional de *ciberseguridad* puede ser incluso menor.

Hay poca literatura sobre los principios en los que se debe asentar una conciencia de *ciberseguridad,* lo cual no es de extrañar dado que la *ciberseguridad* es algo extraordinariamente novedoso en lo que unos pocos empezaron a pensar algún tiempo después de que los sistemas informáticos empezasen a conectarse a través del ciberespacio utilizando redes, fundamentalmente Internet, que no eran propiedad del propietario del sistema. Además, al principio se veían los ataques informáticos con la misma óptica con la que se veían las películas y se leían las novelas de piratas o se recreaba la lucha de David contra Goliat por lo que muy poca

gente se preocupaba del asunto. Sí que se ha escrito bastante sobre conciencia de seguridad y de defensa y se ha resaltado como un problema grave de nuestra sociedad la falta de conciencia de *ciberseguridad*.

Por todo lo anterior, hay que buscar una actividad humana que pueda servir de referencia. Esta actividad debe estar extendida por todo el mundo, y la conciencia de seguridad en esa actividad debe haber conseguido que sea muy segura aunque intrínsecamente sea muy peligrosa; además, las personas involucradas en esa actividad deben estar contentas y orgullosas de tener esa conciencia de seguridad. Asimismo es necesario que esa conciencia no lleve aparejado el miedo atenazador que dificultaría el desempeño de esa actividad.

La primera actividad que me viene a la mente que cumpla esos requisitos es el volar. Además, el mundo de la aeronáutica tiene desde hace décadas conciencia de seguridad de vuelo. Se conciencia a todos los involucrados y a los pasajeros. Creo que puede ser un buen referente. Tanto el Ejército del Aire (7) como Aeropuertos Españoles y Navegación Aérea (AENA) (8) tienen diversos manuales y publicaciones sobre seguridad de vuelo y sobre conciencia de seguridad.

¿Por qué la seguridad de vuelo puede ser un buen referente? Hay varias razones para ello, entre las cuales podemos citar las siguientes:

- En primer lugar, las amenazas a la seguridad de vuelo son muchas, pero las tripulaciones son conscientes de ellas, las asumen y se preparan para el caso de que se materialicen.
- En segundo lugar, todos los involucrados en la operación de las aeronaves están concienciados de su importancia en la seguridad de las mismas y se preparan para ello.
- En tercer lugar, existe una organización de seguridad de vuelo presente en las instituciones que operan aeronaves, empresas de aviación, centros de control, etc.
- En cuarto lugar, hay conciencia y cultura de seguridad de vuelo, que cubre todas las fases del vuelo desde antes incluso de que las tripulaciones suban a bordo. La cultura es no punitiva, excepto casos de delito o negligencia flagrante, y se anima a todos los involucrados a notificar los errores cometidos y las incidencias sufridas.
- Los pasajeros también son conscientes de las amenazas inherentes al vuelo y sus riesgos pero los asumen y contribuyen, mayoritariamente, de acuerdo con las instrucciones comunicadas por los tripulantes de cabina de pasajeros.
- Esta conciencia y la cultura creada por esa conciencia han conseguido que volar, una actividad a priori peligrosa, sea de las más seguras con una tasa de accidentes muy baja.

Principios en los que se debe basar la conciencia nacional de *ciberseguridad*

Por las razones anteriores creo que se puede establecer un cierto paralelismo entre la seguridad cibernética y la seguridad de vuelo y, por tanto, establecer los siguientes principios de la conciencia de *ciberseguridad:*

- Conocimiento de las amenazas y de los riesgos y asumirlos.
- Notificación por los usuarios de los errores cometidos e incidencias sufridas.
- Información por los responsables de seguridad de los sistemas informáticos de los proveedores de servicios de Internet (ISP), de las instituciones y empresas a los usuarios, miembros, empleados y clientes.
- Formación de todos, cada uno en el nivel que corresponda, en *ciberseguridad*.
- Adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio.

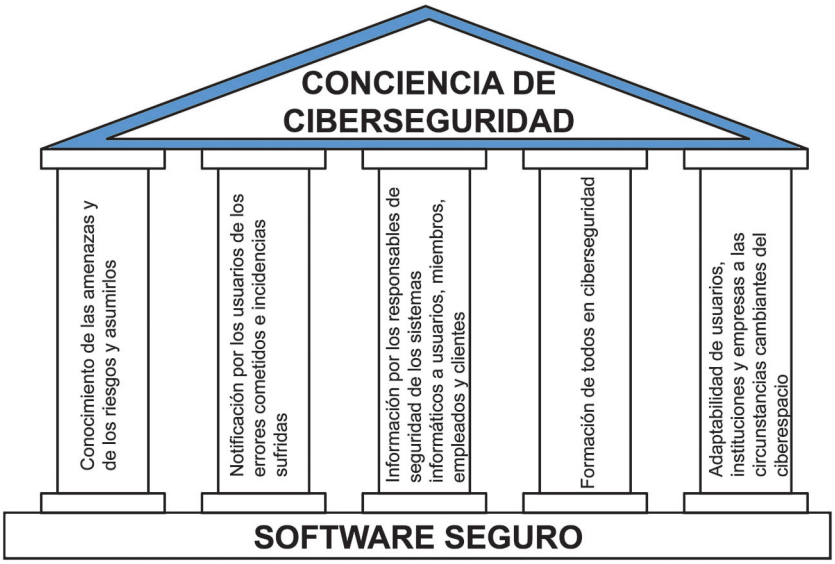


Figura 1. El edificio de la conciencia de ciberseguridad.

Conocimiento de las amenazas y los riesgos y asumirlos

Las tripulaciones aéreas son plenamente conscientes de las amenazas y los riesgos de las mismas; pero, en lugar de estar atenazados por el miedo, las asumen, las estudian y se preparan para ellas.

La asunción de los riesgos implica, de acuerdo con la segunda parte de la definición de «conciencia» y con la definición de «asumir» que da la Real Academia de la Lengua, aceptar y cumplir las obligaciones y deberes necesarios para hacer frente a los mismos. Nunca la asunción de un riesgo puede implicar pasividad ni repudio del mismo; todo lo contrario, implica proactividad, que forzosamente debe estar basada en el conocimiento y el estudio, para hacer frente a los riesgos de materialización de las amenazas.

Los diseñadores, constructores y todos los que trabajan en la construcción y mantenimiento de las aeronaves y en su operación, tanto personal de vuelo como personal de tierra, y todos los que trabajan en los centros de control, en el diseño, construcción y mantenimiento de los sistemas de control aéreo, son también conocedores de las amenazas y riesgos inherentes a la actividad aeronáutica, los asumen y cumplen con sus deberes y obligaciones relacionados con la seguridad de vuelo.

De la misma forma, todos los usuarios del ciberespacio, los administradores de los sistemas informáticos, las autoridades, los directivos de las empresas, los diseñadores, programadores, etc. deben ser plenamente conscientes de las amenazas que hay en el ciberespacio y los riesgos inherentes a las mismas; de esta forma, podrán actuar, cada uno en su ámbito, de manera que las posibilidades de éxito de los ataques se reduzcan.

El tener consciencia de las *ciberamenazas* no quiere decir que haya que evitar hacer uso del ciberespacio, sino que implica hacer un uso responsable del mismo.

De la misma manera que no dejamos de utilizar el avión, el tren o el automóvil por las amenazas, que se materializan en forma de accidentes, que se ciernen sobre esos medios de transporte, debemos seguir haciendo uso del ciberespacio.

Es impensable no hacer uso del ciberespacio y mantener, ni hablar de mejorar, los actuales niveles de calidad de vida. Cosas tan básicas como el abastecimiento de energía eléctrica, combustible o agua en nuestras casas o empresas dependen de la informática y el ciberespacio. El disponer de nuestro dinero rápidamente en cualquier sitio o pagar sin llevar dinero en efectivo es hoy en día imposible sin ayuda de la informática y el ciberespacio.

Pero hacer un uso irresponsable del ciberespacio puede llevar a que no podamos disponer de energía eléctrica o de otros servicios básicos. No me refiero con uso irresponsable a un uso delictivo, que será perseguido con arreglo al ordenamiento legal vigente, sino simplemente a un uso negligente, posiblemente por desconocimiento, del ciberespacio al no tener correctamente configurado el sistema operativo o no tener antivirus actualizado, por citar un par de ejemplos.

Se sabe que el ataque con el virus Stuxnet a las centrifugadoras de la planta iraní de Natanz se hizo a través de una memoria USB que, supuestamente, cayó accidentalmente en manos de uno de los ingenieros que trabajaban en la planta y que lo usó bien directamente en un ordenador de control de la planta o bien en otro ordenador en el que trabajaba en el *software* del sistema de control de la planta para luego copiarlo, junto con el virus, al sistema de control de la planta. Un uso responsable del ciberespacio implica que antes de usar una memoria USB que nos llega casualmente, hay que comprobar qué tiene y cómo se comporta y, desde luego, antes de usarla en un ordenador del trabajo pedir a los responsables de seguridad informática del trabajo, si los hay, que la comprueben; después, si no se está completamente seguro de que no tiene ningún *malware,* mejor no usarla.

De la misma manera que llevamos el ordenador al servicio técnico para que le reparen cuando se avería, también debemos llamar al técnico para que revise la configuración o tener instaladas las utilidades que nos pueden ayudar a mantener una configuración segura y eficiente.

Los responsables de seguridad de cada sistema informático tienen que asegurarse de que sus usuarios sean conscientes de las amenazas que existen en el ciberespacio y de las consecuencias, directas e indirectas, que tiene tanto el mal uso como el no uso. No se trata de meter miedo, que siempre es un mal aliado, sino de dar a conocer las amenazas y que hay medios para seguir utilizando el ciberespacio con un cierto grado de seguridad, nunca la seguridad absoluta. Además, deben tratar de conseguir que los usuarios tengan el hábito de notificar –la notificación se tratará en el apartado siguiente– todas las incidencias al responsable de seguridad del sistema o del ISP, en caso de usuarios domésticos.

Ni esta concienciación ni todos los medios disponibles para la *ciberdefensa* pueden conseguir que seamos inmunes a los ataques, pero sí pueden conseguir que la mayor parte de ellos no tenga éxito y que tengamos una resiliencia mucho mayor ante los que consigan tener éxito de tal forma que el daño sea mínimo y los efectos de dicho daño poco duraderos.

Notificación por los usuarios de los errores e incidencias sufridos

En el mundo de la aviación, todas las tripulaciones y controladores cuentan las incidencias y hasta los errores propios al responsable de seguridad de vuelo. Esta cultura de seguridad no punitiva, excepto en los casos de negligencia grave y conductas delictivas, va acompañada de algo que puede asimilarse perfectamente al secreto profesional: ningún responsable de seguridad de vuelo divulgará jamás datos que puedan identificar a las personas involucradas en un incidente. En los boletines de seguridad de vuelo se comentan incidentes y accidentes pero no se identi-

fica a las personas. Se analiza la actuación de las personas para sacar conclusiones y mejorar la seguridad de vuelo, y tanto si la actuación ha agravado el incidente como si la ha solventado con éxito se dice; en el primer caso, para que otros no vuelvan a hacer lo mismo en las mismas o similares circunstancias, y en el segundo, para que si alguien se tiene que enfrentar a una situación igual o similar haga lo mismo.

En el mundo de la aviación los usuarios son sujetos pasivos, a pesar de lo cual en cada vuelo se les informa de procedimientos de seguridad básicos; sin embargo, en el ciberespacio los usuarios son sujetos activos: los usuarios «vuelan» en el ciberespacio, de hecho se usa el verbo «navegar» para la acción de ir a diferentes sitios y buscar en la red, y «pilotan» su ordenador en ese «vuelo».

En el ciberespacio los usuarios deberían notificar al responsable de *ciberseguridad* de su organización, o de su ISP si es en el entorno del hogar, todas las incidencias, incluso los errores propios aunque crea que no están directamente relacionados con ataques informáticos.

Este principio es el que, sin ninguna duda, genera más resistencia entre los usuarios. Significa un cambio de mentalidad, un giro copernicano en la actitud de los ciudadanos. Admitir que hemos cometido un error no es lo habitual, ni siquiera admitirlo en la intimidad; pero es necesario que todos los usuarios colaboren contando a los responsables de seguridad del sistema que utilizan, en el caso de los hogares y las pymes con menos recursos, las incidencias sufridas y los errores cometidos. El responsable de seguridad informática les guiará y dará consejos para evitar los errores cometidos, pues de otra forma se volverán a cometer los mismos errores. Debemos ser plenamente conscientes de que errar es de humanos y de que al mejor escribano le cae un borrón; todos cometemos errores y son errores porque son fallos no intencionados debidos a falta de conocimiento, estrés, etc., y por ello no perdemos ni categoría ni imagen ni nada. Repetir los errores por no reconocerlos y no pedir la ayuda necesaria sí que implica orgullo desmedido y eso no es bueno ni para las personas ni para las organizaciones.

Los usuarios deben saber que sus datos personales están protegidos por la Ley Orgánica 15/1999 de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (LOPD), y que los responsables de *ciberseguridad* no deben desvelar nada que permita identificar al usuario que ha notificado un incidente o error. En el mundo de la aviación, tanto civil como militar, mucho antes de que existiera la LOPD, los responsables de seguridad de vuelo nunca han desvelado los datos personales de los notificantes ni de los protagonistas de los incidentes o errores ni otros datos que pudieran permitir su identificación. Este es uno de los pilares fundamentales de la cultura y conciencia de seguridad de vuelo.

También deben saber los usuarios que notificar las incidencias que les ocurren contribuye a mejorar la *ciberseguridad* de todos, incluida la suya. En el ámbito de la seguridad de vuelo, todos son conscientes de que las notificaciones de incidentes y errores contribuyen a salvar vidas; pues en el ámbito de la *ciberseguridad* todos debemos ser conscientes de que nuestras notificaciones contribuyen a que todos podamos utilizar mejor el ciberespacio y que las infraestructuras críticas puedan seguir proporcionándonos calidad de vida e incluso vida propiamente dicha.

Cada usuario debe tener muy claro quién es el responsable de seguridad cibernética en cada ámbito y como dirigirse a él.

Las notificaciones deben ser sencillas de hacer por vía telemática o, en su defecto, telefónica, aunque preferentemente la primera. Cualquier usuario debe ser capaz, independientemente de su nivel de formación, de rellenar los datos que deban ser aportados manualmente por el usuario, mientras que los datos automáticos del formulario deben poder ser accesibles por el mismo usuario. Debe garantizarse la confidencialidad de la notificación por lo que no deben incluirse datos personales de manera obligatoria; una dirección de correo electrónico o número de teléfono puede ser de gran ayuda para facilitar un posterior contacto del responsable de *ciberseguridad* que puede necesitar más datos, incluso meras percepciones, en la investigación del incidente.

Sin notificaciones es extremadamente difícil desarrollar una *ciberseguridad* real que pueda minimizar la efectividad de los ataques. Esto no es como la batalla de Inglaterra donde el premier Churchill dijo: «nunca en el campo del conflicto humano, tanta gente le debió tanto a tan pocos». En el campo del *ciberconflicto* todos debemos participar en nuestra defensa desde mucho antes de que empiece el conflicto y una de las formas es que todos los usuarios del ciberespacio notifiquen todos los incidentes y errores a los responsables de seguridad. Con las notificaciones de los usuarios se crea una base de conocimiento que siempre será de extrema utilidad para poder defenderse de otros ataques parecidos; además, ayudará a mejorar la información que se dé en los boletines de *ciberseguridad*.

Información por los responsables de seguridad de los sistemas informáticos de los ISP, de las instituciones y empresas a los usuarios, miembros, empleados y clientes

En el ámbito de la seguridad de vuelo, los responsables de los distintos niveles redactan y difunden periódicamente boletines de seguridad de vuelo. En estos boletines se dan consejos, se difunden buenas prácticas, se comentan incidentes y accidentes, con el debido ocultamiento de datos que puedan identificar a los implicados en los mismos, explicando las causas, qué hicieron las tripulaciones y qué efectos produjeron dichas

acciones. Si la actuación de la tripulación fue la adecuada se explica y si no lo fue se explica qué debía haber hecho.

En el ámbito de la seguridad informática, los responsables de seguridad de los sistemas informáticos deberían, al igual que se hace en el ámbito de la seguridad de vuelo, elaborar, cada uno dentro de su ámbito y en colaboración con los homólogos de otras empresas, administraciones, instituciones e ISP, boletines de información sobre *ciberseguridad* y recibir y analizar las notificaciones de incidencias de los usuarios del sistema del que es responsable. Además, son también responsables de diseñar una política de *ciberseguridad,* que será aprobada por la dirección o autoridad competente, y de difundirla.

El hecho de que la informática esté tan difundida añade dificultades para el establecimiento de las redes de seguridad necesarias para que la notificación y la información sean efectivas; pero no por ello deberíamos cejar en el empeño de tratar de implantar esa red. También las mismas redes que se utilizan en el ciberespacio facilitan la difusión de los boletines de *ciberseguridad*. En este aspecto siempre es preferible pecar por exceso que por defecto. Los delincuentes suelen preferir objetivos fáciles y poco defendidos que aquellos otros que saben que están bien defendidos y el personal alerta.

Los boletines deben estar redactados de forma sencilla y amena porque van dirigidos tanto al personal que tiene una formación sólida en informática y *ciberseguridad* como a aquellos usuarios que carecen de ella aunque la tengan en otras áreas del conocimiento.

Formación de todos, cada uno en el nivel que corresponda, en «ciberseguridad»

Desde la escuela a la universidad, desde los más jóvenes a los más mayores, en todas las administraciones, instituciones, empresas, a empleados y desempleados, en el hogar.

No se trata de formar *hackers,* que también lo es –de *white hat hackers*[1]–, sino de que todos los ciudadanos tengan unas mínimas nociones de cómo mantener su entorno cibernético seguro, de qué y cómo se puede publicar en el ciberespacio sin comprometer la privacidad, confidencialidad y disponibilidad de esos datos. Así mismo, hay que enseñar a todos los ciudadanos a utilizar las herramientas básicas de *ciberseguridad* como pueden ser antivirus, configuración del *firewall* y actualizaciones automáticas.

[1] *White hat hacker* es el nombre dado a los *hackers* que trabajan en empresas y organizaciones, públicas y privadas, para probar los sistemas informáticos que produce y/o usa la empresa u organización para la que trabajan.

Es curioso comprobar cómo en los estudios de ingeniería informática del plan anterior a Bolonia había, como mucho, una única asignatura dedicada a la seguridad informática que era optativa o de libre elección en 5.º curso; en los de grado en ingeniería informática, ingeniería de computadores, ingeniería del *software*, ingeniería telemática o similares solo hay entre una y como mucho tres asignaturas, entre obligatorias y optativas, sobre seguridad informática. La cuestión no es baladí: si los profesionales que deben, o deberían, desarrollar los sistemas informáticos no están concienciados ni tienen una sólida formación en materia de seguridad cibernética, difícilmente podremos desarrollar sistemas informáticos seguros, siempre asumiendo que la seguridad absoluta no existe.

Lo mismo ocurre en los estudios de formación profesional del área de informática, donde solo hay una titulación de grado medio y otra de grado superior con una única asignatura de *Ciberseguridad*.

Sin embargo, es una cuestión de seguridad nacional tener profesionales con una sólida formación en *ciberseguridad* trabajando en todos los sectores de la nación, tanto privados como públicos, en el desarrollo y en el mantenimiento de sistemas informáticos, con mentalidad de seguridad informática, y en el aseguramiento de los ya existentes cuando no lo estén.

Además, existe un área de investigación y desarrollo en informática que conlleva la búsqueda e implementación de algoritmos y sistemas más eficientes y más seguros y de métodos de pruebas de seguridad del *software* y de los sistemas informáticos.

En la actual situación, hay que empezar por formar y concienciar a los docentes en todos los niveles para que estos a su vez puedan formar a sus alumnos. Dependiendo del nivel y del área, esta formación variará; en la mayor parte de los casos se trata solo, y no es tarea banal ni fácil, de enseñar buenas prácticas en el uso de sistemas informáticos y de comunicaciones. Estas buenas prácticas no dejan de ser una especie de buena educación informática que podríamos llamar *ciberurbanidad* o *cibereducación*.

Hay que enseñar el valor de la información, de los datos propios y del daño que podemos sufrir nosotros y la colectividad a la que pertenecemos por el mal uso de esa información y de los datos personales y de los sistemas informáticos y de comunicaciones. Unos docentes con una sólida conciencia de *ciberseguridad* y con la *ciberurbanidad* perfectamente interiorizada son imprescindibles para implantar una conciencia de *ciberseguridad* basada en estos principios entre sus alumnos.

La labor de estos docentes será de vital importancia aunque sus frutos no podrán verse a corto plazo sino a medio y largo plazo.

Caso aparte es el de las escuelas y facultades de Informática. La gran mayoría de los directores y decanos de las mismas están concienciados

y practican, en mayor o menor medida, la *ciberurbanidad*. Sin embargo, hasta ahora los planes de estudio oficiales apenas incidían en la *ciberseguridad*. Esto está cambiando con los nuevos planes de estudio basados en el Espacio Europeo de Enseñanza Superior (EEES), también conocidos como planes Bolonia. Distinto es el caso de la formación profesional donde la *ciberseguridad* sigue siendo una rareza. Esperemos que esta situación cambie y haya pronto nuevos planes de estudio de formación profesional donde, aparte de una especialización en la materia, en todos los cursos haya alguna asignatura de seguridad informática.

Para el corto plazo es necesaria la colaboración de las diferentes administraciones públicas y de la sociedad civil. El papel de la sociedad civil se trata en otro apartado de este capítulo, pero quiero adelantar que es fundamental en la formación de una conciencia nacional de *ciberseguridad,* sobre todo pensando en el corto plazo.

Adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio

A lo largo de la historia del planeta, los que no se han sabido adaptar han sucumbido y desaparecido. Esto ha ocurrido en el mundo vegetal y animal, el microscópico y macroscópico; las civilizaciones pasadas han ido desapareciendo bajo la presión de civilizaciones nuevas que introducían mejoras técnicas, científicas y morales que las convertían en superiores.

La historia militar está plagada de casos en los que un Ejército sucumbía a otro que introducía nuevo armamento, estrategia o táctica.

Al ser el ciberespacio un concepto no dimensional, sus posibilidades de cambio y la velocidad a la que ocurren esos cambios son muy grandes, casi podríamos decir que ilimitadas. Esto implica la necesidad de adaptarse a todos esos cambios a la misma velocidad, al menos, con la que se producen.

Pero el ciberespacio es un dominio que requiere una gran especialización por parte de los gestores de la *ciberseguridad* por lo que es necesario que las instituciones y empresas adopten una estructura de *ciberseguridad* con un jefe de *ciberseguridad* al frente que será el encargado de recibir las notificaciones, estudiarlas, eliminar de las mismas datos que puedan permitir identificar a personas, hacer encuestas, estudios, informes y, con todo lo anterior, editar informes de *ciberseguridad* en los que, entre otras cosas, publicará buenas prácticas a los usuarios acompañadas de ejemplos de los que se han eliminado todos los datos que permitan identificar al usuario.

El mero hecho de interiorizar los principios aquí formulados y emplear la *cibereducación* ya supone un cambio y una adaptación a este nuevo dominio. Pero es solo el primer cambio y es de índole personal; las or-

ganizaciones deben adaptarse y el primer signo de esta adaptación es la implantación de una estructura de *ciberseguridad*, incardinada dentro de la más general de seguridad, si existe, que deberá estar dimensionada de acuerdo con el tamaño de la empresa. Para aquellas empresas cuyo tamaño sea tan pequeño que ni siquiera tengan administrador del sistema informático y para los hogares, deberá ser el ISP correspondiente quien proporcione esta estructura de *ciberseguridad*.

La base de los principios de conciencia nacional de «ciberseguridad»

Los principios o pilares sobre los que se asienta la conciencia nacional de *ciberseguridad* deben, a su vez, tener unos cimientos sólidos.

Esos cimientos, cual zapata en una edificación, deben ser la concienciación de los diseñadores, arquitectos y programadores del *software* en hacer *software* seguro. Nunca se conseguirá un *software* que sea totalmente seguro, pero debe tenderse a ello.

De poco vale que los usuarios notifiquen, los responsables de seguridad informática informen, esté todo el mundo bien formado en *ciberseguridad*, las empresas, instituciones, administraciones y usuarios sean flexibles y adaptables y que todos asuman las amenazas; si el *software* es de mala calidad y, por tanto, muy susceptible a los ataques informáticos, al final los ciberdelincuentes serían los «señores» del ciberespacio.

Los ingenieros informáticos y telemáticos también deben ser conscientes de las amenazas y diseñar los sistemas informáticos teniendo muy presentes los factores de calidad del *software* (9) (10) y (11), algo de lo que se han examinado y aprobado para ser ingenieros tanto técnicos como superiores.

Hay que tener presente que los ataques informáticos se aprovechan de debilidades del *software* o usan ingeniería social[2] aunque lo más frecuente es que sea una combinación de ambos medios. En el primer caso, un *software* de calidad presentará menos debilidades y en el segundo, el ingeniero siempre puede diseñar el protocolo de acceso al sistema con más redundancia para evitar, en la medida de lo posible, que un fallo de uno de los usuarios al revelar una contraseña, por ejemplo, pueda permitir el acceso a personas que no deberían poder acceder. Por tanto, un *software* de calidad es siempre mucho más seguro que otro de mala calidad.

[2] Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica) (consultado el 2 de mayo de 2013).

No obstante, hay que recordar una frase célebre de Albert Einstein: *Every day, man is making bigger and better fool-proof things, and every day, nature is making bigger and better fools. So far, I think nature is winning*. («Cada día, el hombre está haciendo cosas más grandes y mejores a prueba de tontos, y cada día, la naturaleza está haciendo tontos más grandes y mejores. Hasta el momento, creo que la naturaleza está ganando»). Por lo que es necesario seguir investigando.

Es de sobra conocido que, durante la Segunda Guerra Mundial (SGM), en Blechtley Park se aprovecharon de la conjunción de debilidades de la máquina Enigma y de fallos de los operadores para descifrar los mensajes; los operadores de la Enigma naval, un poco más compleja, eran más cuidadosos y costó mucho más descifrar estos mensajes. Si Enigma no hubiera tenido la debilidad de que el resultado de cifrar una letra no podía ser ella misma y los operadores no hubieran transmitido mensajes de prueba hechos pulsando repetidas veces la misma letra, su *crackeo* habría sido mucho más difícil.

No es excusa decir que no está en las especificaciones; a un arquitecto no le consentiríamos que nos diseñara una casa sin puertas simplemente porque no le hemos dicho que queríamos puertas en las habitaciones y para entrar en la casa. Del mismo modo, un ingeniero en informática debe diseñar el sistema informático pensando en todos los factores de calidad del *software*, entre los cuales, insisto, están la seguridad, también llamada integridad, la robustez y la fiabilidad.

Esta *ciberseguridad* en el diseño y construcción del *software* no es realmente imposible de conseguir. Para tener unos niveles básicos, bastan ciertas normas de sobra conocidas por los ingenieros informáticos y telemáticos como son, entre otras, el control de las entradas al sistema y a cada módulo, no solo del tipo de datos, algo que suelen hacer automáticamente los lenguajes informáticos con *tipado* fuerte, sino también del valor y longitud de los datos para evitar situaciones indeseadas que pueden permitir una escalada de privilegios. También se deben controlar las pilas[3] y colas[4] para evitar el rebose incontrolado. Implementar un control de excepciones[5], por lo demás disponible en gran parte de todos

[3] Una pila en ingeniería del *software* es como un tubo con uno de los extremos cerrado en el que los elementos introducidos solo se pueden extraer en orden inverso de entrada, primero el último, después el penúltimo y así sucesivamente. Se asocia el acrónimo LIFO (*Last In, First Out*: último en llegar, primero en salir).

[4] Una cola en ingeniería del *software* es como un tubo con los dos extremos abiertos en ella; los elementos se introducen por un extremo y se sacan por el otro en el mismo orden en el que fueron introducidos. Se asocia el acrónimo FIFO (*First In, First Out*: primero en llegar, primero en salir).

[5] En ingeniería del *software* una excepción es un evento no esperado o infrecuente, ejemplos típicos son los errores en tiempo de ejecución como la división por cero o índices de tablas fuera de rango. (14)

los lenguajes de programación modernos –aunque desgraciadamente no en todos– es una garantía de robustez

Finalmente, es importante que los ingenieros diseñen pruebas lo más exhaustivas posibles del *software*, tanto de caja blanca como de caja negra, para las unidades que componen el *software*, así como de integración, validación y del sistema. Estas pruebas deben incluir una mezcla de pruebas manuales y de pruebas automatizadas: en los niveles más bajos habrá un porcentaje mayor de pruebas manuales mientras que en los niveles superiores, integración, validación y sistema, el mayor porcentaje será de pruebas automatizadas. En las pruebas de validación tiene especial importancia la colaboración del usuario al notificar todas las incidencias ocurridas y los errores cometidos por el propio usuario y la reacción del sistema ante esos errores.

Dentro de las pruebas de sistema, son de especial relevancia para la *ciberseguridad* las pruebas de seguridad en las que el sistema debe ser literalmente atacado, usando incluso ingeniería social, para detectar debilidades.

Se puede argüir que todo este cuidado en el diseño y construcción del *software* y las pruebas de calidad encarecen el producto; es cierto, pero de igual manera que no se pueden vender coches sin homologar o aviones sin certificación, no debería venderse *software* sin certificación porque las debilidades que tiene el *software* de mala calidad le hacen más susceptible a los ataques y esos ataques a ordenadores individuales pueden ser parte de un ataque a los sistemas críticos de la nación; ataques que redundarán, en cualquier caso, en pérdidas para el usuario.

Requisitos necesarios para poderlo hacer

De acuerdo con todo lo anterior, la formación de esta conciencia debería empezar de manera inmediata y a todos los niveles, empezando en la escuela, terminando en los centros de mayores y pasando por todos los centros educativos públicos y privados y en todas las instituciones y empresas.

Ya se ha tratado en este capítulo la importancia de la formación de todos los docentes en *ciberurbanidad* por lo que no voy a insistir en este aspecto, aunque quiero resaltar que es un requisito necesario y, al menos en mi opinión, suficiente para formar una conciencia nacional de seguridad cibernética a medio y largo plazo.

El primer y principal requisito es que quienes tienen la potestad de tomar la iniciativa, tanto en los distintos niveles de las administraciones como en las instituciones y empresas, sean conscientes de la necesidad de la *ciberseguridad* y actúen en consecuencia desarrollando u ordenando de-

sarrollar campañas de concienciación en *ciberseguridad* en su ámbito y monitorizando los resultados de las mismas.

Si empezamos a nivel nacional, es lógico que el Gobierno se muestre concienciado y sienta la necesidad, y así lo ha mostrado en diferentes ocasiones en los últimos años mediante la publicación de diferentes documentos oficiales sobre política y estrategia de seguridad nacional en los que hace mención a la *ciberseguridad*, de desarrollar una estrategia nacional de *ciberseguridad*, de fomentar la cultura de *ciberseguridad* y la *ciberurbanidad*.

Paso a paso el Gobierno de la nación ha ido desarrollando una estrategia nacional de *ciberseguridad*, de la cual se ha oído hablar en muy diversos foros dedicados a la *ciberseguridad*, que verá la luz en poco tiempo, si es que no lo ha hecho antes de la publicación de esta monografía; esta estrategia, siguiendo la nomenclatura de la Estrategia de Seguridad Nacional aprobada por el Gobierno el 31 de mayo de 2013 (12), podría llamarse Estrategia de Ciberseguridad Nacional. Esto es un hito de la mayor importancia porque será una clara indicación a toda la nación de que es algo muy importante y contribuirá, de manera decisiva, a que el resto de las administraciones tome el mismo camino.

Precisamente el tercer objetivo de la mencionada Estrategia de Seguridad Nacional es sobre seguridad informática y consiste en «garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los *ciberataques*». Dentro de este objetivo, el Gobierno demuestra su conocimiento de la necesidad de una conciencia nacional de *ciberseguridad* mediante la línea de acción estratégica número 5, que reza: «Implantación de una cultura de *ciberseguridad* sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento».

Por tanto, ya tenemos una base de partida: el Gobierno de España está concienciado e impulsa la concienciación y todo parece indicar que es una política de Estado.

Pero no es suficiente que el Gobierno esté concienciado, es necesario que todos los altos cargos recogidos en la Ley 5/2006, de 10 de abril, *de regulación de los conflictos de intereses de los miembros del Gobierno y de los altos cargos de la Administración General del Estado* (AGE), y los cargos directamente subordinados a los mismos estén concienciados para que sea factible hacer campañas de concienciación en la AGE susceptibles de tener éxito.

El resto de la administraciones debe alinearse con la estrategia de *ciberseguridad* que sancione y publique el Gobierno. Esta alineación es muy importante por dos razones:

- Demostraría a los *ciberatacantes* que todas las administraciones se toman la *ciberseguridad* en serio y que están de acuerdo.
- Sería una contribución importantísima y muy necesaria para la concienciación de la sociedad.

El siguiente hito es que los directivos de las empresas sean conscientes de la necesidad de que sus empresas sean *ciberseguras*. Una buena forma de potenciar esto es que la Administración exija haber superado inspecciones de *ciberseguridad* para poder trabajar con las administraciones, fundamentalmente como proveedores. Algo que ya se hace porque las empresas que trabajan en contratos con las administraciones que incluyen el manejo de información o materiales clasificadas deben tener certificados de seguridad que se obtienen tras superar ciertas inspecciones, tanto la empresa en general como los trabajadores que van tener acceso a dicha información o material. Conseguir que todas las empresas que trabajen como proveedores de las administraciones públicas tengan una certificación de *ciberseguridad* no debería ser un obstáculo de primera magnitud.

Para las empresas que se dedican a producir *software* y sistemas informáticos, a comercializar servicios telemáticos, incluida la venta por Internet, o son proveedores de servicios de Internet, esta concienciación de seguridad debe ir mucho más lejos. Tiene una cuota de responsabilidad en la seguridad de los productos y servicios que comercializan y deben extremar las medidas de seguridad.

Hoy en día la comercialización oportuna, antes que la competencia, de cualquier producto o servicio es fundamental para adquirir cuota de mercado. También es importante poder competir en precio; pero no menos importante es poder competir en calidad y seguridad. Con calidad y seguridad los fabricantes y proveedores de servicios, si además son competitivos en precio, pueden asegurar la fidelización de los clientes.

Hemos visto que es necesario desarrollar e implantar una estrategia de *ciberseguridad* en los cuatro niveles de las administraciones, de las instituciones, de las empresas –tanto públicas como privadas– y de las organizaciones y que el Gobierno de la nación empezó a dar los primeros pasos.

Una estrategia de *ciberseguridad* a nivel organización debe cumplir ciertos requisitos (13); los más comúnmente aceptados son los siguientes:

- Debe poderse implantar.
- Debe entenderse.
- Debe hacerse cumplir.
- Debe definir responsabilidades.
- Debe permitir que siga realizándose el trabajo normal.

- Debe ser exhaustiva.
- Debe incluir mecanismos de respuesta.
- Debe tener mecanismos de actualización.
- Debe cumplir la legislación.

Es evidente que la estrategia de *ciberseguridad* debe contemplar los principios de defensa en profundidad, de diversidad de defensa y para todos los usuarios el uso del privilegio mínimo. Los dos primeros principios son comunes, y muy conocidos en el mundo de la milicia, a cualquier noción de defensa. En efecto, a lo largo de la historia de la humanidad, una defensa mínimamente creíble ha tenido varias líneas de defensa separadas en el espacio, esto es la defensa en profundidad; además, siempre se ha procurado que las defensas fueran de tipos diversos en cada línea y dentro de cada línea, esto es la diversidad de defensa.

El principio del uso de los mínimos privilegios es también conocido en el ámbito militar y es anterior al uso de la informática; es perfectamente equiparable al principio de necesidad de saber a la hora de otorgar privilegios de acceso a la información clasificada.

En el campo de la informática es perfectamente factible que las administraciones, las empresas, instituciones y organizaciones protejan sus sistemas cibernéticos con diversas líneas de defensa y con diversas tecnologías. Los ISP también pueden proporcionar defensa en profundidad a sus usuarios y los usuarios colaborar en dicha defensa de manera activa siguiendo los procedimientos que le debe explicar su ISP. Esta colaboración es también en beneficio del propio usuario porque no solo podrá tener más probabilidades de seguir teniendo acceso al ciberespacio, sino que también protegerá su privacidad y su patrimonio material e inmaterial, el honor y la imagen.

En cada nivel organizativo de las administraciones, empresas e instituciones debe haber una estrategia de seguridad derivada de la del nivel inmediato superior que, basada en los mismos principios, deberá contemplar ciertos aspectos específicos de dicho nivel organizativo; este desmenuzamiento no tiene por qué seguir hasta el nivel más bajo de la organización, de hecho sería poco practicable hacerlo.

Un aspecto a menudo olvidado en las estrategias de seguridad son los equipos rojos, del inglés *red team*. Estos equipos tienen como misión permanente atacar el sistema para descubrir y evaluar las debilidades y proponer medidas para evitar las mismas; dependiendo del tamaño de la organización, el equipo rojo puede ser o no interno a ella. En el caso de las administraciones y empresas públicas, lo recomendable es que los equipos rojos sean internos. Los equipos rojos de la Administración central, deben, así mismo, ser los encargados de ejercer su función en los sistemas informáticos de las infraestructuras críticas.

Derivada de la política de *ciberseguridad*, debe establecerse una estrategia de *ciberseguridad* e iniciar campañas de concienciación.

Es necesario construir, de manera formal y efectiva, una estructura de *ciberseguridad* en la que se establezcan los responsables de *ciberseguridad* y las vías y formatos de notificación, y se insista en la protección de la identidad de los notificantes aparte de lo especificado en la LOPD, la periodicidad y contenido mínimo de los boletines de seguridad cibernética, así como su distribución. La creación de esta infraestructura reúne aspectos tanto formales como físicos, lógicos y legales que sin el impulso decidido de las autoridades en todos los niveles de las administraciones y de la dirección, asimismo en todos los niveles, en las instituciones y empresas, tanto públicas como privadas, no puede darse de manera efectiva. Sin esta infraestructura, las políticas de *ciberseguridad,* las campañas de concienciación y las estrategias valdrán de muy poco pues los usuarios no recibirán información y no serán conscientes de las amenazas ni podrán notificar incidentes por lo que un ataque de denegación de servicio distribuido (DDoS), por ejemplo, será más fácil de hacer, el número de ordenadores esclavos será mayor y su efectividad también.

Ya se ha escrito que uno de los factores de calidad del *software* es la seguridad; pues bien, la seguridad unida a la fiabilidad y robustez propicia que los ataques sean menos efectivos y más difíciles de ejecutar.

Otro requisito importante para poder poner en marcha campañas de concienciación efectivas, es la certificación del *software* de acuerdo con los factores de calidad en general y en particular los tres reseñados.

Al igual que se certifica cualquier electrodoméstico en relación con la eficiencia energética y se les asigna un código de eficiencia energética, los certificados de seguridad del *software* podrían tener un código para que los usuarios sepan y sean conscientes del nivel de seguridad del *software* que compran; aunque hay que insistir que por muy seguro que sea un sistema, nunca será inmune a los ataques y siempre habrá alguno que tenga éxito. Esta certificación siempre podrá utilizarse como argumento de ventas.

El principal problema para la certificación del *software*, desde un punto de vista técnico, son las métricas de los factores de calidad; pero siempre será factible establecer unos mínimos para los factores de seguridad, fiabilidad y robustez.

La certificación del *software* debería ser un requisito indispensable como lo es en los vehículos a motor. Esto necesita de una infraestructura tal y como se ha hecho con la industria del automóvil. En este caso hay todo un edificio legislativo y una autoridad de homologación. En el mundo de la aeronáutica, el término es certificación y se certifican tanto las aeronaves como sus componentes y el personal que opera las mismas, las mantiene

o ejerce el control, y se ha montado una infraestructura formal, legal, organizativa y física para ello. Del mismo modo, teniendo en cuenta que el *software* y el *firmware* pueden ser tan críticos para la seguridad nacional y el bienestar de los ciudadanos, debería implantarse algo análogo.

Para que la certificación del *software* sea efectiva debe existir una autoridad nacional de certificación tanto a nivel nacional como dentro de la Unión Europea. En España el Instituto Nacional de Tecnologías de la Comunicación (INTECO) y el Centro Criptológico Nacional (CCN) son los organismos encargados de la certificación de productos de las tecnologías de la información (IT) y son los representantes españoles en los comités de redacción de los «Common Criteria»[6]. La certificación del *software* pasa por exigir unas pruebas y comprobaciones del código en cuanto a su seguridad, para lo cual debe ponerse a disposición de la autoridad de certificación el código fuente para comprobar que hay manejadores de excepciones y que se controlan, entre otras muchas cosas, las entradas y el desbordamiento tanto de memoria como de las pilas y colas. Por supuesto, debe someterse a las pruebas pertinentes, que deberían ser lo más exhaustivas posibles. Los CC y CEM son, hoy por hoy, los documentos de referencia para estas pruebas En la fase final de estas pruebas debería participar un *red team* haciendo ataques reales al *software* que se quiere certificar.

Los CC y CEM actuales, aunque prolijos y necesarios, parecen no ser suficientes pues es frecuente que el *software* certificado de acuerdo con ellos siga presentando vulnerabilidades. De hecho, el CEM recoge en su introducción que no da respuestas a todas las cuestiones relativas a la evaluación de la seguridad de las IT.

La ventaja que tiene el *software* frente al *hardware* es que todas las copias que se vendan o distribuyan tendrán la misma calidad; en el *software*, al contrario que con el *hardware*, solo se diseña y fabrica una vez, con el *hardware* se diseña una vez y se fabrican múltiples unidades. Las evoluciones siguen en ambos casos las mismas pautas descritas. El hecho de que, en el caso del *hardware*, se fabrique unidad a unidad aunque sea fabricación en cadena implica que debe haber un control de calidad de fabricación para las unidades fabricadas, además del control de calidad del diseño. En el caso del *software*, el control de calidad debe ejecutarse

[6] Los *Common Criteria for Information Technology Security Evaluation* (15) (CC) son procedimientos y criterios de evaluación de la seguridad de productos IT que pueden ser implementados en *hardware, firmware* y *software.* Están desarrollados de forma colaborativa por agencias de los Gobiernos de Alemania, Australia, Canadá, España, Estados Unidos, Francia, Japón, Nueva Zelanda, Países Bajos y Reino Unido. Además, está el *Common Methodology for Information Technology Security Evaluation* (16) (CEM), que es un documento adicional y que define las acciones mínimas que debe ejecutar un evaluador para llevar a cabo una evaluación siguiendo los criterios y las evidencias definidas en los CC.

de manera exhaustiva durante todas las etapas del proceso de diseño y construcción hasta llegar al producto final porque luego no hay que invertir dinero, de manera significativa, en el proceso de copia de ese producto, más allá del control de las máquinas copiadoras y del soporte de copia.

Una buena medida adicional para potenciar la certificación del *software* es obligar a las administraciones, instituciones, empresas públicas y proveedores de todas ellas a usar solo *software* certificado. Si, además, la infraestructura de *ciberseguridad* está implantada y funcionando, será más probable descubrir y desbaratar ataques cibernéticos antes de que hayan conseguido todos los efectos deseados.

La unión de usar *software* certificado y de tener y usar una buena infraestructura de *ciberseguridad* elevaría la resiliencia nacional ante ataques informáticos. Varios países europeos y la Comisión Europea, por ejemplo, en sus estrategias de *ciberseguridad,* dan una gran importancia a la resiliencia y tienen razón. En efecto, es imposible evitar los ataques y tampoco es asumible pensar que vamos a evitar que ningún ataque consiga éxito, pero sí podemos prepararnos para que los daños de los ataques sean los más pequeños posibles y para que nos podamos recuperar lo más rápidamente posible.

Es de sobra conocido que una de las causas, posiblemente la principal, de todas las crisis del *software* ha sido la pobre calidad del mismo y se sigue investigando en herramientas de aseguramiento de la calidad. Posiblemente, quien fuese capaz de desarrollar e implementar algoritmos de prueba del *software* y del *firmware* tanto a nivel unidad como a nivel de integración, validación y sistema que asegurasen que el *software* tiene un determinado nivel (alto) de calidad ganaría, o al menos sería firme candidato, al premio Turing[7].

La unión de *software* seguro, *software* de protección de las estaciones de trabajo, sistemas de protección de las redes, cifrado de la información transmitida y uso de sistemas de ficheros seguros es necesaria pero no es suficiente para que un sistema informático tenga un mínimo de seguridad.

[7] El premio Turing, considerado por muchos como el Nobel de la Informática, premia a quienes hayan contribuido de manera trascendental al campo de las ciencias computacionales. Fue instaurado en 1966 en honor de Alan Mathison Turing, matemático y científico británico que hizo avances fundamentales en la informática, en el campo de los algoritmos, arquitectura de ordenadores, inteligencia artificial, formalización de la informática, entre otros; es el diseñador del modelo formal de computador conocido como máquina de Turing. Fue uno de los artífices del descifrado de la máquina alemana Enigma, en particular la Enigma naval, en la II Guerra Mundial (SGM) lo cual contribuyó de manera decisiva a la victoria de los aliados. Su ordenador electromecánico, concebido junto con Gordon Welchman y conocido como «La Bomba», creado durante la SGM, puede ser visitado en Bletchley Park, Bletchley, Milton Keynes, Buckinghamshire, Reino Unido.

En efecto, falta el eslabón principal de todo el sistema: las personas. Es necesario formar a las personas en seguridad informática o *ciberseguridad.* No todo el mundo puede ni debe tener la misma formación. Los usuarios deben estar formados en buenas prácticas, algo así como *ciberurbanidad* o *cibereducación*.

Esta *ciberurbanidad* o buenas prácticas de seguridad informática debe ser algo que se repita con frecuencia hasta que la sociedad lo tenga interiorizado como tiene interiorizadas normas de buena educación o buenas maneras.

Algunas de estas buenas prácticas podrían ser las siguientes:

1. Las contraseñas: cómo deben ser las contraseñas, cuándo hay que cambiarlas, cómo protegerlas.
2. Protección contra virus. El antivirus: su importancia, razones para tenerlo activado y actualizado, necesidad de los análisis periódicos, tipos de análisis, etc.
3. Beneficios para el usuario y la organización del cumplimiento de las normas de seguridad y las implicaciones de su incumplimiento para el usuario y para la organización.
4. El correo electrónico: buenas prácticas en el uso del correo electrónico, en el envío de adjuntos, qué hacer si se recibe correo electrónico de direcciones que no son realmente conocidas aunque nos sean familiares, qué hacer con los adjuntos.
5. Qué está permitido y qué prohibido en la organización respecto del uso de Internet.
6. Copia de seguridad de los datos: aunque la organización disponga de medios para hacer copias de seguridad, hay que concienciar a los usuarios de la importancia de hacer copia local de los datos que utiliza en el día a día.
7. En caso de incidente: qué hacer, con quién contactar.
8. Medidas de prevención ante la ingeniería social: mostrar y analizar ejemplos de correos electrónicos solicitando claves, adjuntando documentos para reuniones, etc.
9. Seguridad en el empleo de los dispositivos USB: explicar la importancia que estos dispositivos tienen en las organizaciones y casos como el Stuxnet.
10. Normas para el envío de información sensible o clasificada: mostrar claramente qué medidas de seguridad deben adoptarse para el envío de dicha información.
11. Normas básicas de seguridad de los equipos: uso de protectores de pantalla, el bloqueo del PC, etc.

12. Instalación de *software* por parte del usuario: el *software* instalado por el usuario en los PC puede poner en riesgo la seguridad de nuestras organizaciones; el *software* debe ser instalado por un administrador.
13. Normas básicas de seguridad en los viajes y, en general, fuera del trabajo: tener siempre vigilado el equipo portátil, cuidado con las conversaciones, etc.

Cada una de las buenas prácticas reseñadas, que no agotan en absoluto el catálogo de buenas prácticas, puede dar lugar a, al menos, un panfleto y conferencia.

La *ciberurbanidad* debe ser una extensión de las buenas maneras, de la buena educación e incluir normas básicas de protección de la información. Debe inculcarse a todos los niveles y en todos los ambientes. Las buenas maneras se inculcan desde la familia y la escuela, también se inculca la seguridad vial en las escuelas, por tanto las buenas prácticas en *ciberseguridad* deben ser parte del currículo de los colegios, institutos, universidades y academias militares. No todas las familias pueden en la actualidad colaborar activamente con las instituciones de enseñanza en la educación básica de *ciberseguridad*, pero estas instituciones sí pueden y deberían hacerlo. No solo porque es un problema de seguridad nacional, es que es también un problema de seguridad personal.

En el caso de la enseñanza en el ramo de la informática y telemática, desde la formación profesional a la universitaria, no se pueden contentar con la *ciberurbanidad.* Los profesionales que se forman en estas ramas de la ingeniería, sea cual sea su nivel, tienen una responsabilidad en toda la estructura nacional. Serán diseñadores, arquitectos, programadores, administradores o mantenedores de sistemas informáticos y son una parte esencial en la seguridad de esos sistemas.

Afortunadamente, las universidades en las nuevas titulaciones de grado suelen incluir alguna asignatura de seguridad informática, aunque no siempre es obligatoria. Siendo la seguridad informática vital para que podamos tener una cierta seguridad de que podemos seguir manteniendo nuestra forma de vida, parece lógico que la seguridad informática fuese asignatura obligatoria en todos los planes de enseñanza, tanto de grado como de máster, de las facultades y escuelas de ingeniería informática. Aparte de que se establezcan titulaciones oficiales de máster en seguridad informática.

El caso de la formación profesional en informática es distinto; de los planes consultados para el curso 2012-2013, solo el de grado medio y uno de los tres de grado superior incluyen una asignatura de seguridad.

Para poder hacer *software* seguro, que es la plataforma donde se asientan los principios de la conciencia de *ciberseguridad*, es necesario que los

ingenieros y programadores estén concienciados y tengan la posibilidad de hacerlo. En muchos casos es difícil porque sienten la presión de las prisas para sacar un producto al mercado y poner operativo un sistema o una ampliación del mismo. La creación de *software* seguro requiere más tiempo, igual que la creación de un vehículo seguro, a lo largo de todo el proceso de la ingeniería del *software*. Las pruebas serán más largas y es más probable que se tenga que modificar la aplicación.

Pero hay que pensar que esa aplicación puede ser o estar en un cortafuegos[8], por ejemplo, si el *software* no es seguro el propio cortafuegos tiene vulnerabilidades. Es como si los frenos del coche no frenasen cuando hay que frenar a fondo porque el ingeniero que los diseñó no pensó que era importante y el mecánico que los construyó tampoco creyó que era importante.

Todo el *software* nuevo y las ampliaciones o mejoras del existente deben diseñarse y construirse pensando que los factores de calidad del *software* son todos igual de importantes y tan importantes como hacerlos pronto. En este sentido, no ayuda el que los proyectos de *software* no necesiten ser visados por un ingeniero como lo son los proyectos en el resto de las ingenierías.

Los responsables de las empresas de producción y de mantenimiento de *software* y de sistemas informáticos deben considerar la seguridad de sus productos y servicios como un atributo de la mayor importancia de cara a conseguir mejores resultados comerciales.

Participación de las instituciones de la sociedad civil

El paradigma de la *ciberguerra* implica a todos y cada uno de los ciudadanos en la defensa pasiva. El gran problema es que la gran mayoría de esos ciudadanos no tiene conciencia de *ciberseguridad* ni tiene los conocimientos necesarios para participar porque no le han enseñado un mínimo de buenas prácticas de protección de los sistemas informáticos que usan. En demasiados casos, los directivos de las empresas, instituciones, grupos, asociaciones, etc. no tienen tampoco conciencia de seguridad ni creen que sus empresas u organizaciones vayan a ser objeto de ataque o parte de un ataque a terceros por lo que el coste de implementar medidas de seguridad más allá de las básicas de exigir nombre de usuario y clave para entrar en el sistema informático de su organización es, para ellos, inasumible.

[8] El cortafuegos, en inglés *firewall,* es un dispositivo implementado solo como *software* embebido dentro del sistema informático, normalmente estaciones de trabajo, o implementado como un dispositivo externo para proteger una red y en este caso consta de *hardware* y *software*.

Es imprescindible la participación de las instituciones de la sociedad civil, de las empresas, de los ISP, universidades, institutos, escuelas. Estamos en el paradigma de la guerra total y los ciudadanos, lo quieran o no, están todos involucrados. Pero no solo la sociedad civil; los cuatro niveles de la administración deben participar por la misma razón anterior.

El Spanish Cyber Security Institute (SCSI), en su informe *La ciberseguridad nacional, un compromiso de todos* (14), deja muy claro que el estado de concienciación en *ciberseguridad* de la sociedad civil es muy bajo; que las campañas desarrolladas por el INTECO, el CCN y el propio SCSI «de momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil», y enumera una serie de causas que divide en cuatro grupos: «organizacionales, operacionales, jurídicas y políticas». De entre las causas enumeradas en el citado informe quiero resaltar las siguientes:

> *Escaso protagonismo de los actores privados en materia de ciberseguridad. La ciberseguridad nacional, hoy en día, es un sistema cerrado y exclusivo de los actores gubernamentales. En la actualidad, más del 80% de las infraestructuras críticas de nuestro país son propiedad, están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales). Por tanto, la aportación del sector privado al proceso de construcción de la ciberseguridad nacional resulta esencial.*
>
> *Ausencia de una política estatal en materia de ciberconcienciación y cibereducación. Muchos países de nuestro entorno están desarrollando ambiciosas políticas en materia de ciberconcienciación y ciberseguridad como eje fundamental para la creación de una cultura de ciberseguridad. Estas políticas han sido desarrolladas e impulsadas, en primera instancia, por el sector privado y, posteriormente, han recibido un fuerte apoyo gubernamental.*
>
> *En este caso, cabe destacar una doble función, por un lado, concienciar y educar al conjunto de la ciudadanía de los riesgos del ciberespacio y, por otro, identificar futuros talentos en el campo de la ciberseguridad dentro de la comunidad escolar y universitaria.*
>
> *En España, INTECO y el CCN disponen de programas de ciberconcienciación y ciberseguridad. Desde el sector privado, organismos como el ISMS Forum Spain han lanzado su propia campaña de ciberconcienciación bajo la denominación protegetuinformacion.com. De momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil.*
>
> *Ausencia de políticas específicas para el I+D+i nacional en materia de ciberseguridad. No existen políticas, programas o iniciativas para el I+D+i de ámbito nacional que promuevan y faciliten actividades en materia de ciberseguridad, lo que contrasta con el gran protagonismo que a nivel europeo el nuevo marco de trabajo del Horizonte 2020 (continuación del 7.º Programa Marco) otorga a la Ciberseguridad.*

En una conferencia en el IX Curso de Alta Gestión del Recurso Financiero de la Escuela de Altos Estudios de la Defensa (EALEDE), el profesor D. Juan Iranzo dijo que España debería invertir más en las IT para salir de la crisis. La inversión en I+D+i en seguridad cibernética es parte de esa inversión en las IT y nos reportaría doble beneficio: más seguridad y la posibilidad de exportar algo que hoy tiene un alto valor añadido.

La participación de la Administración del Estado y de las empresas públicas podría considerarse asegurada si el poder político toma la decisión. Pero es necesario el compromiso de todos los dirigentes para que se puedan hacer campañas de concienciación. Es cierto que los sistemas informáticos de la Administración del Estado tienen un cierto nivel de seguridad de la información, adecuado al nivel de confidencialidad de la información que manejan, y que suele estar certificado por la autoridad competente. El problema, como con todos los sistemas de información y comunicaciones, es que los usuarios no suelen estar bien concienciados y se convierten en el eslabón débil de todo el sistema.

La participación de las instituciones de la sociedad civil será más difícil de conseguir y solo se conseguirá mediante campañas de concienciación y es en estas campañas donde los grupos, asociaciones, fundaciones, universidades y centros educativos de todos los niveles tienen un protagonismo de la mayor importancia.

Ya se ha hablado de la participación de las instituciones de enseñanza que se dedican a la enseñanza oficial o reglada. Esto no agota en absoluto la participación de la sociedad civil, aunque la participación de estas instituciones es de vital importancia pero sus frutos se obtienen siempre a medio y largo plazo. Es preciso involucrar al resto de instituciones de la sociedad civil para que se puedan obtener frutos a corto plazo.

Hay muchos grupos, fundaciones y organizaciones que aglutinan a muchísimos ciudadanos que, por la razón que sea, no están en el circuito de la enseñanza oficial como alumnos ni como enseñantes. Estos grupos y organizaciones se dedican a multitud de actividades, incluida la enseñanza no reglada, y pueden, o quizás habría que decir deberían, participar activamente en la promoción de la *ciberurbanidad.* Entre estos grupos y organizaciones habría que citar, sin ánimo de ser exhaustivos, a asociaciones de vecinos, academias de enseñanza –independientemente de la materia que impartan y del cliente al que orientan su oferta educativa–, asociaciones o clubes deportivos, sociales y culturales, etc. Todos estos grupos y asociaciones pueden colaborar de manera muy activa en la promoción de la cultura de *ciberseguridad*, empezando por la *ciberurbanidad*, y de los principios de la cultura nacional de *ciberseguridad*. La forma habitual sería mediante talleres y conferencias impartidos por expertos cercanos a dichos grupos y, siempre que sea factible, por expertos de

referencia por su trabajo en la Administración o en empresas en puestos dedicados a la *ciberseguridad*.

Las fundaciones, tomadas en su conjunto sin distinguir aquellas que tienen como fin la promoción de la cultura de seguridad de las que tienen otros fines, pueden tener un papel importantísimo en la promoción de la conciencia de *ciberseguridad* y de la *ciberurbanidad* mediante la celebración de congresos, seminarios, etc. dirigidos a toda clase de público en los que se expliquen los principios reseñados en este trabajo y se expongan las normas de *ciberurbanidad.*

Es muy importante que se hagan campañas a todos los niveles para concienciar a todos los ciudadanos de la importancia de la notificación de errores e incidencias. Cuantos más usuarios comenten a los responsables de seguridad informática los errores cometidos y las incidencias sufridas mejores boletines información de *ciberseguridad* podrán hacer dichos responsables y, sin ninguna duda, se contribuirá a que el ciberespacio sea un poco más seguro.

Además de los grupos y asociaciones ya mencionados, hay que estudiar el papel que los grupos formadores de opinión, como puede ser por ejemplo la prensa en cualquiera de sus formatos, pueden desempeñar.

Los medios de difusión, tanto los especializados como los no especializados en *ciberseguridad,* pueden contribuir de manera decisiva en la promoción de la cultura de *ciberseguridad* y en la *cibereducación*. No es necesario que estos medios desarrollen decálogos de *cibereducación* ni de *ciberseguridad,* simplemente con que se hagan eco de la labor de organismos como el ya mencionado INTECO y de la existencia de guías y herramientas, todas gratuitas, sobre diversos aspectos de la *ciberseguridad* para ciudadanos y empresas ya estarían haciendo una gran labor.

Cualquier fundación o asociación puede siempre contactar con el INTECO y con empresas dedicadas a la seguridad informática para que expertos vayan a dar conferencias y consejos sobre *ciberseguridad* y *ciberurbanidad.*

La colaboración de las empresas, incluidos los ISP, con organismos como el reseñado INTECO en la creación de una infraestructura propia de *ciberseguridad* mediante la cual sus usuarios puedan, de forma fácil y anónima, contactar con los responsables de *ciberseguridad* para el proceso de notificación de incidencias y errores y estos responsables puedan difundir a sus usuarios los boletines de *ciberseguridad* y los decálogos de *cibereducación* facilitaría enormemente la creación, difusión y promoción de una cultura y conciencia nacional de *ciberseguridad*.

Estas estructuras de *ciberseguridad* son esenciales para que los ciudadanos puedan colaborar en mejorar la seguridad del ciberespacio. Esta

mejora de la seguridad del ciberespacio implica mejoras en la propia seguridad y una menor probabilidad de sufrir daños catastróficos tanto en lo personal como en lo colectivo.

En la actualidad, los ciudadanos y muchas empresas tienen intereses que defender frente al *cibercrimen*, fundamentalmente estafas, fraudes, acoso, robo de información, incluida información comprometedora, y similares, pero hay muy poco interés en la defensa colectiva de los intereses de todos. Además, como se ha repetido anteriormente, hay poca conciencia de las amenazas que nos rodean como colectividad en el ciberespacio y menos aún de que podemos ser usados por esas amenazas para encubrirse. Los medios de comunicación pueden colaborar para que los ciudadanos conozcan que pueden ser parte, sin saberlo, de un ataque que tenga efectos catastróficos sobre la colectividad y ellos sufrirán dichos efectos catastróficos. El conocimiento debe ser positivo, es decir, no debe dar solo la información de que podemos ser utilizados, sin que lo sepamos ni colaboremos, como vector en un ataque a infraestructuras críticas; también debe divulgar las normas básicas de *cibereducación* que harán más difícil que nos usen como vectores en un ataque cibernético.

Pero no solo se trata de evitar que nos usen como vectores; esas mismas medidas de *ciberseguridad* nos harán también un poco más seguros frente al *cibercrimen* y nos permitirán seguir haciendo uso del ciberespacio. Si fuesemos capaces de evitar o parar la difusión de *malware* de creación de *botnets*[9], obtendríamos beneficios porque aunque un ataque distribuido de denegación de servicio no nos afecte directamente ni a servicios que usamos, siempre reducirá el ancho de banda de la red y, por tanto, nuestra capacidad de acceder a servicios que, en teoría, no están afectados.

La cultura y la conciencia de *ciberseguridad* nos protegen no solo en caso de una *ciberguerra* o de ataques contra infraestructuras críticas o contra las Administraciones Públicas. Normalmente, un tipo de ataque llamado *advanced persistent threat* (APT), que actualmente son considerados los más elaborados y peligrosos, no tendrá como objetivo un ciudadano cualquiera pero el *cibercrimen* sí puede tener como objetivo a cualquier usuario del ciberespacio. Sin embargo, las normas básicas de *ciberseguridad*, tan mencionadas en este capítulo, también ayudan a todos los usuarios del ciberespacio a protegerse contra el *cibercrimen*.

Los grupos, asociaciones y fundaciones que forman las instituciones de la sociedad civil tienen la capacidad de movilizar las conciencias de millones de ciudadanos que usan el ciberespacio, de manera profesional o privada, y que trabajan usando las tecnologías de la información y de las

[9] Redes de ordenadores infectados y esclavizados por un controlador que los puede usar entre otros tipos de ataques en ataques distribuidos de denegación de servicio (DDoS).

comunicaciones (TIC). Todas estas instituciones tienen un rol de primerísima magnitud en la formación de la conciencia de *ciberseguridad,* que se convierte en nacional cuando la mayoría de los ciudadanos la tiene.

Es de sobra conocido y muy estudiado que en cualquier sistema informático la parte más débil en cuanto a seguridad terminan siendo las personas. En efecto, muchos de los ataques más importantes sufridos por empresas, administraciones y ciudadanos particulares han comenzado por un ataque de ingeniería social. Contra estos ataques pueden poco la tecnologías de *hardware* y *software*, aunque algo se avanza también en dificultar el éxito de los ataques de ingeniería social; sin embargo, las buenas prácticas en el uso de los sistemas informáticos, la *ciberurbanidad* o *cibereducación*, sí que pueden disminuir de manera ostensible el éxito de dichos ataques.

Empezando ahora la labor de *cibereducación* en las escuelas, institutos y universidades, en unos años las personas de menos de 35 tendrán interiorizada esa educación cibernética. Pero serán solo una parte de la sociedad. Para *cibereducar* –y esto no tiene nada que ver con adoctrinamiento como tampoco lo tiene la educación vial, por citar algún ejemplo– al resto de la sociedad deben ser las instituciones de la sociedad civil las que tomen el testigo.

Hay que tener presente que entre las instituciones de la sociedad civil y los medios de comunicación se llega a la práctica totalidad de los ciudadanos, por ello es tan importante su papel.

Ciertamente, se debe evitar la sobreeducación porque puede producir la reacción contraria y que un buen número de ciudadanos, aun conociendo las buenas prácticas de la *ciberurbanidad,* se opongan al uso de esa *cibereducación*.

La buenas prácticas en la seguridad informática y de la información son muy conocidas y se han publicado en muchos boletines de *ciberseguridad*; el problema es que la mayoría de esos boletines no han tenido el eco suficiente porque el usuario los percibía como emanados de la autoridad. Es demasiado frecuente ver que los usuarios tienen escrito su nombre de usuario y su clave de acceso al sistema informático en un papel bajo el teclado o en una libreta en un cajón de la mesa o encima de la mesa. Sigue siendo posible convencer, con cierta facilidad, a personas para que nos den su nombre de usuario y clave de acceso. Todas estas malas prácticas se podrían evitar con la ayuda de las instituciones de la sociedad civil.

Para que las instituciones de la sociedad civil participen en la promoción de la conciencia de seguridad y de sus principios, es necesario que sus responsables estén concienciados y tengan asumidos los principios de la conciencia de *ciberseguridad* y de la base sobre la que se asientan. La concienciación de estos responsables debe ser objetivo de las cam-

pañas de concienciación organizadas por las autoridades. Sin ellos será muy difícil que sus instituciones hagan algo en pro de la conciencia de *ciberseguridad*.

Por supuesto, será imposible llegar a todas las instituciones de la sociedad civil; pero se podrá llegar a muchas tanto en el entorno urbano como el rural y estas instituciones serán las que tomen el relevo por su proximidad al ciudadano.

Conclusiones

El paradigma de la *ciberguerra* es una mezcla de los paradigmas de la guerra total y de la guerra asimétrica.

Desde finales de la década de los 90, ya se propugna el uso de la informática como arma para luchar contra enemigos más poderosos en una guerra asimétrica en la que la parte débil no se atendrá a las leyes y usos de la guerra.

Los efectos de la *ciberguerra* alcanzan a todos los ciudadanos independientemente de su estatus de conexión y uso del ciberespacio.

Todos los ciudadanos que usan el ciberespacio son partícipes de la *ciberguerra*.

Como las amenazas son difíciles de percibir por su propia naturaleza, los ciudadanos tienen dificultades para sentir la necesidad de conciencia de seguridad informática. Sí que pueden percibir algo más la amenaza que supone el *cibercrimen* por su incidencia en su imagen y en su propia economía.

Volar es una actividad intrínsecamente peligrosa pero que, debido a la conciencia y cultura de seguridad desarrollada en torno a la misma y entre todos los que trabajan de cualquier manera en la misma, se ha vuelto una de las más seguras. De esta cultura y conciencian participan los diseñadores, constructores, operadores, tripulaciones, personal de mantenimiento de las aeronaves y de los sistemas de control en tierra y el personal que utiliza estos últimos.

La conciencia de seguridad de vuelo tiene unos principios que podrían extrapolarse, no copiarse, a la conciencia de *ciberseguridad.*

Los principios de la conciencia nacional de *ciberseguridad* son:

- Conocimiento de las amenazas y de los riesgos y asumirlos.
- Notificación por los usuarios de los errores cometidos e incidencias sufridas.
- Información por los responsables de seguridad de los sistemas informáticos de los proveedores de servicios de Internet (ISP), de las instituciones y empresas a los usuarios, miembros, empleados y clientes.

– Formación de todos, cada uno en el nivel que corresponda, en *ciberseguridad*.
– Adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio.

Es fundamental conocer las amenazas y los riesgos y asumirlos en el sentido de aceptarlos y enfrentarlos, nunca en el sentido de conformidad y pasividad ante los mismos.

La notificación de los incidentes y de los propios errores es uno de los principios más difíciles de conseguir, pero la consecución proporcionará a los responsables de seguridad de cada organización, incluidos los ISP, una información muy valiosa para poder mejorar la *ciberseguridad* de todos.

Es necesario que el proceso de estas notificaciones garantice el anonimato y el respeto de la LOPD. Además, debe ser extremadamente sencillo para cualquier usuario, independientemente de su nivel de formación, poder rellenar la parte manual de los formularios.

La información sobre *ciberseguridad* y buenas prácticas que deben proporcionar los responsables de *ciberseguridad* a sus usuarios debe ser sencilla y periódica y no debe permitir que nadie pueda identificar a quienes han notificado incidentes y errores cometidos.

La formación es fundamental y hay que diferenciar la formación de los usuarios de la de aquellos que diseñan, construyen, mantienen y administran los sistemas informáticos.

Dado que la forma de las amenazas cambia de manera constante y a velocidad vertiginosa, es necesario que los usuarios, las instituciones y las empresas sepan adaptarse a los cambios que ocurren en el ciberespacio.

Lo que soporta estos principios es el *software* seguro. Todos los ataques explotan vulnerabilidades del *software*, por lo que una mejora en la seguridad del mismo redundará en una disminución del éxito de los ataques, que serán no solo producto de la *ciberguerra* sino también y de forma más frecuente para la mayoría de los usuarios del *cibercrimen*.

La primera y más fundamental condición para que estos principios puedan ser promocionados entre todos los ciudadanos es que las autoridades en los cuatro niveles de la Administración estén concienciadas de la necesidad de la seguridad cibernética. Por ello, la certificación del *software* de acuerdo con los CC y CEM debería exigirse para todo producto IT de las Administraciones Públicas y los de aquellas empresas y particulares que trabajan con o para las mismas.

Hay que seguir investigando para mejorar los CC y CEM.

El estado actual de conciencia nacional de *ciberseguridad* es, cuando menos, manifiestamente mejorable. Lo cual no es de extrañar dado que el grado

de compromiso de la sociedad española con la seguridad y defensa dista mucho de ser óptimo y la *ciberseguridad* es un concepto que ha empezado a llegar al público no especializado hace relativamente poco tiempo.

El compromiso de altos cargos de la AGE y del resto de las Administraciones Públicas, de los cargos directamente subordinados a ellos y de sus administraciones es fundamental para llegar a la sociedad civil.

Las escuelas, institutos y universidades juegan un papel primordial en la creación de conciencia de *ciberseguridad*, que será nacional cuando alcance a la mayor parte de la población. Para conseguir la participación de los docentes es necesario primero concienciarlos y formarlos en *ciberseguridad*. Los resultados de la actividad de las instituciones de enseñanza se verán a medio y largo plazo.

En de gran importancia para España que se potencie la I+D+i en *ciberseguridad* y en general en las IT, con ello se conseguirá un doble beneficio: aumento de la *ciberseguridad* y mejora de la economía.

Para obtener resultados a corto plazo, es imprescindible que las instituciones de la sociedad civil y los medios de comunicación en todos sus formatos se involucren. Para ellos es necesario que los dirigentes de esas instituciones se conciencien de la necesidad de la seguridad informática. En cuanto a los medios de comunicación, los dirigentes tienen un doble papel: concienciarse y concienciar al personal que trabaja en sus medios.

La conciencia de *ciberseguridad* es necesaria porque las personas forman parte del ciberespacio; de acuerdo con el paradigma de la *ciberguerra,* son parte de este tipo de guerra; las personas finalmente son el eslabón débil de los sistemas informáticos hasta el punto de que la mayor parte de los ataques informáticos, ya sean efectuados por organizaciones estatales o paraestatales o por criminales, empiezan por un ataque de ingeniería social.

La conciencia de *ciberseguridad* puede plasmarse en buenas prácticas informáticas o en algo más amplio que podría llamarse *ciberurbanidad* o *cibereducación* y que sería una extensión de las normas y usos de la buena educación al ciberespacio.

El papel de la sociedad civil es fundamental en la concienciación a corto plazo de todos los ciudadanos y complementa a la obtenida a medio y largo plazo mediante las instituciones de enseñanza.

Bibliografía

1. SCHMITT, Carl. *Der Begriff des Politischen («El concepto de lo político»).* Berlín: s. n., 1932.
2. CABRERIZO CALATRAVA, Antonio Jesús. *El conflicto asimétrico.* Universidad de Granada: I Congreso Nacional de Estudios de Seguridad, 2002.

3. LIANG, Qiao y XIANGSUI, Wang. *Unrestricted Warfare («Guerra sin restricciones»).* Beijing: PLA Literature and Arts Publishing House, febrero de 1999.
4. TZU, Sun. *El arte de la guerra.* 550-500 a. C.
5. LÓPEZ BLÁZQUEZ, Manuel, y otros. *La cultura de seguridad y defensa. Un proyecto en marcha.* Madrid: s. n., 2011. ISBN 978-84-9781-702-8.
6. Centro de Investigaciones Sociológicas. *Estudio n.º 2912. La defensa nacional y las Fuerzas Armadas (IX). Septiembre-octubre 2011.* 2011.
7. Ejército del Aire. Estado Mayor del Aire. División de Operaciones. *IG 10-9 Seguridad en vuelo.* 1988.
8. Aeropuertos Españoles y Navegación Aérea (AENA). *Libro blanco de la cultura de seguridad.* 2012.
9. CERRADA SOMOLINOS, José A., y otros. *Introducción a la ingeniería del software.* Madrid: Editorial universitaria Ramón Areces, 2007.
10. MEYER, Bertrand. *Object-Oriented Software Construction.* Hemel Hempstead, Hertfordshiere: Prentice Hall International (UK) Ltd., 1988.
11. PRESSMAN, Roger S. *Software Engineering: A practitioner's approach.* New York: McGraw-Hill, 1986.
12. Gobierno de España. *Estrategia de Seguridad Nacional.* Madrid: s. n., 2013.
13. DÍAZ, Gabriel, y otros. *Seguridad en las comunicaciones y en la información.* Madrid: Universidad Nacional de Educación a Distancia, 2004.
14. Spanish Cyber Security Institute. *La ciberseguridad nacional, un compromiso de todos.* Junio de 2012.
15. LOUDEN, Kenneth C. *Programing Languages: Principle and Practice. Second Edition.* Boston, Massachusets, EE. UU.: Course Technology, 2003.
16. Common Criteria for Information Technology Security Evaluation, versión 3.1. Julio de 2009. CCMB-2009-07-001.
17. Common Methodology for Information Technology Security Evaluation, versión 3.1. Julio de 2009. CCMB-2009-07-004.

Conciencia ciudadana de *ciberseguridad*

Por José Manuel Roldán Tudela

Capítulo segundo

1. Change vs. more of the same
2. Cyber security, stupid
3. Don't forget the economy

Cartel en un cuartel general electoral. Campaña presidencial en EE. UU. Año 2020

Introducción

En el capítulo anterior se han visto los dos significados del concepto de «conciencia de *ciberseguridad*». Por un lado, es necesario ser «conscientes» de su importancia, las dificultades y los problemas que plantea. Por otro, en tanto que «conciencia moral», hay que ser sensibles a las responsabilidades, individuales y colectivas, en el campo de la *ciberseguridad*, responsabilidades que son personales, ciudadanas, éticas y políticas. Estos dos aspectos deben estar presentes simultáneamente. En este capítulo se va a tratar la creación de una conciencia nacional de *ciberseguridad* en las personas consideradas individualmente; en definitiva, en los ciudadanos como usuarios de las diferentes tecnologías de la información y las telecomunicaciones (TIC).

La Estrategia de Seguridad Nacional (1), aprobada en mayo de 2013, describe en su tercer capítulo los riesgos y amenazas que afectan singular-

mente a la seguridad nacional e incluye entre ellos las amenazas informáticas después de los conflictos armados y el terrorismo. En su capítulo cuarto, señala como cuarta línea estratégica en el ámbito de actuación de la ciberseguridad:

> *Implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.*

La creación de una conciencia ciudadana de *ciberseguridad* es, pues, un elemento esencial de la estrategia nacional.

Las personas poseen una percepción de lo que es la «seguridad ciudadana», de su necesidad y de las implicaciones que una deficiente seguridad ciudadana puede tener para su vida diaria y el ejercicio de sus derechos. Ello viene dado por el conocimiento que poseen sobre las amenazas a esta seguridad, derivadas fundamentalmente de las actividades delictivas más comunes. Aun así, las autoridades se ven obligadas periódicamente a lanzar campañas de concienciación para sensibilizar a los ciudadanos sobre nuevas formas de delincuencia.

Hablando desde un punto de vista «macroscópico», una deficiente seguridad ciudadana no produce (mientras no rebase ciertos límites de degradación) graves efectos en la seguridad nacional, entendida en su más clásica acepción. Sin embargo, la concepción actual de seguridad nacional, que atiende a la preservación de un modo de vida y a la protección de las personas, obliga a modificar este punto de vista. Por otro lado, en la sociedad de la comunicación en la que vivimos, la alarma social y el estado de opinión pública subsiguiente harían muy difícil para las autoridades la pervivencia de una situación degradada de la seguridad ciudadana. De lo anterior se deduce que es necesario mantener la seguridad ciudadana y que la conciencia de seguridad de la población es importante para mantenerla. Por otra parte, esta conciencia requiere necesariamente del conocimiento de las amenazas a su seguridad por parte de los ciudadanos.

Llegados a este punto, es necesario reflexionar sobre cómo la rápida introducción del uso de las TIC y la aparición de un nuevo dominio, el denominado ciberespacio, inciden notablemente en la seguridad de los ciudadanos. Ello es debido a la aparición de nuevas amenazas que ponen en peligro bienes y derechos de los ciudadanos como usuarios de los nuevos servicios de nuestra «sociedad de la información». La seguridad pasa a ser *ciberseguridad,* al desarrollarse la acción humana en el ciberespacio.

Sin embargo, hay diversos factores por los cuales el ciudadano, como persona, no tiene una completa noción de las amenazas que debe evitar en el uso de las nuevas tecnologías. El más importante de todos ellos es la enorme rapidez con la que evoluciona el ciberespacio y el poco tiem-

po transcurrido desde que nuestra sociedad se ha visto inmersa en este nuevo medio de relación. Otro importante factor es la complejidad de las tecnologías en uso y su enorme variabilidad.

La cuestión que se plantea es, entonces, la necesidad de crear en el ciudadano una conciencia de *ciberseguridad*. Se trata, como se ha dicho anteriormente, de ser conscientes de las amenazas y la complejidad del ciberespacio, así como de asumir las responsabilidades individuales en el campo de la seguridad informática. En resumen, se trata de concienciar al ciudadano para que «habite» el ciberespacio, haciendo un uso seguro de las numerosas posibilidades que se le ofrecen.

Para tratar este asunto, se empezará por reflejar las relaciones entre el ciberespacio y la persona. Para ello, se comenzará por una definición del ciberespacio, la adopción de un modelo y una descripción del mismo. Se tratará después la persona en sus aspectos relacionados con el ciberespacio: los datos personales, la identidad digital y la evolución hacia el nuevo «ciudadano digital».

Una vez sentadas las bases de la relación de las personas con el ciberespacio, se realizará un análisis basado en el riesgo, para poner de manifiesto qué es lo que deben temer las personas al actuar en el ciberespacio y cómo se pueden defender contra ello. Se analizarán los orígenes de los ataques en el ciberespacio, las víctimas de estos ataques, los activos o bienes que corren peligro, las amenazas y las medidas para disminuir el riesgo.

La tercera parte resulta la más significativa, puesto que se refiere a la creación de la conciencia de *ciberseguridad*, basada en los análisis de los apartados anteriores. Se hablará de los grados de conciencia de *ciberseguridad* a alcanzar, de los sujetos a los que se les va a imbuir esta conciencia, de los actores que participan activamente en estas actividades, de las materias objeto de concienciación y de las vías y los medios a emplear.

El capítulo terminará con unas breves conclusiones.

El ciberespacio y la persona

El ciberespacio

Existencia

El ciberespacio está relacionado íntimamente con la información. Desde el comienzo de los tiempos históricos, ha habido repositorios de información y esta se ha tratado y transmitido, si bien de una forma poco evolucionada. En todos los tiempos y en todas las áreas de actividad humana, la información ha producido una ventaja competitiva a quien la poseía y

manejaba adecuadamente. En ello radica el embrión del ciberespacio: la humanidad era consciente del valor de la información.

Hay muchas definiciones de ciberespacio. El *Cuaderno de Estrategia* núm. 149 (2) del IEEE (pág. 51) recoge varias, de las que nos quedamos, como más conveniente, con la que da el Departamento de Defensa de los EE. UU.: el ciberespacio es *un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores*.

El ciberespacio es un nuevo dominio para la acción humana. A diferencia de los otros dominios, que existen naturalmente, es una creación artificial como resultado de una ruptura tecnológica que fue facilitada por importantes avances técnicos en el campo de los equipos electrónicos. Sin embargo, lo que la propició definitivamente fue la estrecha unión de las telecomunicaciones con el tratamiento automático de los datos; todo ello en gran volumen, a gran velocidad y a escala global[1].

Se trata de la aparición de un nuevo entorno, como otras veces se ha dado en la evolución humana. En realidad, poco importa la discusión sobre si existía antes o no, porque lo importante es que ahora hay que actuar en él y antes no. Ocurrió lo mismo con otros dominios, como el aire o el espacio exterior: se produjo una ruptura tecnológica que hizo preciso operar en estos «nuevos» dominios, donde antes no había actividad humana. La necesidad de operar en estos dominios vino dada por la gran ventaja política, estratégica y económica que obtenía el que fuera capaz de ello. Al mismo tiempo, se produjo una gran revolución en el modo de vida, a escala global.

Por tanto, hay una necesidad de adaptarse a este nuevo entorno, y lo tienen que hacer también las personas consideradas individualmente. La manera de adaptarse es mediante la evolución; la especie humana se caracteriza por su capacidad de rápida evolución, porque posee un rasgo único: la transmisión del conocimiento. El conocimiento adquirido se transmite tanto dentro de una misma generación como en el salto intergeneracional. Es, por tanto, mediante el conocimiento como se crearán las condiciones para adaptarse al ciberespacio en tiempo útil.

Modelo

Al considerar el ciberespacio como un nuevo dominio para la acción humana, se tiende a explicarlo en términos de sitios o lugares donde se puede estar de forma virtual a través de la tecnología. De esta manera,

[1] Se puede considerar la completa implementación del protocolo TCP/IP en Internet, en enero de 1983 (37), como el inicio de la ruptura.

uno puede «visitar» un sitio web o «subir» un fichero a la «nube». Esta es una concepción geográfica que se deriva de la falta de adaptación y asimilación de sus características y que se focaliza en aspectos comunitarios del ciberespacio. Pretendemos trasladar nuestra experiencia vital al nuevo entorno, donde estamos en un sitio y nos relacionamos con alguien que está en otro lugar. Sin embargo, el ciberespacio es un «no lugar». La lejanía entre dos lugares físicos y sus equivalentes en el ciberespacio puede ser muy diferente (3). Es probable que en el futuro se cree una terminología adecuada para el ciberespacio y sus características[2].

En realidad, el ciberespacio es un medio más que un espacio, y existe porque se producen flujos de información, esto es, relaciones. Lo mismo que el espacio físico se asocia a la masa y su movimiento, el ciberespacio se contempla como un medio asociado a la información y su transmisión y tratamiento, lo que pone el énfasis en los avances tecnológicos que le dieron nacimiento. A pesar de que esta es la visión que parece más adecuada, no se deben olvidar los aspectos comunitarios del ciberespacio.

A la hora de estudiar el ciberespacio, lo primero que se necesita es un modelo que nos permita describirlo y representar sus características. En este capítulo no se va a tratar de *ciberguerra* ni de seguridad de infraestructuras críticas; se trata de personas individuales y no de organizaciones complejas, por tanto, hay que buscar el modelo más sencillo.

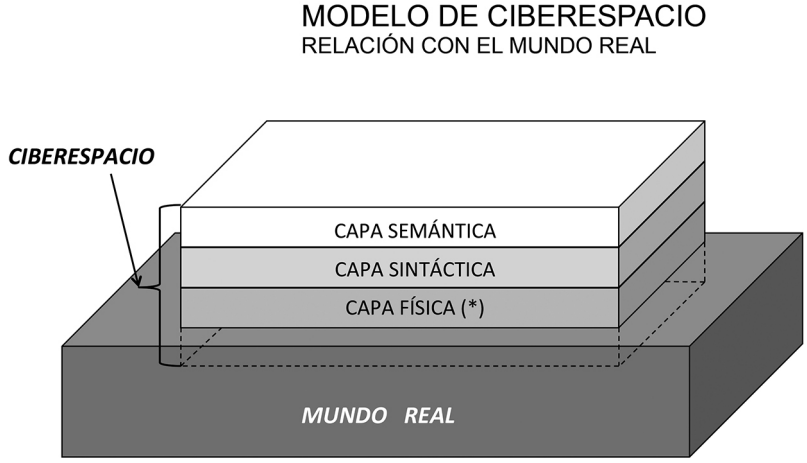
El modelo del Ejército de los Estados Unidos (4) es un modelo de tres capas (física, lógica y social) construido por cinco componentes (geográfico, red física, red lógica, *ciberpersonas* y personas reales). La capa física incluye el componente geográfico y el componente de red física; la capa lógica contiene el componente de red lógica, y, finalmente, la capa social contiene a las *ciberpersonas* y las personas reales.

Otro modelo comúnmente admitido es el propuesto por Libicki (5). Consta de tres capas, sin desglosarlas en componentes: capa física, sintáctica y semántica, siendo esta última la de más alto nivel. Entre las capas existen interfaces o zonas de transición que resultan de interés por la posibilidad de explotar vulnerabilidades en ellas y acceder a niveles más elevados.

La ventaja del primer modelo es que incluye en sí la persona. No obstante, lo que aparentemente es una ventaja puede crear confusión. La razón es que resulta necesario mantener la diferencia entre ciberespacio y mundo real. Son dos dominios diferentes para la acción humana y, por tanto, hay que mantener una separación entre ellos. De lo contrario, habría que señalar explícitamente, cada vez, si estamos hablando de *ciberpersonas* o de personas reales.

[2] Por ejemplo, la lejanía en distancia podría asimilarse inversamente al ancho de banda (cuanto menos ancho de banda disponible tiene uno, más «lejos» está).

Por todo esto, parece adecuado adoptar el segundo modelo (de Libicki), que reduce el número de capas y separa los actores humanos, permitiendo mayor flexibilidad. Tiene la desventaja de que es preciso buscar después la integración de la persona (real) en el modelo; para ello, se puede añadir una nueva capa o un dominio secante. Esto último parece más lógico ya que, de lo contrario, nos encontraríamos con algo parecido al modelo del Ejército de los EE. UU., que ya se ha considerado menos adaptado a nuestras necesidades. El modelo que se usará puede verse reflejado en la figura 2.1: en ella se aprecia cómo una parte de la capa física del ciberespacio penetra en el mundo «real», sirviendo de interfaz con él.



(*) La capa física del ciberespacio entra en el mundo real y constituye su interfaz con él.

Figura 2.1. Modelo de ciberespacio.

Cuando se habla de ciberespacio, la mayoría de las personas lo asimilan directamente a Internet, también conocida como «la red». Sin embargo, Internet es solo una parte del ciberespacio, el cual contiene en sí otras partes que podríamos denominar «regiones». Es cierto que Internet es la principal y mayor región del ciberespacio, situada entre las capas física y sintáctica; sin embargo, no hay que olvidar que existen otras regiones, asimismo importantes. Entre ellas destaca la *World Wide Web*, la popular web, que se sitúa «encima» de Internet, entre las capas sintáctica y semántica. Una parte importante de la web no está accesible a los buscadores normales y constituye la llamada web oscura o profunda que, por sus características, puede facilitar actividades ilícitas. No hay que olvidar otras, como las redes de intercambio de ficheros o P2P y muchas que utilizan Internet como soporte.

Relacionadas con las comunicaciones hay regiones interesantes como *Wifi, WiMAX, Bluetooth,* comunicaciones móviles y las «ancestrales», constituidas por el mundo de las comunicaciones telefónicas y que ac-

tualmente sigue siendo una importante zona del ciberespacio. Una importante región es la de los dispositivos de geolocalización por satélite, en la que varios sistemas, unos muy consolidados (como GPS) y otros en implantación (como Galileo) proporcionan servicios ampliamente utilizados. Finalmente, hay regiones muy particulares, como las que utilizan la radiación en distancias cortas para usos específicos: RFID (Radio Frequency Identification, o identificación por radiofrecuencia, de uso en la industria, transporte, comercio, medicina, museos, bibliotecas, deportes, etc.), NFC (Near Field Communication, o comunicación por campo próximo, usada en aplicaciones de comercio, intercambio de datos, identificación, etc.) o DSRC (Dedicated Short Range Communications o comunicaciones dedicadas de corto alcance, de uso fundamentalmente en sistemas de transporte inteligente). Finalmente, el mundo de los dispositivos médicos electrónicos constituye una pequeña pero interesante región.

Faltan muchas regiones por señalar, pero esta pequeña muestra sirve para hacerse una idea de la variedad y amplitud del ciberespacio.

El ciberespacio está considerado, cada vez más, como uno de los *global commons*[3]. Las repercusiones del daño a un espacio de este tipo exceden el ámbito concreto donde se producen y no son proporcionales al daño, sino de mayor entidad. De ahí la necesidad de preservar estos espacios.

Una manera de causar daño a estos espacios es mediante su contaminación. A veces, la contaminación del ciberespacio se produce por motivos técnicos: paquetes de información perdidos, duplicaciones, fallos en los sistemas o en las redes, programas que terminan mal, etc. Sin embargo, la mayor parte de las veces, la contaminación tiene un origen humano. La lista puede ser larga, pero citemos las más importantes: correo masivo, sitios web falsos o sin contenido, reenvío innecesario de correos o comentarios de medios sociales, buzones de correo electrónico sin uso, bases de datos obsoletas sin eliminar, ataques distribuidos de denegación de servicio, vídeos o fotografías innecesariamente subidas a Internet, etc. La seguridad y la eliminación de conductas contaminantes resultan de la mayor importancia para preservar el ciberespacio.

La persona

Datos personales

En la legislación española, el concepto de dato personal comprende «cualquier información concerniente a personas físicas identificadas o

[3] *Global commons* son los espacios o medios que no son de soberanía de ningún estado y se pueden utilizar libremente conforme a unas reglas universalmente aceptadas. Otro rasgo distintivo es que constituyen los espacios de tránsito de bienes, servicios e información a nivel global.

identificables»[4]. Esta definición comparte los elementos más importantes con otras definiciones legales sobre el mismo concepto[5]. En todos los casos concurren, necesariamente, dos condiciones: la existencia de un dato y su asociación con una persona identificada o identificable. En la actualidad, cada día se envían diez mil millones de mensajes, se introducen mil millones de entradas en medios sociales y se generan millones de registros médicos electrónicos (6). Las empresas y los Gobiernos utilizan esta enorme cantidad de datos para desarrollar poderosas, útiles y rentables capacidades analíticas. Dicho de otro modo, la creciente cantidad y calidad de los datos personales aportan un enorme valor para la economía global.

Los datos son, en palabras de Francis Maude, ministro de la Presidencia del Reino Unido, «la nueva materia prima del siglo XXI» (7). Como toda materia prima, la creación de riqueza que de ella depende surge del movimiento, de su transporte de un lugar a otro. Y, si hay algo que las nuevas tecnologías favorecen es, precisamente, la transmisión de datos.

Por otra parte, los datos como mercancía[6] poseen unas características que los diferencian notablemente de las mercancías tradicionales: por un lado, no están tan influidos por barreras como otras mercancías, ya que pueden copiarse y transmitirse globalmente de un lugar a otro indefinidamente; por otro, los datos no se consumen al usarlos: se pueden reutilizar sin pérdida de valor; en tercer lugar, al procesar datos se crean nuevos datos que poseen mayor valor y que pueden ser procesados de nuevo, y, finalmente, las personas (sobre todo tras la implantación de la web 2.0) tienen un papel cada vez más activo en la creación de datos que les están unidos estrechamente. Estas características hacen que sean necesarias nuevas normas y marcos de actuación si no se quiere que se pierda el potencial de los datos personales como motor económico.

A la vista de ello, existe necesariamente una tendencia a la «monetización» de los datos. Las personas han comprendido el valor que los datos personales tienen para las administraciones y las corporaciones y quieren aprovecharlo en su beneficio. Este valor está creciendo continuamente, ya que cuantos más datos hay, más valor poseen, al contrario que otras mercancías como el oro. En enero de 2012, la comisaria europea de Justicia, Viviane Reding, dijo en la presentación del Reglamento General de Protección de Datos: «Los datos personales son, en el mundo de hoy, la moneda del mercado digital. Y, como cualquier moneda, debe ser es-

[4] Artículo 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

[5] Por ejemplo, la Directiva de Protección de Datos (Directiva 95/46/EC) de la Unión Europea o lo que, en diferentes regulaciones, entiende el Gobierno Federal de los EE. UU. por *personally identifiable information*.

[6] En el sentido anglosajón de *commodity*.

table y digna de confianza» (8). La estabilidad depende de la disposición de las personas para comunicar sus datos, que se ve mermada si sienten amenazada su privacidad. Resulta necesario, por tanto, que las empresas y administraciones sean capaces de crear y mantener la confianza que hace fluir los datos. La protección de datos personales y la posibilidad de usarlos en un contexto económico deben alcanzar un equilibrio en el que la persona pueda decidir libremente si comunica o comparte sus datos y en qué grado.

Hay condiciones personales que influyen en la facilidad con la que se comunican los datos. Un estudio de The Boston Consulting Group (9) muestra que muchas personas se sienten preocupadas por un posible mal uso de sus datos. Sin embargo, hay menos que sean conscientes de cómo son empleados de verdad sus datos, y menos aún son capaces de utilizar adecuadamente los mecanismos de que disponen para controlar su privacidad.

El mismo estudio refleja que las personas se muestran sensibles a la comunicación de sus datos en función de varios factores, ordenados de mayor a menor peso:

- Tipo de datos: algunos datos son más sensibles que otros. Las personas están menos dispuestas a comunicar datos sobre su salud o sus finanzas que sobre sus intereses o su correo electrónico. Es el factor más significativo.
- Beneficio: mediante un incremento en la compensación recibida, es posible incrementar, hasta un cierto límite, la disposición a comunicar datos. No se aplica a datos muy sensibles.
- Sector: hay sectores, como el del comercio electrónico, a los que existe una mayor proclividad a comunicar datos. Las redes sociales se encuentran en el extremo contrario.
- Uso de los datos: el uso previsto de los datos influye notablemente, de forma que, por ejemplo, existe una gran resistencia a comunicar datos a una empresa que vaya a transferirlos a una tercera parte.
- Forma de obtención: en este factor se ve implicada la percepción sobre «de quién es el dato». Si los datos se comunican de forma completamente voluntaria, hay una mayor disposición a ello. La disposición disminuye si los datos le son requeridos necesariamente para una determinada transacción[7]. La predisposición disminuye mucho cuando los datos son observados, es decir, capturados por otro, o cuando se utilizan técnicas de «minería de datos» para inferir nuevos datos a partir de los que ya se han comunicado.

[7] El término «transacción» se utilizará en adelante en sentido amplio, no siendo necesariamente una transacción comercial.

– Derecho a cancelación: si la organización que pide los datos implanta mecanismos para ejercer efectivamente este derecho, la disposición a comunicar datos es mayor.

En definitiva, podemos decir que una regulación adecuada de la protección de datos personales, la creación de un clima de confianza, la educación de las personas en relación con el control de su privacidad y una compensación equitativa pueden hacer sumamente provechosas las aplicaciones de los datos personales. En otras palabras, se trata de un crecimiento económico que podría alcanzar en 2020 la cantidad de un billón de euros, según el citado estudio de The Boston Consulting Group.

Identidad digital

En el mundo real, cada persona posee una identidad[8]. La identidad personal es un conjunto de características y atributos que la describen unívocamente. Por tanto, se trata básicamente de una colección de datos personales. Aparte de las personas, otras entidades del mundo real también poseen una identidad (p. ej. un comercio o un equipo deportivo) y ello permite que existan relaciones y transacciones (10), al poder determinar con veracidad quiénes intervienen en ellas. La esencia del concepto es que no existen dos identidades iguales: cada identidad se corresponde con un único conjunto de características, para lo cual habrá, a veces, que incrementar el tamaño de este conjunto. Ello no quiere decir que una misma persona no pueda poseer más de una identidad, pero para conseguirlo hay que disponer de varios conjuntos de características únicos que le puedan ser atribuidos, de los cuales uno solo será verdadero en un momento dado. Por otra parte, la posesión de varias identidades suele estar considerada como algo fraudulento o ilegal, entre otras cosas porque facilita la comisión de delitos.

El ciberespacio es un nuevo medio de actuación para las personas. Para poder actuar y relacionarse necesitan, como se ha dicho, una identidad digital que asegure verazmente quiénes son. Hay datos de su identidad personal que siguen siendo útiles para identificarse en el ciberespacio, como, por ejemplo, el número del DNI. Sin embargo, hay datos que se requieren para actuar en el ciberespacio que no son necesarios en las relaciones del mundo real (p. ej., certificados digitales o dirección de correo electrónico). La identidad digital de la persona deberá reunir esos datos para poder desenvolverse en el ciberespacio.

La identidad digital es el conjunto de todos los datos digitales disponibles relativos a una persona, independientemente de su validez, el formato

[8] Se trata de un derecho, desde el nacimiento, recogido por el artículo 8 de la Convención sobre los Derechos del Niño, de las Naciones Unidas, ratificada por España en 1990.

que tengan o lo accesibles que sean. Hay tres tipos de datos, o características del individuo, que pueden estar presentes en este conjunto:

- Características inherentes, ligadas a su persona íntimamente, como pueden ser su fecha y lugar de nacimiento, su nombre, nacionalidad, etc.
- Características adquiridas, que se acumulan a lo largo del tiempo y van creando una línea histórica. Por ejemplo: domicilio, número de cuenta bancaria, historial médico o impuestos.
- Preferencias: música preferida, aficiones, equipo favorito, literatura, etc.

En el mundo real, las relaciones y transacciones acarrean intrínsecamente la identidad. Por ejemplo, al adquirir una mercancía en un comercio el dependiente ve la cara del comprador, dato importante de la identidad. En la mayoría de las transacciones importantes se exige un cierto grado de identificación. En el ciberespacio, las relaciones y transacciones consisten en un intercambio de información, que no tiene necesariamente que llevar asociado rasgos identificativos de los intervinientes. La transmisión de la identidad digital, o de parte de ella, junto con el resto es lo que permite crear la confianza necesaria para llevar a buen término la transacción.

El conjunto de datos que conforman la identidad digital de una persona puede ser muy amplio. Las personas se preocupan por mantener su privacidad, por lo que se muestran poco dispuestas a comunicar más datos de los necesarios. Por tanto, su tendencia será a acompañar sus relaciones en el ciberespacio del menor número de datos necesarios para su propósito. Evidentemente, esto choca con los intereses de las otras partes, que desearían obtener la mayor cantidad de datos posibles.

Confianza y privacidad son, por tanto, desde el punto de vista de la persona, las principales preocupaciones a la hora de comunicar o compartir su identidad digital. Ya hemos visto cuáles son los factores que influyen en las personas a la hora de comunicar sus datos personales.

Las personas no son las únicas entidades que intervienen en las relaciones y transacciones en el ciberespacio: los otros dos actores importantes son los Gobiernos (incluyendo no solo los estatales, sino entidades supranacionales, en su caso) y las corporaciones (empresas, organizaciones, etc.) del sector privado. En este triángulo es donde se deben dar las condiciones necesarias para que el clima de confianza se cree y se mantenga. Alcanzar esta situación requiere un equilibrio que respete las tendencias, deseos y necesidades de los tres actores:

- Las personas quieren mantener su privacidad, mejorando el control sobre los datos que comunican, obteniendo una mayor transparencia

sobre cómo y dónde se usan estos datos y obteniendo un beneficio justo de retorno por compartir sus datos.

- Los Gobiernos quieren ser impulsores del crecimiento, estimular la innovación y proteger los derechos de las personas.
- Las corporaciones quieren incrementar sus ganancias, mejorar su eficiencia y ser capaces de efectuar predicciones ajustadas.

Para ello resulta necesario un diálogo entre las distintas partes, el establecimiento de unos principios admitidos por todos y la implantación de normas firmes y flexibles, así como una continua experimentación sobre el terreno para ser capaces de discriminar lo que funciona de lo que no.

El control de la privacidad puede ser ejercido, en general, desconectando entre sí los datos que forman la identidad digital (10). Por un lado, separando cada dato de los otros y compartiendo solo los subconjuntos o, incluso, datos aislados necesarios para las transacciones; de esta manera, nos encontramos con un amplio espectro de posibilidades, en el que en un extremo se encuentra la privacidad total o anonimato (no se comunica ningún dato) y en el otro la revelación completa de la identidad digital. Por otra parte, el enlace existente entre la identidad digital y la identidad real, es decir, el proceso de «autenticación», puede ser más o menos fuerte. Si se consigue hacer tan débil el enlace que este se rompe, tendremos una identidad personal y una identidad digital diferentes, lo que muestra que en el ciberespacio es posible el verdadero anonimato. Es más, roto ese vínculo, nada impide tener varias identidades digitales que pueden ser completamente diferentes, incluso contradictorias, lo que en el mundo real es mucho más difícil y, a veces, imposible[9]. Pero no es lo mismo tener distintos perfiles en diferentes servicios en Internet que poseer distintas identidades digitales; el enlace de los perfiles con la persona real es lo que marca la diferencia. Las amenazas en el ciberespacio explotan estas posibilidades.

A veces, se da una confusión entre identidad digital y reputación digital. Son conceptos diferentes aunque relacionados. La reputación digital es un concepto similar al de la reputación personal, pero aplicado a la identidad digital del individuo y a sus diversas manifestaciones. También llamada reputación *online,* reúne la opinión, consideración o prestigio que se percibe de una persona a partir de los datos o informaciones que aparecen sobre ella en el ciberespacio. La explosión de los contenidos generados por el usuario (*user generated content, UGC*) y el uso masivo de los medios sociales (*social media*) desarrollados sobre la web 2.0 originan una huella (11) que permite construir la reputación digital de una persona mediante la acumulación de los contenidos creados por sí mis-

[9] Por ejemplo, que un hombre de más de cincuenta años adopte la identidad de un adolescente, caso frecuente en delitos de acoso sexual a menores en la red.

ma y los creados por otros y referidos a ella. La gestión de la identidad digital y su traducción en una buena reputación digital es un factor clave actualmente de la presencia personal, de empresas e instituciones en el ciberespacio[10].

La identidad digital es la expresión de nuestro yo en el ciberespacio. Muchas tensiones en el individuo, relativas a la comunicación de su identidad digital, se derivan de la necesidad psicológica de formar y preservar adecuadamente los componentes de esta. Estos aspectos psicológicos deben ser tenidos en cuenta, ya que explican conductas aparentemente contradictorias.

Ciudadano digital

Provistas de su identidad digital, las personas actúan en el ciberespacio. Inicialmente, su papel tenía un marcado carácter pasivo: recibían la información que diversas organizaciones «ponían en red» para ellas. Sin embargo, la implantación de la web 2.0 supuso la asunción por parte de las personas de un papel más activo: generan contenido, usan los medios sociales, compran, hacen transacciones bancarias, etc. Del mismo modo que las personas participan en la sociedad del mundo «real» asumiendo su condición de ciudadanos, las posibilidades abiertas por la tecnología permiten asumir las responsabilidades de ciudadanos digitales.

El grado de conciencia ciudadana digital se puede expresar, al igual que el grado de conciencia ciudadana ordinaria, de tres maneras distintas, que no siempre se acumulan en el mismo individuo (12):

- Ciudadano responsable, que actúa cumpliendo con sus deberes cívicos, cuida el entorno, observa las reglas, no hace mal uso de la tecnología, etc.
- Ciudadano participativo, que usa la web 2.0 para implicarse en los asuntos de su comunidad, desde el nivel local al estatal.
- Ciudadano orientado a la justicia, que utilizará activamente los recursos tecnológicos para intentar ayudar a resolver problemas sociales.

Independientemente del grado de conciencia ciudadana digital, hay varios elementos constitutivos de la ciudadanía digital. El primero de ellos es el respeto a la ley al actuar en el ciberespacio. Existen leyes aplicables específicamente al ciberespacio, si bien es verdad que la legislación va en este terreno por detrás de la tecnología. Sin embargo, la legislación ordinaria se aplica por analogía y las actividades en el mundo digital no pueden hurtarse a sus reglas.

[10] Es cada vez más común la presencia de los gestores de comunidades virtuales (*community manager*) en las organizaciones para sostener, acrecentar y, en cierta forma, defender las relaciones externas en el ámbito digital.

En segundo lugar, hay que considerar los derechos y deberes del ciudadano digital. Se incluyen aquí, por ejemplo, el respeto a la propiedad intelectual de otros, no contaminar el ciberespacio y no molestar a los demás cuando se usa el teléfono móvil. Abarca también lo que se llama tradicionalmente urbanidad o buena educación, pero referido al uso de las tecnologías.

En tercer lugar, se deben considerar los aspectos relativos a la comunicación en el mundo digital. Aquí interviene no solo el uso adecuado de cada medio, sino también cuándo y para qué usarlo. La creciente necesidad de estar continuamente «conectado» es un ejemplo de mal uso de los medios. Los contenidos que se transmiten son un aspecto importante, ya que, en determinados casos, pueden dar origen a responsabilidades legales y, sin llegar a este extremo, pueden producir daño a los demás.

Un cuarto aspecto es el de la seguridad. El ciudadano digital debe ser consciente de que informándose y prestando atención a la seguridad de sus propios medios, y adoptando conductas seguras, colabora a la seguridad del ciberespacio en su conjunto. Aparte de ello, disminuye la posibilidad de ser víctima de ataques, cuyas consecuencias pueden ser muy nocivas para él.

Finalmente, es necesario considerar al ciudadano digital como consumidor. Existen muchos servicios disponibles en la red para el ciudadano, y se requiere un uso responsable de estos servicios, ya sea a la hora de comprar, vender, operar con el banco, etc. La conducta de los consumidores influye en la actividad económica en el ciberespacio, que puede ser un importante motor de crecimiento.

Los riesgos

Los ciudadanos habitan, adaptándose a él, un nuevo entorno: necesitan seguridad. Esta se mide por el valor de lo que está en riesgo. Por lo tanto, la mejor manera de analizar la seguridad es centrarse en los riesgos.

Análisis centrado en los riesgos

El análisis centrado en los riesgos es una metodología muy extendida, de la que un ejemplo usado en las Administraciones Públicas en España es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) (13). En este apartado se va a seguir un análisis de este tipo, adaptado a las circunstancias y los requerimientos que definen el caso: riesgos de las personas actuando individualmente en el ciberespacio.

Procederemos, en primer lugar, a identificar las posibles víctimas. Se ordenarán según su debilidad.

Luego se determinarán los posibles *atacantes,* que son los entes, personales o impersonales, que se encuentran en el origen de los ataques. Un atacante puede ser un *ciberdelincuente* o un empleado descontento, aunque también puede ser una inundación. Se descartan los más improbables, ordenando los demás según su peligrosidad.

Después hay que determinar los *activos* en riesgo, entendiendo como activo un elemento o atributo, material o inmaterial, que la persona posee y que tiene un determinado valor para ella, objetivo o subjetivo. Este valor hay que determinarlo. Ejemplos de activos materiales son un ordenador personal o un teléfono móvil inteligente. Del mismo modo, los datos bancarios o de salud son activos inmateriales. Los activos se relacionan entre sí, formando lo que se llama un árbol de activos, que es un grafo que indica cómo el daño o pérdida de algún activo influye en los demás, en el que cada «rama» está formada por los activos relacionados por una línea del grafo[11].

Hay que ver cuáles son las *amenazas* a los activos. Las amenazas son sucesos formados por cadenas de eventos, relacionados entre sí, que conducen a la pérdida o degradación de los activos. Una amenaza se define como una acción. Por ejemplo: «un virus infecta al ordenador al abrir el usuario un fichero anexo a un correo electrónico». Hay que determinar su posibilidad de ocurrencia, con lo que, para cada rama del árbol de activos, sabremos cómo de *vulnerable* es a cada amenaza. Luego se verá la cuantía del daño de cada amenaza sobre cada activo (la degradación o pérdida de valor que produce), lo que nos proporciona una medida del *impacto* que tiene esa amenaza al materializarse. De la relación *vulnerabilidad-impacto* obtendremos, para cada par amenaza/activo, una medida del *riesgo.*

El concepto de riesgo combina la vulnerabilidad y el impacto sobre una rama del árbol de activos. Cuanto mayor sea la vulnerabilidad y más grande el impacto, mayor será el riesgo. El riesgo nulo no existe, por lo que deberemos aceptar un determinado nivel de riesgo para cada rama del árbol de activos, denominado riesgo residual.

Lo anterior se puede representar en la figura 2.2. En esta figura[12], el punto muestra la representación del riesgo de una determinada rama del árbol de activos. El riesgo del conjunto del árbol formaría una nube de puntos. Tanto si actuamos sobre la vulnerabilidad como si lo hacemos sobre el impacto, reducimos el nivel de riesgo, como se aprecia en las flechas que llevan el punto a otras regiones. Se debe actuar, en la medida de lo posible, sobre ambas, ya sea *minimizando la posibilidad de ocurren-*

[11] Ver figura 2.6.

[12] Este tipo de matriz de riesgo es común en diversas metodologías de análisis de riesgo cualitativo, como la del European Telecommunications Standards Institute (ETSI) en su informe técnico TR 101 771V1.1.1 (40), la que contiene el MIL-STD-882E (41), la contenida en la publicación 800-30 *del* National Institute of Standards and Technology (44) o el estándar ISO/IEC 27005 (45).

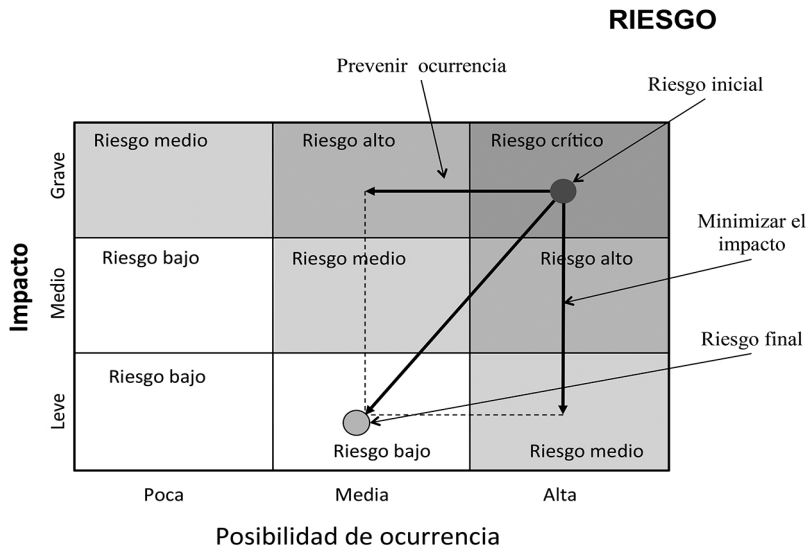


Figura 2.2: Riesgo (una rama del árbol de activos)

cia de las amenazas (p. ej., usando contraseñas robustas) o *mitigando el impacto* en caso de que se produzca (v. g. haciendo copias de respaldo). Con ello obtendremos una mayor eficacia, sumando vectorialmente los efectos de nuestras medidas.

La figura 2.3 representa, mediante una nube de puntos, el riesgo total del conjunto de ramas del árbol de activos. La reducción del riesgo consigue llevar cada punto a una región de riesgo aceptable para ese activo. Hay

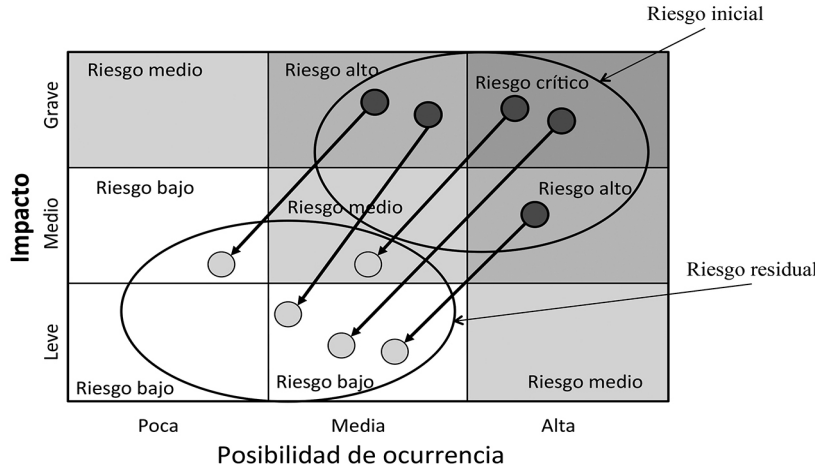


Figura 2.3: Reducción del riesgo del conjunto.

que desplazar toda la nube para que quede repartida en regiones aceptables. En caso contrario, tendremos eslabones débiles, lo que equivale a sacrificar esas ramas.

Se ordenarán los riesgos de mayor a menor. Todo ello con la idea de deducir las medidas para reducir los riesgos, lo que constituirá la conclusión del estudio.

Atacantes

En el arte de la guerra es esencial el conocimiento del enemigo, sin el cual cualquier campaña está destinada al fracaso. En el campo de la *ciberseguridad*, el conocimiento de los enemigos, a los que denominaremos atacantes o también orígenes de ataques, resulta asimismo esencial.

Al hablar de acciones hostiles en el ciberespacio en sus diferentes modalidades nos enfrentamos a un primer problema, que es el de la *atribución*. La atribución es la capacidad de poder identificar quién ha atacado un determinado objetivo y desde dónde. Se trata de un problema con trascendencia legal que plantea un fuerte reto técnico, ya que los orígenes de los ataques emplean medios y técnicas muy elaborados para ocultar sus huellas (14). A veces, es muy difícil incluso determinar el verdadero objetivo del ataque, debido al empleo de técnicas de decepción.

Una de las características esenciales del ciberespacio es su continua y rápida evolución, y las amenazas en el ciberespacio evolucionan también rápida y continuamente. Para conocerlas, no basta con elaborar una lista, más o menos completa, de los posibles atacantes, por muy actualizada que esté[13]; es necesario establecer unos criterios que permitan elaborar una taxonomía de los orígenes de los ataques en el ciberespacio. Los criterios pueden ser muy variados y se puede hacer crecer bastante su número, si se consideran todos los factores de interés. Sin embargo, para que sean útiles, hay que tener en cuenta no solo los actores inmediatos de los ataques, sino también los verdaderos agresores y sus motivaciones (15). Una taxonomía con pocos criterios proporciona unos grupos amplios que son fáciles de manejar; por el contrario, el empleo de muchos criterios permite alcanzar un elevado grado de detalle en los grupos (se aumenta la granularidad del análisis) a cambio de un resultado complejo y poco manejable (16). Es necesario, pues, encontrar un término medio, apto para los fines de este capítulo. Una adecuada clasificación nos dará, además, una idea de cuál es la más probable evolución de los atacantes en el futuro.

Utilizaremos como primer criterio el de distinguir entre orígenes de ataque conscientes o fortuitos. Los primeros son personas o grupos, mien-

[13] La Inspección del Gobierno (Government Accountability Office, GAO) de los EE. UU. ha elaborado una tabla de atacantes que se puede consultar en (36).

tras que los segundos son consecuencias no buscadas de la acción humana o de la naturaleza. Entre estos últimos, los más importantes son:

- Catástrofes naturales, de mayor o menor gravedad.
- Accidentes, generalmente de tipo físico, aunque incluiremos también aquí los errores cometidos por el usuario o por mal diseño o funcionamiento de los sistemas.
- Averías, de tipo físico o lógico, ya sea en los propios equipos o en el suministro de energía eléctrica, servicios de telecomunicación u otros.

Entre los orígenes humanos, emplearemos inicialmente el criterio de la capacidad de acceder a los recursos atacados. Los atacantes internos, denominados generalmente *insiders*, tienen acceso ordinario y están familiarizados con el equipo o equipos objeto de ataque, siendo el «empleado descontento» el ejemplo más notorio. Utilizan la facilidad de acceso y el conocimiento de los sistemas para lograr sus fines. Los demás son atacantes externos. Desde el punto de vista que nos interesa, los *insiders* pueden ser de dos tipos, atendiendo a sus capacidades:

- Normales: usuarios de los sistemas, con privilegios y perfil normal.
- Cualificados: debido a sus conocimientos, experiencia o al nivel de acceso a los sistemas que poseen, tienen posibilidades de producir graves daños.

Todos los atacantes externos hacen uso de, o son ellos mismos, lo que se conoce como *hackers*[14]. La palabra *hacker* es de difícil traducción al español; la denominación española más corriente es la de «pirata informático» pero este término, con connotaciones peyorativas, no proporciona el verdadero sentido, ya que hace referencia a un aspecto particular de un determinado tipo de *hackers*. Por tanto, será necesario mantener el anglicismo a fin de conservar su significado. Para los efectos que nos interesan, un *hacker* es un individuo que posee grandes conocimientos y experiencia en sistemas de información y telecomunicaciones, hasta el punto de que es capaz de sortear las distintas medidas de seguridad establecidas en ellos y conseguir acceso y control de equipos o sistemas. Desde principios del siglo XXI, los *hackers* han evolucionado hacia comunidades con identidad definida, constituyendo grupos en función de sus intereses. Aparecen espacios y mecanismos de comunicación entre ellos, así como reuniones y convenciones[15]. Generalmente, se suelen distinguir tres tipos de *hackers*[16]:

[14] Algunos *insiders* cualificados también pueden entrar, simultáneamente, en esta categoría.

[15] Para una historia de los *hackers*, ver Goldstein, 2006 (34).

[16] Hay quien añade otro tipo, denominado *hackers* de sombrero gris, pero no nos resulta útil, ya que, para los fines de este trabajo, pueden ser asimilados a los *hackers* negros.

- Hackers «de sombrero blanco»: siguen un código ético[17] y sus acciones se realizan con buenos fines. Normalmente buscan la mejora de la seguridad de los sistemas, utilizando sus habilidades para penetrar en ellos y descubrir sus vulnerabilidades, que luego dan a conocer para que sean subsanadas. Por su propia definición, no deben ser considerados atacantes, aunque penetren la seguridad de los sistemas.
- Hackers «de sombrero negro»: sus acciones son malintencionadas, no siguen un código ético y suelen estar motivados por intereses financieros. Al contrario que los otros dos tipos de hackers, no buscan publicidad de sus acciones.
- Hacktivistas: están políticamente motivados y dirigidos y utilizan el ciberespacio para sus acciones, generalmente de protesta, que buscan venganza contra sus objetivos. Estos suelen ser gubernamentales, institucionales o corporativos. Se organizan en grupos que actúan coordinadamente.

El desarrollo por parte de los *hackers* de herramientas cada vez más perfeccionadas y de más fácil uso ha dado lugar a la aparición de los denominados *script kiddies.* Son personas que no poseen experiencia ni grandes conocimientos de informática, por lo que no son capaces de desarrollar sus propias herramientas o programas de ataque. En cambio, utilizan programas desarrollados por otros para sus ataques y están motivados por el ansia de reconocimiento dentro de las comunidades *hacker*, en las que el término *script kiddy* es despectivo. Se pueden asimilar a *hackers* de sombrero negro poco cualificados, aunque su motivación sea distinta y sus ganas de notoriedad también.

El segundo criterio aplicable a los orígenes conscientes de ataques es el de la motivación (17). Simplificando, podemos encontrar las siguientes motivaciones detrás de los ataques:

- Política (incluye también el patriotismo y la ventaja estratégica o táctica de grupos o estados, así como la obtención de información para esos fines).
- Lucro (beneficio o ventaja económica o comercial, obtención de información y financiación de otras actividades).
- Sentimientos negativos (venganza, y también odio, agresividad, deseo de dominación, rivalidad y otras expresiones de este tipo de sentimientos).
- Satisfacción personal (conducta sexual desordenada, narcisismo, afán de notoriedad, curiosidad o pura diversión).
- Ética (mejorar la seguridad de los sistemas, ayudar a otros).

[17] Un estudio sobre la ética *hacker* puede encontrarse en Mizrach, 1997 (35).

Se deben considerar el lucro, la venganza o la satisfacción personal como las motivaciones más probables de ataques a las personas en el ciberespacio. Las otras motivaciones son propias de atacantes que buscan otras víctimas.

Finalmente, se ha de tener en cuenta la naturaleza del atacante. No se trata de quién realiza directamente el ataque, sino de quién está detrás y cuál es su relación con él. Desde ese punto de vista, podemos distinguir estas clases de atacantes:

- Individuos: no tienen relación con otras personas o grupos.
- Corporaciones: entidades legales con intereses, generalmente económicos.
- Grupos: que pueden tener distintas motivaciones, estar constituidos de forma permanente o crearse ad hoc y cuyo grado de organización es variable.
- Estados: naciones o estados soberanos que ejecutan ataques por motivos estratégicos o políticos.

De la aplicación de estos criterios podemos deducir esta clasificación de los orígenes de ataques:

- Fortuitos o no conscientes:
  - Catástrofes.
  - Averías.
  - Accidentes.
- Conscientes:
  - Internos (*insiders)*:
    - Normales.
    - Cualificados.
  - Externos.
    - Individuales:
      * Delincuentes informáticos (*hackers d*e «sombrero negro»).
      * *Hacktivistas.*
    - Corporaciones.
    - Grupos:
      * *Ciberactivistas.*
      * *Ciberanarquistas.*
      * *Ciberdelincuencia organizada.*
      * *Ciberterroristas.*
      * *Cibermilicias* (generalmente bajo el paraguas de un estado).
    - Estados.

La figura 2.4 representa esquemáticamente estos tipos de atacantes. En la figura 2.5 se representan las posibles evoluciones entre ellos.

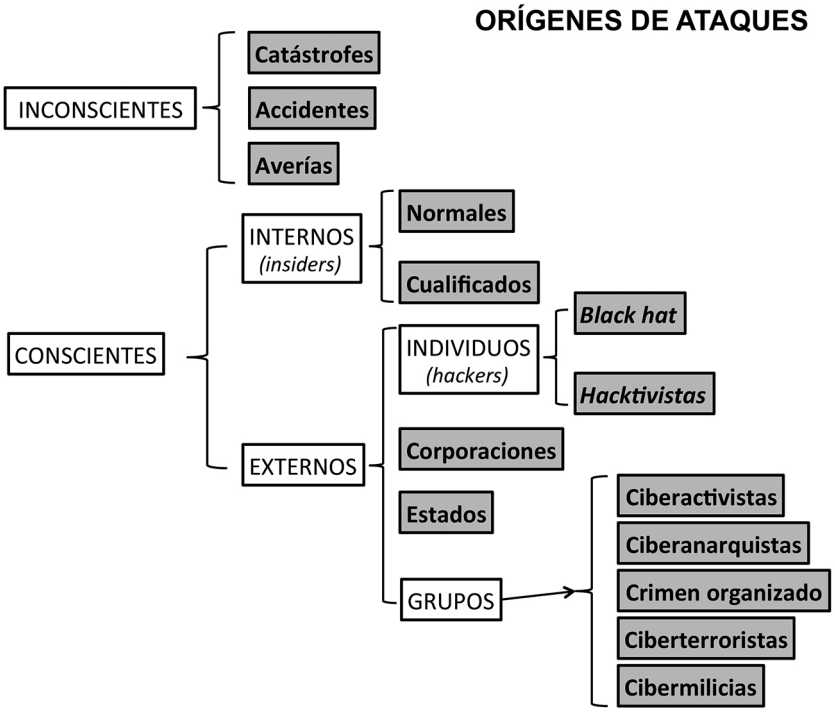


Figura 2.4: Orígenes de ataque.

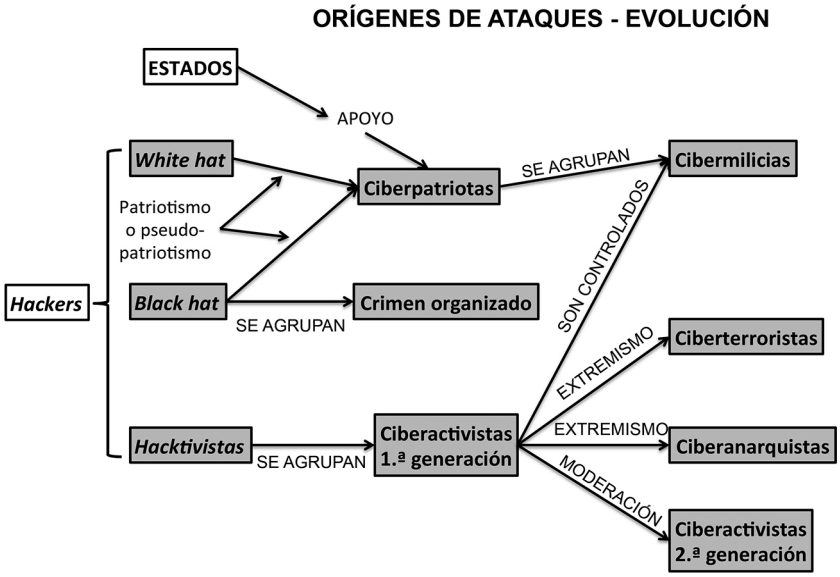


Figura 2.5: Orígenes de ataque, evolución.

De todos estos orígenes, hay que prestar atención a los más probables y los más peligrosos por el posible impacto de sus acciones. Contra los ciudadanos «normales» debemos considerar como de baja probabilidad, en general, la acción de determinados agresores, como puedan ser los estados, las corporaciones[18], los *hacktivistas* y grupos de activistas cibernéticos, así como los *ciberanarquistas.* Nos centraremos, por tanto, en esta relación más reducida:

- Orígenes fortuitos.
- Atacantes internos (insiders) de perfil normal, cuya motivación suele ser la venganza o la expresión de otros sentimientos hostiles, sin descartar el lucro.
- *Ciberdelincuentes* (18) individuales o grupos de crimen organizado, que actúan motivados por afán de lucro. Otras posibles motivaciones son la satisfacción personal o los sentimientos negativos.
- Ciberterroristas (19), motivados por la necesidad de conseguir financiación para sus actividades. Por ello, los agruparemos con los *ciberdelincuentes*, ya que usarán sus mismos métodos. No son de esperar ataques directos a los ciudadanos por los terroristas, ya que preferirán blancos de mucha mayor entidad con los que crear el terror que buscan. En este sentido, hay que temer, únicamente, la apropiación de los equipos de los ciudadanos (creación de *botnets*[19]) o la suplantación de identidad.
- *Cibermilicias*, bajo el paraguas del Estado. Su motivación es política y buscarán apropiarse remotamente de los equipos individuales para conseguir los objetivos marcados (creación de *botnets*).

Como conclusión, se puede decir que la persona debe estar atenta y precaverse contra tres orígenes genéricos de ataques: causas fortuitas, personas próximas y amenazas en la red.

Víctimas

No resulta útil, para los propósitos de este trabajo, describir una completa tipología de las potenciales víctimas de *ciberataques.* Sin embargo, conviene discernir, entre toda la población concernida, aquellos tipos que pueden provocar o ser más susceptibles a determinados ataques.

[18] Sin embargo, una corporación como la revista dominical *News of the World* tuvo que cerrar tras ser acusada de espiar comunicaciones y correos electrónicos de personajes famosos, pero también de ciudadanos corrientes relacionados con sucesos de interés periodístico (p. ej., familiares de soldados muertos en Afganistán).

[19] *Botnet:* Red formada por un conjunto de ordenadores que han sido infectados con un tipo de *software* malicioso, con funcionalidad de «puerta trasera», que permite a un atacante controlar dichas máquinas sin necesidad de acceso físico a ellas y sin el conocimiento del propietario.

Una primera clasificación nos lleva a considerar dos grupos: los menores y el resto. Los menores son un grupo especial porque se encuentran en una etapa muy importante del desarrollo de su personalidad y las acciones contra ellos pueden ver multiplicados sus efectos. Por otra parte, por motivos legales y morales, el Estado, la sociedad y todos sus integrantes tienen un imperativo que obliga a su protección. Este grupo, por tanto, debe ser objeto de una atención especial. Hay que tener en cuenta, además, que el tipo de menores que, por motivos psicológicos o sociales, son vulnerables en el mundo real son especialmente vulnerables en el ciberespacio. El informe de los resultados de la encuesta en España del proyecto europeo *EU KidsOnline* muestra el uso que los menores de entre 9 y 16 años hacen de Internet (20). Por otro lado, los que actualmente son menores de edad pertenecen a la generación de los llamados «nativos digitales» por haber tenido acceso desde muy pequeños a Internet y a las tecnologías de la información y las telecomunicaciones. Esta generación será la que marque las pautas para la adaptación al ciberespacio.

Hay tres perfiles sociodemográficos con mayor número de internautas en España (21). El primero se corresponde a personas con primera etapa de educación secundaria, entre 16 y 24 años y residentes en municipios de más de cincuenta mil habitantes; el segundo a personas con estudios superiores universitarios, que trabajan por cuenta ajena o estudian y tienen menos de 45 años, y el tercero a personas con segunda etapa de educación secundaria y edad entre 16 y 24 años. Las actividades en la Red de los internautas de perfil primero y tercero están más asociadas al uso de redes sociales, descarga de juegos, imágenes o música y a subir contenidos. En cambio, las del perfil segundo corresponden a consulta de noticias, búsqueda de viajes y alojamientos y a la banca electrónica.

Acorde con las actividades más comunes de los distintos perfiles, se pueden deducir, aproximadamente, a qué tipos de amenazas se enfrentarán con mayor probabilidad. Por ejemplo, debido a sus actividades de descargas de juegos, imágenes o música, los internautas de perfil primero y tercero estarán más expuestos a infecciones por código dañino, que veremos más adelante. Los del segundo grupo, por hacer amplio uso de la banca electrónica, estarán más expuestos a ataques de suplantación de identidad, que también serán considerados más adelante.

Activos

Un activo es un elemento o atributo, material o inmaterial, que la persona posee y que tiene un determinado valor para ella, objetivo o subjetivo. En el análisis centrado en el riesgo, los activos son un elemento determinante y, por tanto, su identificación es esencial. A fin de hacer más sencillo el análisis, se prescindirá de aquellos activos que no tienen relación con la actuación humana en el ciberespacio ni con las consecuencias, en el

mundo real, de estas acciones. No se trata de elaborar un mero inventario de los activos sino de establecer una jerarquía entre ellos y determinar las relaciones y dependencias existentes. En definitiva, se necesita establecer un «árbol de activos» en el que cada rama muestre cómo el daño o pérdida de uno de sus elementos influye en otros.

A lo anterior hay que añadir una valoración de los activos. El criterio para realizar la valoración se basa fundamentalmente en evaluar su ausencia y la trascendencia que ello tiene. Hay activos que se pueden valorar objetivamente, como los elementos patrimoniales; otros tendrán una valoración meramente subjetiva, y, por último, los hay que requieren combinar elementos cuantitativos y cualitativos. Lo importante de la valoración es que permite, en una fase posterior, estimar el impacto producido por la pérdida o daño del activo o de la rama del árbol de activos, en su caso.

El primer activo que se va a considerar es el *equipo físico* (que incluye el *hardware* y el *software*). Para la persona, constituye el punto de acceso, deseado o no, al ciberespacio. Se trata de ordenadores personales, portátiles, tabletas, consolas de videojuegos, teléfonos móviles (inteligentes o no), etc. También hay otros no tan extendidos como dispositivos biomédicos o tarjetas inteligentes de diverso tipo. Su valor se puede medir objetivamente y, generalmente, es su valor de cambio o de mercado. Normalmente es posible su reposición.

Los *datos personales* son un activo que se ha tratado extensamente en este capítulo. También se ha mencionado el valor que poseen, tanto para las personas como para la economía global.

La *identidad digital* también ha sido considerada anteriormente; es un atributo de la persona que posibilita su actuación en el ciberespacio. El valor de la identidad digital se deriva, fundamentalmente, del grado de privacidad que su propietario desea y de la necesidad de comunicarla para las transacciones en el ciberespacio.

La *identidad personal* es un conjunto único de características y atributos esenciales que describe unívocamente a una persona. Esta identidad es la que se presenta ante otras entidades del mundo físico y se requiere para realizar interacciones de diversa importancia o frecuencia (10). El valor de la identidad personal se puede medir con criterios similares a la identidad digital. Sin embargo, hay que señalar que el daño a la identidad personal es más difícil de reparar, ya que los mecanismos legales para recuperar los diversos atributos pueden llegar a ser complejos y dilatados, aparte de consumir recursos económicos.

La *integridad moral* es un atributo de la persona, a la que se reconoce dotada de dignidad por el solo hecho de serlo. Proviene de considerar al ser humano como sujeto moral en sí mismo, investido de la capacidad para decidir responsablemente sobre el propio comportamiento y no

ser tratado como una cosa. El ordenamiento legal internacional reconoce el derecho a la integridad moral, al igual que la Constitución Española, en su artículo 15. Ello supone, en definitiva, el derecho de toda persona a ser libre y respetada o, en sentido negativo, a no sufrir degradación ni humillación. El acoso, en sus diversas formas, atenta directamente contra este atributo. Su valor depende de la persona (fundamentalmente de su madurez) y de otras circunstancias. Si el valor se mide por las consecuencias de atentar contra ella, puede ser elevado, ya que no es raro que se produzcan daños a la salud y, en casos extremos, muerte por suicidio (22).

La *reputación personal* es un concepto que cualifica a la persona frente a los demás. Siguiendo la definición del diccionario de la Real Academia Española, la reputación es la opinión o consideración que se tiene de alguien, o bien el prestigio o estima en que esta persona es tenida. Es un concepto cualitativo: no se puede tener mucha o poca reputación, sino buena o mala; de hecho, no existe la reputación neutra. Una buena reputación personal es un importante activo que facilita la actividad de la persona que la posee. La reputación se construye por la persona mediante sus acciones frente a los demás, pero en la reputación también existe un componente que no depende del sujeto mismo, sino de cómo es visto por los otros. El valor de la reputación personal se mide por las consecuencias de su pérdida, que puede no depender de los actos de la persona sino de cómo son vistos por los demás.

Ya se ha hablado de la *reputación digital,* concepto similar al de la reputación personal pero aplicado a la identidad digital del individuo y a las diversas manifestaciones de esta. La reputación digital puede ser medida (23) mediante mecanismos de realimentación y puntuación existentes en las propias aplicaciones. De este modo y a diferencia de la reputación personal, no solo se tiene una buena o mala reputación digital, sino que se cuantifica la misma, lo que permite estimar su valor.

La *intimidad* es otro activo importante que debemos considerar, puesto que está directamente relacionada con la información sobre las personas[20]. La intimidad atañe al fuero interno de la persona y, como activo, consiste en poseer y mantener íntegro el control sobre los datos e informaciones que atañen a la esfera más privada, personal y familiar. El derecho a la intimidad personal está recogido en el artículo 18 de la Constitución Española. Con el advenimiento de la sociedad de la información, el ejercicio de este derecho ha sufrido un cambio (24). Anteriormente, lo importante era defender a la persona de las intrusiones en su intimidad, consideradas como un atentado a su libertad; ahora, el ciudadano digital asigna a la intimidad un valor social, superando el derecho a no ser

[20] Se puede asimilar, en términos generales, a lo que en el mundo anglosajón se conoce como *privacy*.

molestado. Por tanto, lo que requiere es controlar y tener conocimiento de las informaciones que le atañen como persona, decidiendo sobre la forma y contenido de su divulgación. El valor que la intimidad tiene como activo depende de factores muy subjetivos, llegando a ser muy pequeño cuando es la propia persona la que expone su intimidad de forma voluntaria atendiendo a diferentes motivaciones.

Cuando hablamos de *patrimonio* nos referimos a un activo real, formado por las posesiones materiales o derechos de la persona que poseen un valor de cambio mensurable. Dinero, valores mobiliarios e inmobiliarios, joyas, etc. constituyen activos cuyo valor es claro para el propietario y cuya necesidad de protección no necesita ser glosada.

Finalmente, denominamos *integridad legal* al atributo de la persona mediante el cual está libre de ser sujeto a procedimiento judicial o administrativo que le pueda acarrear sanciones o penas de cualquier tipo. La integridad legal supone que no existe razón para imputar a la persona ninguna actuación que contravenga las normas y legislación en vigor, ya sea en el lugar donde se encuentra físicamente o en otro país. Se trata, en principio, de un activo inmaterial. Sin embargo, una primera valoración de este activo vendría dada por las consecuencias que acarrearía la declaración de culpabilidad respecto a una determinada imputación. Hay que señalar que este activo reviste particular valor para la persona en los casos de robo de identidad, en los que puede verse obligada a pagar las consecuencias de la actuación del ladrón.

Podríamos hacer referencia a otros activos importantes que, finalmente, pueden verse afectados por acciones en el ciberespacio: la integridad psicológica y la salud en general. No obstante, parece que incluirlos en este análisis introduce demasiadas variables, pertenecientes a un ámbito que escapa de los límites del trabajo. Baste decir que, como ya se ha mencionado, en casos extremos se pueden producir graves daños a la salud o, incluso, la muerte (22). También hay que señalar que la evolución de las amenazas, en función de sus motivaciones (principalmente, búsqueda de beneficio), puede sacar a relucir activos «explotables» no contemplados aquí.

En el modelo adoptado en este capítulo, los activos anteriores se ubican en distintas posiciones. Por ejemplo, el equipamiento (*hardware*) se sitúa en la capa física del ciberespacio, en la interfaz con el mundo real. Los datos personales, identidad digital y reputación digital se encuentran en la capa semántica del ciberespacio. Finalmente, la identidad personal, reputación personal, integridad moral, patrimonio e integridad legal forman parte del que hemos convenido en llamar mundo «real».

Como se ha indicado anteriormente, conviene elaborar un árbol de activos para representar las relaciones entre ellos. Las ramas del árbol indican cómo el daño o pérdida de algún activo influye en los demás. Vamos

a denominar «degradación» al daño de un activo, que será del 100% en caso de que este se pierda o inutilice totalmente. Se puede empezar por una relación muy sencilla: la degradación del activo equipo físico puede conducir a la degradación, en un valor equivalente, del activo patrimonio. Otra rama sencilla de deducir sería la de considerar que la degradación por sustracción de datos personales puede llevar a la pérdida de la identidad digital, que conduce a la sustracción de la identidad personal y, de ahí, a posibles operaciones en el mundo «real» que desembocan finalmente en una pérdida económica, es decir, una degradación del patrimonio, o bien en la posibilidad de ser acusado de una falta o delito, o sea, a la degradación de la integridad legal. En la figura 2.6 se representa el desarrollo del árbol de activos, que muestra las principales relaciones que se pueden establecer, suficientes para los fines de este trabajo. No se han mostrado todas las posibles ramas ya que algunas solo tienen un interés residual.

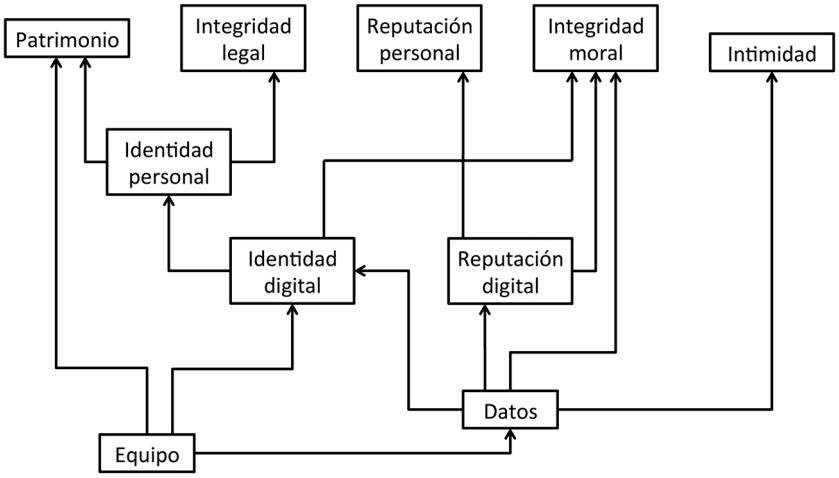


Figura 2.6: Árbol de activos.

Amenazas

Al considerar las amenazas debemos hablar en términos de acción. Las amenazas son sucesos formados por cadenas de eventos relacionados entre sí en el tiempo y en el (cíber) espacio. Como resultado de estos sucesos se produce una degradación de los activos.

La posibilidad de que una amenaza se produzca, es decir, de que el suceso asociado se materialice, da lugar a una vulnerabilidad determinada sobre una rama del árbol de activos: si es muy posible que el suceso se

produzca, la vulnerabilidad es grande; por el contrario, si el suceso es poco posible o improbable, la vulnerabilidad es escasa o nula. Por otro lado, el daño o degradación producido por la realización de una amenaza constituye el impacto de esta[21]: hay amenazas que producen poco impacto, porque el daño es pequeño y los activos afectados se pueden reponer fácilmente; otras, por el contrario, son realmente destructivas. En el apartado anterior se ha discutido sobre la manera de valorar los activos para estimar el impacto. También se ha hablado anteriormente sobre cómo adoptar medidas para reducir el riesgo[22].

Para caracterizar las amenazas es preciso fijarse, primeramente, en dónde se sitúan los activos (al decir «dónde» hablamos en términos de ciberespacio y no del espacio ordinario). Aunque no lo parezca, la situación del activo reviste una gran importancia. En efecto, cualquier vector de ataque tiene su punto de aplicación en un arranque de una cadena de activos. Los procedimientos y técnicas de ataque dependen, necesariamente, de la posibilidad de acceder a este arranque, por lo que el tipo de ataque dependerá de dónde se sitúa el primer activo. Protegiéndolos se reducirá, por tanto, la «superficie de ataque» que se presenta, lo que es esencial en una defensa en profundidad de los activos. Para nuestros propósitos, se puede decir que los activos que forman el inicio de cada rama del árbol de activos se sitúan, en general:

- Sobre la persona. La persona es en sí un repositorio de información que puede o no estar compartida con la capa semántica del ciberespacio. También hay activos (p. ej. la integridad moral) que radican sobre la persona de forma intrínseca.
- En soportes físicos de datos. Estos soportes varían desde una nota adhesiva, con un nombre de usuario y contraseña apuntados, hasta un listado de ordenador de varios cientos de páginas con datos personales. La información que contienen pertenece a la capa semántica del ciberespacio, pero una persona puede acceder a ella directamente por sí misma.
- En soportes lógicos removibles. Pueden ser llaves USB, discos duros extraíbles, disquetes, CD, DVD, etc. Una vez introducidos en los sistemas, forman parte de la capa física, pero la información que contienen puede pertenecer a la capa sintáctica (p. ej. programas ejecutables) o a la semántica (p. ej. datos personales, fotografías, etc.). Por tanto, constituyen un excelente vector para diversos tipos de ataque[23].

[21] Por ejemplo, los activos son poco vulnerables ante un ataque de seres extraterrestres. Sin embargo, tal ataque, en el caso improbable de producirse, podría tener un efecto (impacto) devastador.

[22] Ver figura 2.2 y figura 2.3.

[23] Por ejemplo, el ataque a las centrifugadoras iraníes mediante el gusano *Stuxnet*, que fue introducido mediante soportes removibles. Ver el informe de Symantec en (38)

– En medios de tratamiento de la información. Aquí se consideran todos los sistemas y equipos que puede poseer una persona. La principal distinción que debemos considerar es la relativa a la movilidad o portabilidad del equipo, ya que no es lo mismo un ordenador personal de sobremesa ubicado en el domicilio que un *smartphone*. La diferencia se refiere, fundamentalmente, a la mayor posibilidad de acceder físicamente al equipo móvil, robándolo, por ejemplo.

Lo anterior nos muestra dónde se deben poner obstáculos a los atacantes. En una estrategia defensiva, estos son los puntos que se deben proteger en primer lugar, y las acciones de concienciación deben hacer hincapié en recordar su importancia a la hora de reducir las vulnerabilidades.

Una vez conocidas las ubicaciones de los activos, es importante considerar los principales mecanismos que permitirán acceder a ellos y materializar las distintas amenazas.

No se deben olvidar los orígenes no conscientes de ataques, cuya acción se materializa en amenazas que pueden resultar muy destructivas. Una catástrofe natural (p. ej. inundación o terremoto) puede producir la destrucción de los equipos y la pérdida de los datos o, simplemente, la indisponibilidad temporal de estos; la vulnerabilidad dependerá de las circunstancias geográficas y físicas del lugar. Por otro lado, una avería del equipo, de la instalación eléctrica o de agua también puede causar este mismo tipo de daños. Se incluye en este tipo de amenazas la rotura por accidente de los equipos o el manejo por personas sin conocimientos con las mismas consecuencias. Ante estas amenazas, se deben adoptar medidas preventivas de vigilancia, precaución en la ubicación y manipulación, protección ante sobretensiones, uso de fuentes de alimentación ininterrumpidas, etc. La medida más importante para reducir el impacto de estas amenazas es la realización de copias de respaldo regulares, con el almacenamiento de la copia en lugar seguro.

Los *insiders* no suelen ser un origen de ataque común para las personas consideradas individualmente. Sin embargo, determinadas circunstancias personales o familiares pueden hacer más probable la amenaza de ataques por personas del entorno próximo que gozan de acceso a los equipos. En estos casos, las medidas más recomendables son las preventivas, basadas en un estricto control de acceso físico y lógico, sin descuidar la realización de copias de respaldo.

Lo primero que viene a la mente al hablar de amenaza en el ciberespacio es un ataque que infecta los equipos produciendo efectos catastróficos. La infección mediante código (o *software*) dañino (o malicioso), conocido

y la investigación sobre este ataque en el artículo de Zetter (2011) para *Wired.com* (39). También se atribuyó oficialmente (43) un origen similar al ataque sufrido en 2008 que afectó a sistemas del Mando Central de EE. UU. (USCENTCOM).

en inglés como *malware*[24], es, en general, la amenaza más conocida y a la que se atribuyen los peores efectos. Sin quitarle la importancia que merece, no es la única y, a veces, tampoco es la más dañina.

Se llama código dañino o *malware* a un programa o a una pieza de código ejecutable que produce cambios en el funcionamiento correcto de un equipo informático, dañándolo o apoderándose de él con intención maliciosa. La característica fundamental del código dañino es que causa un funcionamiento incorrecto del sistema infectado porque produce cambios en el entorno (sistema operativo, memoria, datos, sistema de archivos) o en los programas instalados (25). Otra característica del código dañino es su tendencia generalizada a extenderse, infectando nuevos sistemas por diversos procedimientos. Una clasificación general del código dañino sigue el criterio de si tiene existencia autónoma y puede ejecutarse por sí mismo (independiente) o si necesita para ejecutarse de un programa u objeto anfitrión (código dañino embebido).

Los representantes más significativos de *software* dañino independiente son los gusanos (*worm*). Los gusanos son programas cuya principal característica es su capacidad de reproducirse y propagarse masivamente usando distintos medios. Esto hace que consuman muchos recursos de la máquina y de la red, lo que provoca un descenso en el rendimiento de los sistemas. Pueden o no provocar daños por sí mismos en el equipo y se usan también para transportar otros tipos de código dañino, como troyanos.

Dentro del código dañino embebido distinguimos:

- Virus. Se trata del primer tipo del código dañino conocido[25]. Los virus se caracterizan por producir daño al equipo y por reproducirse a fin de propagarse, y el daño producido puede variar entre causar molestias o hacer inutilizable el equipo. El anfitrión o huésped donde se alojan puede ser muy variable: un archivo ejecutable, el sector de arranque o incluso la memoria del ordenador.
- Caballos de Troya o troyanos. Simulan ser un programa o archivo útil para el usuario, que los abre y permite la ejecución oculta del troyano. Suelen ser juegos, programas, videos, imágenes o archivos de audio. A diferencia de los virus, los troyanos no se replican a sí mismos, por lo que precisan otros mecanismos de dispersión. Hay muchas clases de troyanos, según el fin que persigan[26]. Los tipos más importantes son:

[24] *Malware* es la contracción de *malicious software*.

[25] El primer virus con las características de un verdadero código dañino fue *Creeper*, creado por Bob Thomas en el año 1971 y escrito como una demostración para atacar al sistema operativo Tenex. Sin embargo, el primer virus que tuvo una expansión real fuera del laboratorio fue *Elk Cloner*, que atacaba las máquinas Apple II y fue creado en 1982 por un adolescente llamado Rich Skrenta.

[26] Según el Informe Anual de Seguridad 2012 de Panda Security, el 76,56% de los ataques de código dañino en 2012 fue causado por troyanos.

- Bot. Un troyano bot se usa para crear botnets. Actualmente, las botnets constituyen la amenaza más ampliamente difundida y seria entre las distintas clases de código malicioso. Una botnet es una red formada por un conjunto de ordenadores (llamados bots o zombis) que han sido infectados con un tipo de software malicioso, con funcionalidad de «puerta trasera», que permite a un atacante controlar remotamente dichas máquinas sin el conocimiento del propietario. El atacante ejerce el control de la botnet por medio de una infraestructura de servidores llamados de «mando y control». Cada red puede estar formada por decenas de miles de ordenadores infectados, proporcionando estas redes a los atacantes una plataforma distribuida para realizar ataques a mayor escala. Entre estos, se cuentan algunos de los que se verán más adelante, como distribución de malware, ataques de denegación de servicio distribuido[27] contra determinados objetivos, correo masivo, suplantación de identidad, etc. La creación y mantenimiento de botnets se ha convertido en un negocio en sí mismo, ya que pueden ser comercializadas alquilándolas a organizaciones o individuos como instrumento para sus propósitos delictivos. Las cifras relativas a las infecciones por botnets se incrementan continuamente, de forma que, según el informe del cuarto trimestre de 2012 de Kindsight (26), cuatro de las cinco principales amenazas de malware de ese año fueron infecciones de botnets y casi el cincuenta por ciento de las redes domésticas infectadas tenían un problema de este tipo. Puesto que un ordenador zombi puede estar realizando una actividad ilegal sin conocimiento de su propietario, este tipo de ataque es doblemente nocivo, ya que a los daños producidos a la víctima se pueden sumar las posibles responsabilidades exigidas o, al menos, la necesidad de demostrar que la actividad ilegal no era intencionada.
- Puerta trasera. Permiten al atacante conectarse al equipo infectado de forma remota, de manera que puede realizar diversas acciones (p. ej. enviar correos, ejecutar programas, crear servidores *web*, etc.).
- Descargador (*downloader*). Su función principal es la de descargar otros archivos dañinos, así como de preparar la máquina para su ejecución automática al arranque o de ejecutarlos tras la descarga.
- *Rootkit*. Los *rootkit* son un conjunto de herramientas que permiten mantener oculta la actividad del *software* dañino en un equipo. To-

[27] Un ataque de denegación de servicio distribuido utiliza los equipos de la *botnet* para generar una cantidad enorme de peticiones a un servicio (p. ej., una página web), de forma que este no dé abasto para responderlas, se sobrecargue y quede inoperativo. De esta manera, los legítimos usuarios del servicio quedan privados de él.

man el control del sistema operativo con los máximos privilegios y hacen muy difícil su detección y remoción.

- *Proxy*. Permiten al atacante utilizar el equipo infectado como un servidor *proxy*[28]. Sirve como paso intermedio para otro ataque, cuyo origen real no se puede determinar.
- *Ransomware*. Este tipo de troyanos «secuestra» el equipo, ya sea impidiendo acceder a él o cifrando los archivos de datos. Al mismo tiempo, exige una cantidad en concepto de rescate para recibir una clave que restablezca el uso normal del ordenador[29].
- *Keylogger*. Son usados para detectar y registrar las pulsaciones del teclado en los equipos y así obtener información sensible. Una variante son los ladrones de contraseñas (o *password stealer*) que están específicamente programados para robar información introducida en formularios web. Los datos recogidos se remiten por distintos medios al atacante.
- Bancario o financiero. Están especializados en buscar y enviar al atacante datos bancarios, de tarjetas, etc., almacenados en el equipo de la víctima. Frecuentemente utilizan herramientas de *rootkit* para pasar desapercibidos el mayor tiempo posible[30].
- *Dialer*. Crean conexiones telefónicas en el equipo, utilizando las funcionalidades del módem, o bien envían mensajes SMS suscribiéndose a servicios de alto coste. Tuvieron una primera difusión cuando el acceso a Internet se realizaba con módem telefónico. La generalización de la banda ancha los hizo inútiles por un tiempo, pero la proliferación de teléfonos móviles inteligentes (*smartphones*) les ha dado un nuevo uso. Por eso también son conocidos actualmente como «troyanos *premium SMS*».

– Bombas lógicas. Comparten características de virus y troyanos en el sentido de que necesitan un programa anfitrión; sin embargo, no se reproducen ni actúan continuamente. Permanecen inactivas hasta que algún evento (una fecha, una determinada cantidad de ejecuciones del programa anfitrión, etc.) hace que se ejecuten. Pueden producir serios daños, aunque no están muy extendidas.

Esta clasificación es útil para orientarse inicialmente en el amplio dominio del *malware*. Sin embargo, hay otros tipos de código dañino menos

[28] Un *proxy* es un ordenador que da acceso a otros ordenadores a las redes. El atacante utiliza el ordenador infectado como *proxy* para enmascarar su identidad, accediendo a Internet a través de él.

[29] El más conocido en la actualidad es el «virus de la Policía» o «virus *Ukash*».

[30] El más famoso y aún activo troyano bancario es Zeus, aparecido en 2007 y responsable, junto con sus variantes, de haber infectado a más de 400.000 ordenadores en 2012, según S*ymantec* (48).

significativos que no se han citado. Por otra parte, existen piezas de código dañino que mezclan características de varios tipos o que sirven para transportar unos a otros. Finalmente, el mundo del código dañino está en continua evolución y cada vez aparecen nuevos ejemplares, muchas veces de características desconocidas hasta la fecha.

Las vías para infectar los equipos incluyen ataques desde sitios web legítimos pero infectados (*drive-by exploit*), redes inalámbricas, exploración (*scan*) o gusanos exploradores (*scanning worm*). Sin embargo, la principal vía de infección por código dañino es la ingeniería social, por ser la más extendida y la más eficiente, al tiempo que la más tradicional.

Se conoce como ingeniería social, en el contexto de la seguridad de la información[31], al uso de técnicas persuasivas que consiguen engañar al individuo, llevándole a revelar datos o realizar acciones que pueden conducir a la materialización de una amenaza. Se basa en el concepto, generalmente aceptado, de que el factor humano es el eslabón más débil de la cadena de seguridad[32] y de que se pueden explotar tres rasgos presentes en el ser humano: el miedo, la confianza y la inconsciencia (o inadvertencia).

Las técnicas de ingeniería social han sido usadas durante siglos (27) en el ámbito de la política, la diplomacia y la inteligencia. El término, aplicado a la violación de la seguridad de los sistemas de información, fue popularizado en los años 90 del pasado siglo por Kevin Mitnick, uno de los más famosos *hackers* modernos. Arrestado por última vez en 1995, fue puesto en libertad en 2000, fundó su propia empresa y se dedica, desde entonces, al asesoramiento en materia de seguridad de la información, dar conferencias y escribir libros, de los que el más conocido es *El arte de la decepción* (28).

Aunque carente de formación académica en psicología, su experiencia y demostrada eficacia hacen de Mitnick un reconocido experto. En su opinión, la ingeniería social es un arte que se basa en unos pocos principios. El primero es que, ante alguien que se presenta en situación de necesidad, la tendencia es generalmente la de intentar ayudar. De ahí se llega al segundo, que preconiza que el primer movimiento ante otra persona normalmente es de confianza. El siguiente es que las personas se sienten incómodas ante la tesitura de tener que decir «no» a algo que se les demanda. Finalmente, un principio bastante aceptado es que a todo el mundo le gustan las alabanzas. A pesar de parecer obvios y estar expresados casi en un lenguaje de manual de autoayuda, estos principios tienen una indiscutible base empírica. Por su sencillez y reducido número, conviene que sean tenidos en cuenta en los programas de formación y

[31] En otros contextos, se refiere a la planificación del desarrollo económico y social.
[32] Estudios como el del Ponemon Institute de 2012 confirman esta percepción (42).

entrenamiento, que, como veremos, son la mejor medida para enfrentarse a la ingeniería social.

El estudio científico de las técnicas persuasivas comenzó en la primera mitad del siglo XX. Desde entonces, se han sucedido numerosos estudios sobre cómo una persona puede modificar o condicionar comportamientos y actitudes en otros. Robert B. Cialdini es un conocido psicólogo social y escritor, considerado como uno de los principales estudiosos de la psicología de la persuasión. En su libro *Influence* (29), y en otras publicaciones (30), Cialdini expuso las seis tendencias que entran en juego para provocar la respuesta buscada en el comportamiento del otro. En definitiva, equipara la ingeniería social a la ciencia de la influencia e identifica recursos psicológicos aplicables, con una base científica. Las seis tendencias que Cialdini propone como básicas son:

- Reciprocidad, según la cual, si se asocia a una petición el ofrecimiento o la promesa de algo, se dispara una respuesta positiva ante la petición. Lo que se ofrece o promete no tiene que ser algo material; puede ser un favor o un consejo. Es una manera sutil de hacer al otro sentirse «en deuda», lo que facilita obtener algo de él.
- Coherencia, que significa que las personas tienden a ser consecuentes con sus afirmaciones o compromisos expresados con anterioridad. La utilización de esta técnica exige obtener del otro, previamente, una afirmación que le comprometa con un concepto positivo. Posteriormente, se le pedirá algo que aparecerá relacionado con lo anterior, y que se verá impelido a hacer, ya que querrá ser considerado como una persona «formal y consecuente» en sus actos.
- Conformidad social, que implica la tendencia a actuar de la manera que nos piden si sabemos, directa o indirectamente, que ello está en línea con la actuación de los demás. El hecho de pensar que otros muchos actúan de una determinada manera nos hace creer que es la correcta por estar validada socialmente.
- Simpatía, que comprende »gustar», «afecto», «buena relación», «afinidad» y otros conceptos similares. Significa que las personas tienen tendencia a satisfacer las peticiones procedentes de alguien que les gusta, con el que han congeniado o con el que se sienten identificadas por sus creencias o actitudes. El atractivo físico o los halagos pueden jugar aquí su papel.
- Autoridad, según la cual las personas tienden a hacer lo que les demanda alguien que está situado en una posición de autoridad. Esta autoridad no tiene que ser necesariamente la derivada de una jerarquía organizativa, sino que puede ser relativa a títulos académicos, conocimientos, experiencia, relevancia social o, incluso, apariencia

física. Lo importante en el uso de esta tendencia es crear en el otro la percepción de autoridad[33].

– Escasez, por la que el conocimiento de que un bien es escaso o de que estará disponible durante poco tiempo, dispara la tendencia a obtenerlo. El bien puede ser material o inmaterial y la persona a la que se da a conocer su existencia no tiene por qué necesitarlo, ni aun saber de antemano que existe. Se trata, primero, de hacer creer al otro en la existencia real del bien y, luego, de convencerle de que, para su posesión, compite con otros o contra el tiempo y, si no se da prisa, lo perderá.

No es posible ni conveniente intentar una enumeración exhaustiva de las técnicas de ingeniería social. En primer lugar, hay muchas que ocupan nichos específicos, de poco interés para el individuo; en segundo, continuamente aparecen nuevas técnicas que se adaptan a los cambios de los comportamientos de las personas en el ciberespacio; finalmente, se puede decir que cada atacante experto acaba por desarrollar las suyas propias. Sin embargo, se puede intentar clasificar las técnicas (o grupos de técnicas) más significativas a fin de obtener un panorama general de lo que se denominaría «avenidas de ataque» en lenguaje militar. De esta manera, podemos hablar de técnicas pasivas, en las que el atacante no realiza ninguna interacción con la víctima ni con su entorno, y de técnicas activas, que requieren una interacción del atacante con la víctima, con su entorno o con sus pertenencias. Estas pueden ser directas, cuando se requiere una presencia del atacante y una relación en «tiempo real», aunque sea mediante medios técnicos (como el teléfono) o indirectas, si la interacción no es presencial, con lo que normalmente se realizará a distancia, utilizando la tecnología.

Las principales técnicas pasivas se basan en la observación y la escucha. A veces, se emplean medios específicos, como cámaras, lectores de tarjetas camuflados[34] o programas de ordenador que escuchan el tráfico de redes *Wifi* abiertas (aeropuertos, cafeterías, centros comerciales, etc.). Normalmente, los atacantes se limitan a situarse en una situación ventajosa y esperar la oportunidad, aunque a veces emplean tácticas de distracción que facilitan la obtención de información. Lo importante es que el atacante no establece con la víctima ninguna relación con contenido informativo; todo lo más, debe dar la impresión de un encuentro totalmente fortuito. Entre las más utilizadas y rentables destaca el fisgar (*shoulder surfing*) cuando alguien introduce contraseñas u otros datos en

[33] Hay veces que verdaderos expertos asumen equivocadamente que los otros reconocen y aprecian espontáneamente su experiencia, sin darse cuenta de que la posición de autoridad hay que ganarla.

[34] Estos lectores permiten obtener los datos de la tarjeta para luego clonarlos, lo que se conoce como *skimming*. A veces es necesaria la intervención humana en persona, en forma de dependiente o empleado de un comercio, restaurante, etc.

ordenadores, cajeros automáticos, controles de acceso, etc. Otra técnica muy usada es la de escuchar conversaciones[35] entre personas, que se seleccionan por su acceso a determinados datos. En otras ocasiones, se trata de objetivos de oportunidad (p. ej. una nota adhesiva con una contraseña apuntada, un cibercafé en el que alguien ha dejado una sesión de correo web abierta, etc.), por lo que el atacante deberá poseer dotes de observación, paciencia y capacidad de improvisación.

Entre las técnicas activas directas, que exigen una presencia o una interacción en tiempo real, destacan las siguientes:

- Impostura. El atacante plantea un escenario creíble, basado a veces en información previa obtenida sobre la víctima. Utilizando una de las tendencias psicológicas vistas anteriormente, la convence para que revele datos sensibles (credenciales, números de cuenta bancaria, números de identificación, tarjetas de crédito, etc.) o para que realice alguna acción (enviar un correo electrónico, conectarse a una página de Internet, descargarse un archivo, etc.). Exige una preparación previa y una capacidad de interacción alta para responder adecuadamente a la evolución de la situación. Se puede realizar en persona, pero es más arriesgado; la forma más extendida es mediante una o varias llamadas telefónicas que siguen el guión de la farsa preparada. El uso del teléfono es, también, la forma más antigua y hunde sus raíces en los tiempos de los primeros *phreackers*[36], cuando aún no se había extendido el uso de redes y sistemas informáticos por el público. Actualmente, se está incrementando el uso de otros medios como IRC[37], mensajería instantánea[38] y redes sociales.
- Ingeniería social inversa. Comparte con la impostura la creación de un personaje que se reviste de autoridad, generalmente de carácter técnico. El punto de partida es provocar un fallo en algún sistema o servicio (sabotaje). Presentándose como alguien capaz de resolver el problema, el atacante hace que sean las víctimas las que le ofrezcan los datos que desea obtener. Una vez que repara el fallo que él mismo causó, nadie siente haber dado información indebidamente, puesto que era necesaria para solucionar un problema.

[35] En inglés, se denomina a esta técnica *eavesdropping* y, utilizada con constancia a lo largo de cierto tiempo, puede proporcionar un importante volumen de información, sobre todo relativa a corporaciones o instituciones.

[36] El *phreacking* consiste en atacar sistemas de telecomunicaciones para utilizarlos de manera gratuita. El término se originó en la década de los 70 del siglo XX.

[37] IRC (*internet relay chat* o conversación en tiempo real a través de Internet) es un protocolo de comunicación basado en texto sobre TCP/IP que permite conversaciones en tiempo real entre dos o más personas que comparten lo que se denomina un «canal», dedicado a una materia en particular (46).

[38] La mensajería instantánea se diferencia del IRC en que es necesario autorizar, de antemano, que el corresponsal o corresponsales inicien la comunicación.

– Recogida de elementos desechados *(dumpster diving)* arrojados a la basura, papeleras, olvidados en lugares accesibles o perdidos. Los elementos que se desechan pueden contener información muy útil para los atacantes (direcciones, números de cuenta bancaria, de documentos de identidad, fechas, etc.). Estos elementos pueden ser papeles personales, correspondencia privada o de distintas entidades, equipos que se tiran, viejos CD, etc. Esta técnica es más frecuente en las corporaciones o instituciones, ya que el volumen de datos que se pueden obtener es muy rentable.

Entre las técnicas activas indirectas hay que considerar dos tipos: las que podrían denominarse de entrada o iniciales, que constituyen el primer contacto con la víctima, y las posteriores o subsiguientes, que utilizan las anteriores para ganar acceso y luego ejecutar el ataque. Entre las iniciales destacan:

– Correo masivo. Se denomina correo masivo o *spam* a todo correo no deseado recibido por el destinatario procedente de un envío automatizado y masivo por parte del emisor. El *spam* generalmente se asocia al correo electrónico personal, pero no solo afecta a los correos electrónicos personales sino también a foros, bitácoras[39] y grupos de noticias. Para el envío de los mensajes se usan, principalmente, *botnets*, así como técnicas dinámicas que dificultan notablemente conocer el verdadero origen del mensaje. Los mensajes pueden contener archivos adjuntos, enlaces a páginas *web*, texto (a veces sin ningún sentido) o incluso estar vacíos. Normalmente se usan para publicidad de productos o servicios, legales o no. El asunto más común (78,13%) de estos correos está relacionado con contenido sexual o citas, seguido a distancia (14,20%) por productos farmacéuticos; les siguen a mucha distancia ofertas de trabajo, relojes y apuestas (31). El que envía un mensaje de este tipo utiliza resortes de los ya tratados para que el destinatario realice una acción: ir a la página *web*, abrir el archivo adjunto, responder, etc. Estas acciones conducen a lo que hemos denominado técnicas subsiguientes, con resultado de: pérdida de datos, robo de identidad, estafa, infección y pérdida de control sobre el equipo informático, transformación en un miembro de una *botnet*, etc. Evidentemente, la mejor manera de luchar contra el *spam* es no abrir nunca correos de remitentes desconocidos, tener instalado un antivirus y disponer de un filtro *antispam* en el cliente o servicio de correo electrónico. El *spam* que utiliza el correo electrónico tiende a disminuir; en su lugar, se incrementa la utilización de los medios sociales, entre los que destaca la infiltración en redes sociales o el colgar comentarios en bitácoras. También se ha apreciado un incremento en el uso de operadores de redes de móviles, así como del *spam* en los mensajes cortos o SMS. Otros canales usados son IRC, mensajería instantánea y, en menor medida, fax.

[39] Los populares *blogs*, según su denominación en inglés.

– Buscadores envenenados o *search-engine poisoning* (SEP). Es una de las técnicas preferidas por los atacantes para infectar las máquinas de las víctimas[40]. Consiste en manipular los buscadores (p. ej. Google, Bing o Yahoo) para que, al dar al usuario los resultados de una búsqueda, sitúen enlaces[41] a sitios web maliciosos en los primeros puestos de la lista. El usuario pulsa en alguno de estos enlaces, es dirigido a uno de estos sitios y su máquina queda infectada. Es difícil defenderse contra esta técnica porque requiere por parte del usuario prestar atención a los enlaces y detectar posibles irregularidades, lo que necesita mucha formación. La mejor defensa radica en las medidas que apliquen los propios buscadores para defender a sus usuarios.

– Uso de cebos *(baiting)*. Consiste en dar o poner al alcance de la víctima, aprovechando alguna de las tendencias estudiadas, un soporte lógico removible. Lo más común es, simulando una situación creíble (una promoción publicitaria, un olvido, un regalo de material sobrante, etc.), dejar que la víctima se haga con una llave USB con un logo corporativo realista. También puede ser un DVD con la última película estrenada «pirateada». Cuando estos medios se introducen en el equipo, lo infectan y extienden la infección a otras máquinas. Normalmente, aprovechan la característica de ejecución automática *(autorun)* de medios extraíbles del sistema operativo[42]. Evidentemente, la mejor defensa es no fiarse nunca de material que tenga una procedencia semejante y no introducirlo en los equipos.

– Redes de intercambio de ficheros (redes *peer-to-peer* o P2P). Se trata de redes distribuidas en las que no existe ningún tipo de control central ni de estructura jerárquica. Actualmente son el medio más utilizado para compartir ficheros y descargar material de diverso tipo desde Internet. El origen de los ficheros que se descargan no se conoce, por lo que es posible que incorporen algún tipo de código dañino. Un atacante puede disfrazar el nombre y extensión de un fichero, haciéndolo atractivo para la víctima, de forma que esta lo descarga en su equipo, que puede quedar infectado al abrir el fichero. También pueden contener material cuya posesión esté castigada por la ley.

Una vez aplicada con éxito una técnica inicial, se empleará una técnica subsiguiente, de las que las más importantes son:

[40] Según el informe de 2012 de Blue Coat Systems (50), el 40% de entradas a sitios *web* maliciosos fueron provenientes de una búsqueda y 1 de cada 142 búsquedas llevó a un sitio *web* malicioso.

[41] A veces, los buscadores muestran unas cantidades astronómicas de resultados (la búsqueda del término «*love*» en Google da 1.620.000.000 resultados), lo que desalienta al usuario y hace que se centre en la primeras páginas.

[42] Según el informe de 2012 de ENISA (47), el troyano *Autorun*, utilizado para propagar infecciones a través de medios extraíbles, es uno de los dos más extendidos mundialmente (el otro es *Conficker*).

– Suplantación de identidad o *phishing*. En la forma más corriente, la víctima recibe un correo supuestamente enviado por una entidad (generalmente un banco) realmente existente, cuyos servicios usa habitualmente. El correo ha sido enviado por el atacante y es falso, pero su apariencia es realista, logrando confundir a la víctima. Esta queda convencida por el correo de que, para resolver un supuesto problema, debe acceder al servicio pulsando en un enlace. A continuación, es redirigida a una página web falsa controlada por el atacante, pero prácticamente indistinguible del sitio web verdadero de la entidad. Una vez allí, se le pide que proporcione información privada para entrar en la página. La víctima accede a ello y proporciona los datos, que quedan en poder del atacante que envió el correo. Según los datos que se obtengan, la pérdida económica posterior puede ser elevada. La tendencia a desplazarse a las redes móviles ha hecho aparecer técnicas de *phishing* vía mensajes cortos (SMS), con mecanismos parecidos. Otro medio empleado es el phishing sobre voz (o *vishing*), que utiliza servidores vocales automáticos, simulando ser legítimos, para convencer a clientes de servicios telefónicos (p. ej. banca) para que digan o tecleen información sensible con el fin de resolver un supuesto problema. Finalmente, otra técnica aprovecha la proliferación de redes wifi: se activa un punto de acceso *Wifi* abierto, con un nombre de red que induce a confusión y parece de un servicio o institución pública. Los que se conectan a esta red en abierto pueden iniciar sesiones en distintos servicios. Las contraseñas y otra información sensible se transmiten sin cifrar por la red *Wifi*[43], siendo recogida por el atacante que controla el punto de acceso y registra todo el tráfico de datos.

– Fraude electrónico o *scam*. El fraude electrónico es una versión de los «timos» de siempre y representa la verdadera esencia de la ingeniería social. Como variantes principales citaremos:

  • Fraude con tarjetas de crédito duplicadas, mediante el que se adquieren bienes o se obtiene dinero de cajeros automáticos con tarjetas duplicadas. Está asociado al *phishing* o al *scamming*.

  • Esquemas piramidales, que son una transposición de los tradicionales, pero en los que se utilizan las enormes capacidades de Internet para alcanzar un elevado número de potenciales víctimas[44]. Detrás de una gran parte de «cadenas de correos» se encuentra un fraude de esta naturaleza.

[43] Según el *Informe sobre ciberdelincuencia 2012* de Norton, el 24% de los usuarios emplean conexiones *Wifi* potencialmente inseguras para transacciones bancarias por Internet, el 67% acceden a su correo personal y el 63% inician sesión en sus cuentas de redes sociales (de los que un tercio no cierra su sesión al terminar).

[44] Son esquemas de tipo Ponzi, de los que el que se puede considerar pionero y más conocido es el denominado *Make Money Fast*, fichero de texto que fue colgado en 1988 en una BBS de Maryland por alguien usando el nombre de Dave Rhodes.

    - Pago por adelantado, conocido también como el «419» o la «estafa nigeriana». En su expresión primaria, consiste en ofrecer, mediante un correo electrónico, una gran suma de dinero. Si la víctima responde, se le enviarán «pruebas oficiales» de la fortuna que recibirá. Posteriormente, se conseguirá que pague por variados conceptos (tasas, gastos bancarios, honorarios, comisiones o sobornos) antes de recibir la millonaria transferencia, que nunca llegará. Hay variaciones en los pretextos para ofrecer el dinero, entre las que destacan: refugiado político que necesita sacar dinero de un país, obras de caridad que necesitan ayuda para distribuir dinero, una herencia que se pierde, un premio de lotería, dinero mal obtenido que busca redención, magníficas y bien remuneradas ofertas de trabajo, desastres naturales o guerras, etc.

– Infección directa por código dañino. Es una de las más probables consecuencias de abrir ficheros adjuntos a mensajes *spam* en todas sus formas. Los cebos y las descargas en redes P2P también causan este efecto.

– Infecciones por sitios web. Existen las denominadas «redes de *malware*» *(malnet)*, formadas por servidores que están controlados por organizaciones dedicadas a distribuir código malicioso, entre otras actividades. Cuando, por una técnica primaria, se consigue que la víctima siga un enlace a una de estas web, su equipo será infectado. En otros casos, habrá sitios web legítimos, pero vulnerables, que resultan comprometidos por los atacantes: al acceder la víctima a uno de estos sitios, sufrirá un ataque del tipo *drive-by download*, que aprovechará las vulnerabilidades del navegador de su máquina y descargará en ella código dañino. Nótese que, en este último caso, la víctima no tiene que seguir ningún enlace a sitios maliciosos sino simplemente visitar una página web legítima, lo cual es más fácil de conseguir. La condición, sin embargo, para que este último tipo funcione es que el equipo de la víctima tenga vulnerabilidades, es decir, que no tenga al día las actualizaciones de seguridad.

La ingeniería social se mantendrá como una de las principales técnicas para realizar o iniciar ataques. Ello se debe, en primer lugar, a su gran eficiencia, que permite obtener importantes efectos con recursos modestos. Por otro lado, es una manera útil para sortear las (a veces costosas) medidas técnicas implantadas para proteger los equipos y los datos. Además, se basa en atacar el punto más débil de la cadena de seguridad, lo que incrementa las posibilidades de éxito. Finalmente, tiene una gran capacidad de evolución y de adaptación a las nuevas situaciones. La defensa contra la ingeniería social se basa en una inteligente política de uso de los sistemas, en la buena práctica en el empleo de los medios y en la educación para detectar y reaccionar casi automáticamente ante estas técnicas.

Los sistemas móviles merecen una especial atención debido, esencialmente, al enorme incremento que tiene su utilización y a sus características propias. Se trata de los ordenadores portátiles, tabletas (*tablets*) y teléfonos móviles inteligentes, fundamentalmente de estos últimos, por su tamaño y crecimiento en número[45]. Desde el punto de vista de la seguridad, debemos considerar varios factores que inciden negativamente:

- Utilizan como soporte de transmisión canales poco seguros, como GSM o NFC[46], o inseguros, como *Wifi* o *Bluetooth*.
- Los sistemas operativos y las aplicaciones no han alcanzado un adecuado grado de madurez en cuanto a la seguridad. El mercado de aplicaciones ha estado poco controlado desde ese punto de vista.
- Los operadores de telecomunicaciones no han evolucionado, desde la perspectiva de la seguridad, al compás de los avances en los terminales.
- Los usuarios abarcan un gran abanico de edades e incluyen grupos con escasos conocimientos tecnológicos y con poca concienciación sobre seguridad, lo que los convierte en blancos atractivos.
- Precisamente por ser móviles y fácilmente transportables, son muy susceptibles de ser perdidos o robados[47], lo que proporciona al atacante acceso directo a la información.
- El incremento del ancho de banda de las telecomunicaciones móviles hace más fácil que las amenazas antes reservadas para los ordenadores personales «emigren» a estas plataformas móviles.
- Ciertos aspectos, como las técnicas de geolocalización, utilizan tecnologías inalámbricas y medios satélite, como GPS. Atacando el soporte de transmisión por técnicas de ingeniería social o atacando al proveedor de servicio, se puede hacer un seguimiento completo de la posición geográfica de la víctima.
- Son el punto de entrada mayoritario a los medios sociales, especialmente a las redes sociales, lo que produce un efecto cruzado en el que las vulnerabilidades de unos y otros se potencian.

[45] Según el Instituto de Tecnología de Georgia (EE. UU.), en 2012 el número de teléfonos móviles inteligentes vendidos superó al número de ordenadores personales vendidos. Así mismo, ese año los teléfonos móviles inteligentes constituyeron la vía más popular de acceso a Internet.

[46] GSM (*Global System for Mobile communications*) es el estándar de telefonía móvil digital actual. La evolución en curso a sistemas de 3.ª y 4.ª generación hará más seguro el soporte de transmisión.
NFC (*Near Field Communication*) es un sistema basado en inducción magnética y emisiones radioeléctricas de alta frecuencia con un alcance muy corto (normalmente, un máximo de 10 cm.). Se usa, fundamentalmente, para pagos, pero se están desarrollando otras muchas aplicaciones.

[47] Según el *Informe sobre ciberdelincuencia 2012* de Norton, un 35% de los adultos perdió o sufrió el robo de su dispositivo móvil.

– La aparición del fenómeno del *sexting*[48] y su crecimiento plantea problemas que afectan a la intimidad, conducen a ciberacoso y, en algunos casos, puede tener consecuencias legales.

La tendencia a incrementar los ataques a dispositivos móviles se puso de manifiesto en 2012 y se espera que en 2013 se produzca un crecimiento explosivo. Desde 2011 se han detectado *botnets* sobre dispositivos móviles (32) que están compuestas por decenas de miles de terminales. Hay campos muy marginales, como el de los dispositivos médicos inalámbricos, que actualmente no plantean problemas, pero que potencialmente pueden causar graves daños a la salud (33) y alarma social, aunque el número de posibles víctimas no sea elevado. Por otro lado, la «Internet de las cosas» ofrece un nuevo campo de actuación a los atacantes[49].

El notable incremento que ha tenido la utilización de los medios sociales, especialmente de las redes sociales, ha hecho que las amenazas se desplacen hacia esta área del ciberespacio. El enorme aumento del número de usuarios agrava la situación al combinarse con otros factores:

– Debido a su gran conectividad y a que su uso principal es facilitar la interacción entre usuarios, son un medio óptimo para usar una amplia variedad de técnicas de ingeniería social: impostura, correo masivo, buscadores envenenados, intercambio de ficheros, *phishing*, fraude electrónico, infección directa por código dañino e infección por sitios *web*.

– La conectividad las hace muy eficaces para distribuir código dañino y para crear *botnets*, sobre todo en dispositivos móviles.

– Las empresas que explotan estas redes implantan mecanismos de seguridad de la información y de gestión de la privacidad que distan de ser los adecuados, aparte de que su uso no está extendido[50]. Ello las hace vulnerables a los ataques contra los datos personales o a la suplantación de identidad.

– Lo anterior, combinado con que los puntos de entrada a estas redes son, mayoritariamente, dispositivos móviles, produce, como se ha dicho anteriormente, un efecto cruzado que incrementa la vulnerabilidad compuesta.

[48] El término inglés *sexting* hace referencia al envío de imágenes (fotografías o vídeos) con contenido sexual por medio del móvil.

[49] El CAESS (Center for Automotive Embedded Systems Security) ha demostrado la viabilidad de un ataque lanzado mediante la inserción de un CD con archivos MP3 maliciosos en el equipo de audio de un vehículo eléctrico de última generación: el *malware* se hace con el control del ordenador que gobierna el motor del vehículo (49).

[50] Según el *Informe sobre ciberdelincuencia 2012* de Norton, solo la mitad de los usuarios utilizan los controles de configuración de privacidad para determinar qué información comparten y con quién.

– La interconexión de los medios sociales con otras áreas o aplicaciones (v. g. salud, educación, automóvil, Internet de las cosas, etc.) ofrece mayores posibilidades para iniciar un ataque.

Los medios sociales, por tanto, continuarán aumentando su interés como objetivo de ataques. Los principales motivos son el gran número de usuarios, la relación cada vez más estrecha con otras áreas, el gran número de interconexiones y la penetración de los medios sociales en las empresas.

Finalmente, hay un grupo de potenciales víctimas que son especialmente sensibles a ciertos ataques: se trata de los menores y los ataques contra la integridad moral y la intimidad. Estos ataques van desde un leve acoso hasta conductas que ponen en peligro no solo la integridad moral de los menores sino también su salud. Se puede establecer una clasificación general de este tipo de ataques[51]:

– Acecho y acoso *(cyber-stalking)*. Utilización de medios en línea (correo electrónico, mensajería instantánea, redes sociales, SMS, etc.) para acosar y amenazar repetidamente a la víctima, recogiendo datos, realizando sabotaje y llegando, incluso, a usurpar su identidad para este fin.

– Acoso sexual *(online grooming)*. Conducta consistente en establecer lazos y emplear técnicas de convicción con un menor, por medios en línea, con el fin de obtener de él algún tipo de satisfacción sexual ya sea en el ciberespacio o en el mundo «real».

– Intimidación y abuso *(cyber-bullying)*. Es una conducta agresiva, utilizando medios en línea, por uno o varios individuos, de forma repetida e intencionada, contra una víctima que se encuentra en inferioridad de condiciones para defenderse.

– Exposición a contenidos inapropiados o ilegales tales como pornografía, violencia y odio.

– Exposición a medios que promueven conductas dañinas para la salud o antisociales, como promoción del suicidio o daño autoinfligido, anorexia, drogas, etc.

– Revelación de datos personales. La falta de consciencia sobre la importancia de estos datos y la tendencia a comunicarlos a sus amigos acarrean consecuencias negativas. Los datos revelados lo son para siempre y tienen transcendencia en el futuro de los menores.

Para hacer frente a este tipo de ataques específicos es esencial la acción de los padres, tutores y personal docente. Por un lado, deberán educar al

[51] En el ya citado informe de los resultados de la encuesta en España del proyecto europeo *EU KidsOnline* (19), se expone la incidencia, distribución, gravedad y consecuencias de los daños a los menores derivados del uso de Internet.

menor en el uso de la tecnología de forma segura, así como en las pautas de comportamiento respetuosas con los demás; por otro lado, ejercerán una acción vigilante, adaptada a la edad; finalmente, proporcionarán apoyo en caso de sufrir un ataque de este tipo y adoptarán las medidas necesarias para hacerlo cesar y mitigar su impacto. En todos los casos, es imprescindible crear un clima de confianza con el menor que le impulse a informar lo más tempranamente posible de que está sufriendo un ataque.

Para facilitar lo anterior, es preciso trabajar en tres áreas: primeramente, aportando los recursos tecnológicos adecuados para proteger la privacidad de los menores y dificultar las conductas enunciadas; en segundo lugar, se necesita complementar el uso de la tecnología con recursos educativos a disposición de los centros de enseñanza y de los padres o tutores, y, por último, hay que incrementar la formación de los padres, tutores y profesores, a fin de que conozcan las herramientas más adecuadas y sean más conscientes de los riesgos que corren los menores, la manera de atajarlos y la ayuda externa de que pueden disponer (34).

Disminución del riesgo

Teniendo en cuenta los orígenes de ataque más probable, los activos en riesgo y las principales amenazas, se puede obtener una relación razonable de medidas de reducción del riesgo. Es necesario hacer hincapié en las medidas que afecten a amenazas con elevado grado de posibilidad de aparición o con gran impacto sobre los activos. A la vista de lo expuesto en los apartados anteriores, se deben considerar las siguientes medidas:

- Medidas físicas de protección. Se trata de impedir la sustracción o el acceso físico indebido. Entre ellas se deben incluir las precauciones en la custodia de equipos fijos (incluyendo periféricos y elementos de red como *routers*), dispositivos portátiles, soportes lógicos removibles y soportes físicos (agendas, facturas, comunicaciones bancarias, etc.), adoptando también las medidas necesarias para borrar completamente la información o destruir los soportes cuando ya no sean necesarios. También se incluyen las medidas necesarias para proteger los equipos ante orígenes de ataque no conscientes: protección contra sobretensiones, unidades de alimentación ininterrumpida, correcta ubicación y anclaje, uso de cerraduras para evitar el acceso al interior del dispositivo, adecuada manipulación, evitar acceso a personas no apropiadas, etc.
- Protección del acceso lógico. Las medidas de control de acceso lógico buscan impedir que usuarios no autorizados (incluyendo código dañino) puedan hacer uso de sistemas, aplicaciones y servicios o accedan a datos. En los usuarios particulares, el sistema más empleado de

acceso lógico es el de identificación/autentificación mediante el par usuario-contraseña; por tanto, resultan imprescindibles las buenas prácticas en el uso de contraseñas. En la medida de lo posible, se usará la autentificación doble, cuando esté disponible. Por ejemplo, un lector de huella digital en el ordenador portátil, combinado con usuario-contraseña, o el envío de un código por SMS desde la web del banco, combinado con un cuadro de claves. Finalmente, el uso de certificados digitales que se almacenan en el equipo o en un soporte externo (p. ej. el DNI electrónico) suponen un elevado grado de seguridad en el acceso lógico a aplicaciones y servicios.

– Protección del acceso a red. Con cualquier clase de dispositivos, el acceso a la red debe ser lo más seguro posible. En el caso de redes domésticas, es preciso configurar el *router* de forma segura, prestando especial atención a los parámetros de configuración de la red *Wifi* y siendo conscientes de que un *router* seguro es la primera línea de defensa contra ataques informáticos. Es necesario activar un cortafuegos *(firewall)* en el equipo, aunque la mayoría de los *routers* tengan uno. El uso de puntos de acceso inalámbrico públicos exige adoptar medidas específicas de seguridad, aparte de las genéricas: cerciorarse de que la red es verdaderamente la que dice ser, no conectarse a servicios que requieran el tráfico de datos sensibles (banca, compras, etc.), usar servicios seguros de correo, cerrar todas las sesiones, desactivar el uso compartido de archivos, carpetas y servicios y, en general, utilizar servicios que permitan el cifrado.

– Protección del *software*. Gran cantidad de ataques por código dañino aprovechan vulnerabilidades de las aplicaciones y programas instalados en el equipo, incluyendo el sistema operativo. La medida más simple y eficaz para evitarlo es mantener todo el software debidamente actualizado, para lo cual se puede aprovechar la posibilidad de actualizaciones automáticas que suelen ofrecer las empresas que producen las aplicaciones. En caso de que el fabricante de una aplicación no publique actualizaciones de seguridad, puede resultar aconsejable no usar el producto, ya que acabará constituyendo una vulnerabilidad. Por otro lado, es imprescindible tener instalado un programa contra el *malware*, debiendo mantenerlo continuamente actualizado. Existen multitud de programas, de los que los más conocidos son los denominados «antivirus». En realidad, son más que antivirus puesto que también actúan contra otros tipos de código dañino, aunque su denominación original no ha cambiado. Actualmente, están a la venta conjuntos de programas contra el *malware* que incluyen antivirus, *antispyware*[52], protección de correo electrónico,

[52] Específicos contra programas parásitos que recopilan datos sobre el usuario, incluyendo datos sensibles, sin su consentimiento.

cortafuegos, navegación segura y otras prestaciones de seguridad. Son conocidos como «suites de seguridad» y aportan una adecuada protección. No obstante, también existen productos gratuitos de elevada calidad, por lo que alcanzar un buen grado de protección está al alcance de todos. Finalmente, es preciso considerar si de verdad son necesarios todos los programas instalados en el equipo, ateniéndonos a la regla de que cuanto menos *software* tengamos instalado, menos vulnerabilidades podrán ser explotadas. Se deben desinstalar de modo seguro todos aquellos programas que no son útiles o necesarios. Lo anterior es aplicable a servicios como uso compartido de impresoras o archivos, que deben desactivarse si no se van a utilizar.

– Configuraciones seguras. Los equipos, los programas y los servicios se entregan con una configuración inicial que no siempre es la más segura. Es preciso documentarse y modificar la configuración inicial por defecto, prestando atención a contraseñas, usuarios, confianza, qué informes se envían, quién puede acceder a los datos personales y qué acciones se realizan de forma automática. Es importante prestar atención a las aplicaciones de los teléfonos inteligentes, ya que poseen acceso a datos y funcionalidades que no siempre se justifican. Los usuarios de un equipo deben tener los menores privilegios posibles que les permitan realizar sus funciones, sobre todo si el equipo tiene una conexión activa.

– Navegación segura. Primero, es necesario configurar adecuadamente el navegador desde el punto de vista de la seguridad; después, conviene utilizar programas o complementos que faciliten la seguridad en la navegación, y, finalmente, es necesario adquirir hábitos seguros de navegación relativos a páginas que se visitan, enlaces que se siguen, servicios que se utilizan, descargas de ficheros y programas, etc.

– Protección de datos y privacidad. La información importante debe ser almacenada de forma segura. Lo anterior incluye no almacenar sin cifrar datos sensibles en dispositivos portátiles o removibles, siendo también muy aconsejable hacer lo mismo en equipos fijos. No se deben almacenar en la «nube» datos sensibles (en último extremo, usar un cifrado fuerte). Para minimizar el impacto de una pérdida de datos, es necesario realizar regularmente copias de respaldo y almacenarlas en soportes distintos de los equipos, situados físicamente separados y protegidos. Por último, hay que adquirir el hábito de ser crítico ante la necesidad de comunicar datos personales sensibles, evaluando rápida y automáticamente a quién se comunican, por qué medios, para qué propósito y por qué motivo.

– Medios sociales. En el uso de estos medios, sobre todo de las redes sociales, hay que emplear las mismas medidas generales que en el

resto de los servicios a los que se accede; no obstante, hay medidas a las que hay que dar especial importancia. Es preciso utilizar contraseñas robustas. Hay que configurar las opciones de seguridad y privacidad lo más estrictas posibles, revisando periódicamente su validez y los cambios en las políticas de privacidad de los proveedores de estos servicios. Es preciso evitar aplicaciones de terceras partes (p. ej. juegos) que no resulten de garantía, así como limitar su acceso a nuestra información. Se debe considerar que toda la información que se sube a estos servicios es como si fuese pública, ya que, bien por ataques o por cambios en las configuraciones de seguridad del proveedor, puede acabar al alcance de muchas personas; por tanto, no se debe proporcionar a estos servicios información personal ni «colgar» fotografías, vídeos, comentarios u otros documentos cuya difusión pública pueda causarnos daño. Es preciso compartir la información solo con las personas con las que de verdad se quiera hacerlo, para lo cual se deberá emplear la adecuada configuración. También se deberá adquirir la certeza de que quienes quieren ser agregados a nuestros grupos de contactos son quienes dicen ser y no se ha producido una suplantación de identidad. Finalmente, es necesario desarrollar hábitos que nos permitan usar estos servicios sin ser víctimas de técnicas de ingeniería social.

– Ingeniería social. Como ya se ha dicho, la defensa contra la ingeniería social se basa en una inteligente política de uso de los sistemas, en la buena práctica en el empleo de los medios y en adquirir hábitos para detectar y reaccionar casi automáticamente ante estas técnicas. Más concretamente, es necesario prestar atención a los correos electrónicos que se reciben, borrando los no solicitados y los dudosos y no abriendo los ficheros adjuntos aunque procedan de amigos, ya que han podido ser suplantados. Es necesario no seguir ningún enlace que ofrezca dudas ni atender ninguna ventana emergente que solicite descargar algún fichero. Conviene iniciar sesión en los servicios tecleando la dirección directamente en la barra de direcciones del navegador. Al descargar archivos, sobre todo los procedentes de redes P2P, es necesario examinarlos, con uno o varios programas antivirus, antes de abrirlos. Y, sobre todo, detectar incoherencias y detalles extraños que suelen ser síntoma de un ataque de ingeniería social, y aprender a decir «no».

– Teléfonos móviles. Los teléfonos móviles inteligentes constituyen en la actualidad más del 60% de los terminales móviles; el resto son móviles clásicos o 3G. La seguridad de los terminales inteligentes sigue, en general, los mismos criterios que los ordenadores de otro tipo. Hay medidas específicas para los dispositivos móviles: realizar

copias de seguridad de los datos; anotar el IMEI[53] del terminal para desactivarlo en caso de pérdida o robo; desactivar las conexiones inalámbricas (*Wifi*, infrarrojos y *bluetooth*) cuando no se utilicen; desactivar el servicio GPS cuando no sea necesario; usar PIN o similar para bloquear el terminal y el teléfono; usar *software* antirrobo; no abrir mensajes SMS/MMS de origen desconocido o dudoso; y no perder el control físico sobre el dispositivo, sobre todo si está encendido.

– Protección de menores. Para proteger las actividades de los menores en el ciberespacio, ya se ha mencionado que es esencial la acción de los padres, tutores y personal docente; de forma preventiva, mediante la vigilancia y la educación del menor en el uso seguro de la tecnología, así como en pautas de comportamiento respetuosas con los demás. En caso de sufrir un ataque de este tipo, mitigarán sus consecuencias mediante el apoyo y otras medidas paliativas, y adoptarán las medidas necesarias para hacerlo cesar. En todos los casos, es imprescindible crear un clima de confianza con el menor.

Conciencia de *ciberseguridad*

Grados

Ya se ha citado el principio según el cual la seguridad se rompe siempre por el eslabón más débil. También se suele admitir como cierto que, en lo relativo a la *ciberseguridad,* el eslabón más débil es el elemento humano. Sin embargo, esta es una visión negativa de las capacidades de la persona. Considérese un ataque utilizando la ingeniería social, por ejemplo impostura, *spam* o «estafa nigeriana»: el atacante dispone del conocimiento de estas técnicas y de un plan preparado, y los medios tecnológicos le permiten acceder a la víctima; en ese momento, la seguridad reposa sobre la reacción de esta. Si posee los conocimientos, experiencia y conciencia de seguridad necesarios, el ataque será infructuoso y se habrá revelado como el eslabón más fuerte de la cadena de seguridad, puesto que los otros ya han sido superados. Al final, el enfrentamiento se ha reducido a dos adversarios humanos utilizando sus propias capacidades, una vez descartada la infraestructura tecnológica que los ha puesto en relación.

Entendida según se ha expresado en el capítulo primero, la conciencia de *ciberseguridad* resulta de extrema importancia para situar a la persona en un lugar adecuado en la cadena de seguridad. La adaptación al nuevo

[53] IMEI (*International Mobile Equipment Identity* o Identificador Internacional de Equipo Móvil) es un código grabado en los teléfonos móviles que sirve para identificar al terminal de manera inequívoca a nivel global. Cuando un terminal móvil se conecta a la red telefónica, se identifica transmitiendo su IMEI y su número de abonado.

medio que supone el ciberespacio requiere de la creación de esa conciencia, que necesariamente acabará por producirse. Lo importante es acelerar el proceso, ya que con ello se evitarán muchos daños.

La conciencia de *ciberseguridad* se alcanza paulatinamente, según ciertos grados, pues no todas las personas pueden llegar a alcanzar el mismo grado. La edad también influye: cada grado de madurez de la persona permite alcanzar un grado de conciencia de ciberseguridad. Podemos establecer cuatro grados, de los que los tres primeros podrían ser alcanzados por una parte significativa de la población.

- El primer grado puede denominarse *ciberhigiene*. Es el grado básico y procura un nivel elemental de seguridad que, sin embargo, permite hacer frente a una elevada cantidad de amenazas[54]. Consiste en medidas que debe adoptar una persona para proteger sus activos, previniendo los ataques o disminuyendo sus efectos. Se trata, en general, de hábitos, es decir, de acciones aprendidas que necesitan poca o nula intervención de un propósito razonado y que se ejecutan de una manera automática, a veces en respuesta a un determinado estímulo. Nos movemos en el terreno de la psicología y, desde este punto de vista, son una traslación al ciberespacio de los hábitos higiénicos y de limpieza que observamos con nuestra persona y con nuestras pertenencias y lugares de estancia. Mediante la creación de tales automatismos se establece una predisposición favorable a la supervivencia en el ciberespacio y se sientan las bases de los siguientes grados de consciencia.
- Se puede denominar al segundo grado *ciberconciencia*, porque es donde interviene realmente la consciencia personal. Se trata de un grado de conciencia derivado del conocimiento del entorno (el ciberespacio) que permite hacer un uso inteligente y seguro de los recursos tecnológicos. Al contrario que en los hábitos, en los que el raciocinio ocupaba poco espacio, en la conciencia lo importante es el conocimiento, la competencia en una materia, la percepción inteligente y el comportamiento sensato. La creación de *ciberconciencia* requiere instrucción y experimentación, obteniendo los conocimientos necesarios para desenvolverse en el ciberespacio y extraer de forma segura el mayor provecho de sus posibilidades.
- Un tercer grado, que implica la socialización de la conciencia, es lo que se puede denominar *ciberciudadanía*. Anteriormente se ha tratado del «ciudadano digital»; pues bien, la *ciberciudadanía* es el ejercicio consciente de los deberes y derechos que corresponden al individuo como ciudadano digital. Al trascender del ámbito individual, este

[54] Según un informe (52) de la National Audit Office del Reino Unido, el 80% de los ataques digitales podrían haberse prevenido simplemente a través de *ciberhigiene*.

grado de concienciación proporciona un mayor nivel de seguridad, basándose en el poder del grupo organizado mediante reglas. Todas las señas distintivas del ciudadano digital que se han visto anteriormente colaboran a incrementar la seguridad en el ciberespacio.

– Un cuarto grado, que se sale del tronco común de los ciudadanos, es el que podemos denominar ciberespecialista. Se trata de una superación del segundo grado mediante la adquisición de elevados conocimientos, técnicos y de otro tipo. Dentro de este grado existen, a su vez, distintos niveles en función de los conocimientos que se posean, que pueden ser adquiridos mediante el sistema de enseñanza o por otros medios. Este tipo de personas son las que pueden realizar una aportación activa a la *ciberseguridad*. Son ellas quienes idearán las tecnologías, medios, estrategias y procedimientos de seguridad y los aplicarán. Ejercerán funciones en los centros y órganos de *ciberdefensa* a nivel nacional e internacional y serán los encargados de combatir la *ciberdelincuencia* con sus propias armas. Por otra parte, serán unos actores importantes a la hora de concienciar al resto de los ciudadanos. Uno de los objetivos de la creación de una conciencia nacional de ciberseguridad deberá ser detectar y orientar a los individuos con capacidades para llegar a ser ciberespecialistas.

Los sujetos

Los sujetos son aquellas personas en las que se debe crear conciencia de *ciberseguridad.* Aparentemente, no existen muchos matices posibles, ya que podría decirse que los sujetos son toda la población; sin embargo, con ser esto idealmente cierto, no toda la población es igual ni todos pueden ser sujetos de concienciación al mismo tiempo: hay unas personas que deben ejercer las tareas de concienciación y, en consecuencia, deben adquirir unos conocimientos adecuados con anterioridad. Por tanto, se debe hablar de sujetos inmediatos y de sujetos últimos.

Los sujetos inmediatos de concienciación son aquellos que tienen a su cargo esta tarea con respecto a los demás. Se trata de actores de este proceso. Son los padres, tutores, educadores, trabajadores sociales, voluntarios, etc. Una vez implantada y en funcionamiento una política de creación de conciencia de *ciberseguridad*, este tipo de personas solo requeriría una instrucción que les habilitase para ejercer sus tareas de concienciación hacia los demás. Sin embargo, sin esta política implantada, se exige un esfuerzo paralelo: crear conciencia ciudadana de *ciberseguridad* en ellos e instruirlos para ser creadores de conciencia en los demás.

Los sujetos últimos son la población en general que actúa en el ciberespacio. Cada vez quedan menos sectores de población que no hacen uso

de ningún medio perteneciente al ciberespacio. Esto quiere decir que la «brecha digital», debida fundamentalmente a motivos socioeconómicos, se va cerrando, y la creación de una conciencia de *ciberseguridad* tendrá efectos favorables en el cierre de esta brecha. En España, el número de personas de 10 años y más que han accedido a Internet en alguna ocasión aumentó un 3,7% en el año 2012, hasta los 27,9 millones (21). Esto permite hacerse una idea del volumen y del esfuerzo que requerirá la creación de una conciencia de *ciberseguridad* en los individuos.

Es necesario hacer una distinción en este tipo de sujetos: por un lado están los menores, cuyo paso por el sistema educativo permite ayudarles a acabar siendo verdaderos ciudadanos digitales, y por otro lado se encuentran los adultos que, no habiendo recibido en su educación los conocimientos para adquirir una conciencia de *ciberseguridad*, requieren otro tipo de actuaciones. Básicamente, habrá que condensar los conocimientos e ir a buscar a los sujetos, diseñando estrategias más activas.

Los actores

Los actores son los que deben tener a su cargo, en mayor o menor medida, la creación de la conciencia de *ciberseguridad* en las personas. No se debe olvidar que la creación de esta conciencia forma parte de la estrategia de seguridad de la nación (1), por lo que es una tarea en la que debe implicarse toda la sociedad. No obstante, hay personas, organizaciones e instituciones que deben sentirse más concernidas por el ejercicio de esta tarea. A continuación, se entresacan las más significativas.

- Padres. Se incluyen también tutores y otros responsables de la educación en el entorno familiar. Son actores esenciales para la creación de conciencia de *ciberseguridad*, ya que bajo su tutela se producirán los primeros contactos de los menores con las tecnologías de la información y telecomunicaciones. Deberán integrar adecuadamente la educación en este campo con el resto de la educación familiar, para conseguir la adaptación a este medio.
- Docentes. Miembros del sistema de enseñanza, que son también actores esenciales. Prolongan la acción de los padres en la escuela y ayudan a crear el grado de *ciberconciencia* mediante la transmisión de conocimientos sobre el ciberespacio. En ciertos casos sustituyen a los padres que, por su situación socioeconómica, no pueden ejercer sus tareas en este campo.
- Voluntarios. Personas con sensibilidad social que aportan sus conocimientos y experiencia, empleando su tiempo en tareas relacionadas con la creación de conciencia de *ciberseguridad*. Son valiosos auxiliares, siempre que su acción se realice en el marco de la escuela o de

diversas asociaciones, lo que facilita canalizar estos recursos en una acción planificada.

- Instituciones públicas. El Estado es responsable de definir la política de *ciberseguridad*. Por tanto, la Administración en todos sus niveles y sus distintas instituciones deben colaborar, con los medios de que dispongan, a crear conciencia de *ciberseguridad*. Por los recursos de que disponen y su capacidad de actuación, son actores principales. La acción será más eficaz cuanto más cercana se encuentre la Administración al ciudadano. Hay que destacar el papel que juegan los cuerpos policiales por sus conocimientos sobre la lucha contra la *ciberdelincuencia* y la autoridad en materia de seguridad que les resulta inherente.
- Instituciones privadas. Fundaciones e instituciones similares pueden tener entre sus fines la creación de conciencia de *ciberseguridad*. Son una muestra del dinamismo de la sociedad y tienen como ventaja que pueden especializarse en un campo concreto, logrando en él una elevada eficacia.
- Asociaciones. Tienen un papel similar al de las instituciones, pero su pervivencia es más azarosa. Mientras que están activas, pueden ser un refuerzo importante de otros actores, sobre todo en lugares con pocos recursos tecnológicos.
- Empresas. La responsabilidad social de la empresa es un concepto cada vez más implantado en la gestión empresarial. Las empresas del campo de las TIC, como especialistas en estas tecnologías, están muy bien situadas para ejercer su responsabilidad social favoreciendo la creación de conciencia de ciberseguridad.
- Medios de comunicación. En todos los soportes, los medios de comunicación son un importante actor en este campo debido a su gran difusión, a la variedad de público al que alcanzan y a su gran potencial para crear opinión.

El objeto

El objeto es sobre lo que hay que crear conciencia. Para ello, nos vamos a valer del análisis efectuado en la parte anterior, desde el punto de vista de los riesgos. De este modo, a continuación veremos las líneas generales sobre las que se debe actuar. En algunos casos se darán solapamientos, pero ello resulta necesario para dar coherencia a cada «campaña».

- Protección física de los equipos y dispositivos. Tienen un valor en sí mismos y, al tiempo, son los almacenes de nuestros datos personales.

- Protección de los datos personales. Son el elemento más preciado que poseemos en el ciberespacio, y no hay que ponerlos en riesgo. Debemos prestar atención al comunicarlos o compartirlos, protegerlos con cifrado y hacer copias de respaldo, así como tomar precauciones al guardar información en la «nube».
- Protección del acceso a nuestros dispositivos, aplicaciones y servicios. Buenas prácticas en el uso de contraseñas.
- Proteger nuestras redes, físicas o inalámbricas. Buenas prácticas para prevenir la intrusión.
- Buenas prácticas cuando usamos comunicaciones inalámbricas (conexiones a redes *Wifi*, uso de *Bluetooth*, infrarrojos, RFID, NFC, etc.).
- Uso seguro de los dispositivos móviles. *Sexting*. Atención a los servicios que se usan y acciones en caso de pérdida o robo.
- Lucha contra el código dañino. Cierre de las vías de acceso y buenas prácticas en el uso de cortafuegos, antivirus y *antispyware*. Actualizaciones de seguridad de programas, así como mantener una correcta configuración de los equipos y programas.
- Navegación segura por la red. Precauciones con los ficheros que se descargan y en el uso de servicios bancarios y en las compras por Internet.
- Uso responsable de los medios sociales, sobre todo redes sociales. Atención a las configuraciones de privacidad. Saber en quién se está confiando. Los datos que se suben a la red son muy difíciles de eliminar, así que hay que pensar antes de actuar.
- Uso seguro de las diversas mensajerías: correo electrónico, IRC, mensajería instantánea, etc. Ser consciente de que no se sabe con seguridad quién está al otro lado. Combatir el *spam* y el *phishing*.
- Conocimiento de las técnicas de ingeniería social. Creación de hábitos de respuesta para detectarlas y contrarrestarlas.
- Apoyo a los menores frente a ataques específicos. Informar y crear espacios de confianza, así como mecanismos para ayudar a detectar, informar y combatir estos ataques.
- Respeto a las personas en el ciberespacio. Prevenirse contra Conductas ofensivas. Robo de identidad y ciberacoso.
- Respeto a la propiedad intelectual y datos ajenos. Descargas. Acceso a datos de los demás.
- Responsabilidad en el uso de los medios. No contaminar el ciberespacio.

Los medios

Se utilizarán tres vías principalmente para crear una conciencia nacional de *ciberseguridad:* la educación, la enseñanza y la concienciación.

La primera vía por la que se creará conciencia de *ciberseguridad* es la educación. La educación es responsabilidad primaria de los padres, que la comparten con los docentes cuando envían a sus hijos a la escuela. Hogar y escuela son, por tanto, los escenarios en los que se impartirá la educación. El objetivo es crear actitudes y valores en la persona e infundir buenos hábitos. Es aquí donde se conseguirá el adecuado grado de *ciberhigiene,* necesario para subir a los siguientes niveles. Al final de la educación, si se consigue el objetivo, se tendrá un adulto joven con un grado de conciencia que le permitirá desenvolverse como ciudadano digital.

La educación en este campo debe empezar temprano y adaptarse a la edad de la persona. Se integra en la vida cotidiana y encuentra en el ejemplo un gran apoyo. Por este motivo, los padres y docentes deben esforzarse en poseer conciencia de *ciberseguridad* y los conocimientos necesarios para guiar al menor en el uso de las tecnologías. La vigilancia parental es esencial también para evitar situaciones de riesgo a los menores en el uso de medios sociales, mensajería instantánea, teléfono móvil, etc. La acción de los padres se continúa en la escuela, por lo que debe existir una adecuada coordinación. En este campo, las asociaciones del ámbito escolar cumplen una importante misión.

Para poder ejercer su cometido, los padres y docentes necesitan disponer de recursos educativos. Estos recursos deben ser proporcionados por el resto de actores, que deben valorar adecuadamente la importancia básica de la educación en este campo. Un recurso fundamental es la formación.

La enseñanza es otra vía por la que se creará, desde edades tempranas, conciencia de *ciberseguridad* en las personas. Su escenario es la escuela y su objetivo es proporcionar conocimientos y habilidades. Su finalidad, que la persona conozca el nuevo entorno de una manera inteligente, aprovechado sus recursos y anticipándose a los peligros. Además, refuerza las actitudes y valores creados mediante la educación. En ciertos casos, puede ser necesaria una acción dirigida a compensar deficiencias en la educación. Mediante la enseñanza se consigue crear la conciencia digital, grado más avanzado que la *ciberhigiene* ya que permite no solo sobrevivir, sino «habitar» y actuar provechosamente en el ciberespacio. La conjunción de los esfuerzos de educación y enseñanza en el hogar y la escuela favorecen el desarrollo de la ciudadanía digital[55].

[55] Ver en Ribble, 2011 (51), los elementos para una enseñanza en la escuela de las reglas del ciberespacio y del uso seguro y responsable de la tecnología.

La enseñanza como vía de creación de conciencia de *ciberseguridad* debe ser transversal. No debe relegarse exclusivamente a asignaturas sobre tecnología, aunque los conocimientos técnicos se impartan preferentemente en estas. El uso de las TIC en la escuela es necesario y abarca todas las materias. En todas estas circunstancias, el personal docente, e incluso el directivo, deben crear ocasiones de mostrar el uso seguro de las tecnologías. Se debe dar en todos los ciclos formativos, empezando lo antes posible. Por este motivo, se necesita continuidad a lo largo de toda la trayectoria de los alumnos. Una importante función de la enseñanza es la detección y orientación de personas dotadas de aptitudes para sobresalir en el campo de la *ciberseguridad*: los *ciberespecialistas.*

La última vía considerada es la concienciación, entendida como conjunto de acciones dirigidas a que las personas sean sensibles a algo, es decir, sean conscientes de ello, y modifiquen sus actitudes y comportamiento. La concienciación se desarrolla en todos los espacios de la sociedad. Su finalidad es mantener el pulso de esta frente a las posibles amenazas en el ciberespacio. Actualiza y completa lo asimilado en el hogar y en la escuela, por vía de la educación y enseñanza, y entra con sus propios medios en ellos. Es continua, ya que las amenazas y los atacantes evolucionan constantemente. La concienciación es fundamental para reducir las «brechas digitales» a las que se enfrenta la sociedad: regionales, socioeconómicas, generacionales, etc.

La concienciación se debe encuadrar en la estrategia nacional de *ciberseguridad,* que define los objetivos, las prioridades, los medios, la coordinación y otros aspectos relevantes para conseguirla. Involucra al sector público y privado y debe ser liderada e impulsada por el Gobierno. Hace un uso extenso de técnicas de comunicación y persuasión para proporcionar información veraz y útil. En relación a esto último, es importante evitar sesgos en la información proporcionada por los distintos actores, ya que pueden conducir a una falsa sensación de seguridad o, por el contrario, a una alarma social injustificada.

En general, la concienciación utiliza técnicas ya experimentadas y muy similares a las campañas que estamos acostumbrados a ver sobre otros objetos, como, por ejemplo, la seguridad vial. Se utilizan para ello todos los canales de comunicación disponibles y se mantienen a lo largo del tiempo, ya que las amenazas también son permanentes y cambiantes. Las Administraciones Públicas y el resto de actores deben completar las acciones de concienciación con la aportación de recursos en beneficio directo de los ciudadanos. Estos recursos pueden ser servicios, como los CERT, o bien herramientas informáticas de seguridad gratuitas, publicaciones, páginas *web*, etc. De esta manera, las acciones de concienciación se ven reforzadas y ganan credibilidad, al tiempo que se incrementa globalmente la *ciberseguridad*.

Los medios que se emplean para la creación de conciencia de *ciberseguridad* en el ciudadano varían según el escenario, el objeto y los sujetos. Dejaremos a un lado las campañas de concienciación, de las que ya se ha dicho que siguen esquemas de comunicación similares a otros temas. Por un lado, hay que considerar los medios con los que se apoya a los actores para conseguir en ellos una formación adecuada y que estén en condiciones de ejercer sus labores, pero por otro, se deben poner a su disposición diferentes medios de apoyo a sus tareas de crear conciencia de *ciberseguridad.*

Los padres y profesores tienen que disponer de guías escritas con información sobre las amenazas y el modo de combatirlas. También necesitan material escrito sobre cómo programar sesiones o actividades. Es importante, para coordinar y reforzar las acciones en el hogar y la escuela, que existan portales web dirigidos a padres y profesores. Estos portales pondrán a su alcance material didáctico, cursos de formación en línea e información estructurada sobre los aspectos más importantes. También les orientarán sobre dónde buscar recursos educativos en diversas áreas más especializadas. Los portales deben ser creados y mantenidos por instituciones públicas[56] en colaboración con otros actores privados.

Es importante que los padres y profesores reciban formación en vivo de expertos en seguridad. Los demás actores, cada uno en su especialidad, deberán acercarse a la escuela y proporcionar presentaciones, charlas y orientación, no solo sobre la seguridad y sus reglas, sino también sobre cómo organizar las acciones. En temas como el *ciberacoso* se emplea con eficacia la combinación de una presentación en vivo o un vídeo seguidos de un grupo de discusión en el que participan padres y docentes.

Los padres pueden tener como ayuda juegos o cuestionarios, ya sean escritos o en formato electrónico, para poder emplearlos en casa junto con sus hijos.

En la escuela existe una multitud de medios y técnicas que se pueden emplear para apoyar las acciones de creación de conciencia. En primer lugar, es muy importante que el centro tenga una política explícita sobre el uso del ciberespacio y que se haga pública para conocimiento de toda la comunidad escolar. El conocimiento y la aplicación de las reglas de esta política pueden resultar muy eficaces. El compromiso del centro con el uso correcto de las tecnologías de la información y telecomunicaciones se debe poner de manifiesto con la existencia de un sitio web propio debidamente mantenido. La participación de los alumnos en este sitio es un medio importante para su educación y formación en el uso del ciberespacio. La implicación de los menores se consigue también

[56] En España, por ejemplo, el INTECO.

mediante concursos temáticos adaptados a las amenazas más recientes y peligrosas.

Enmarcadas en actividades escolares o extraescolares, se pueden realizar presentaciones por personas expertas, por ejemplo policías, que refuerzan la labor de los padres y docentes. También se pueden programar dramatizaciones, útiles para sensibilizar respecto al *ciberacoso* y sus consecuencias. Otros medios adecuados son los cuestionarios, a ser posible usados en combinación con otras técnicas. Asimismo se deben usar distintos tipos de carteles, que pueden ser objeto de concursos a fin de despertar más interés, y, finalmente, vídeos y otros medios audiovisuales, que completan el conjunto.

Como se ha visto, los medios necesarios para la creación de una conciencia de *ciberseguridad* en los ciudadanos no suponen elevados gastos; es mucho más importante la acción de los poderes públicos definiendo la política y enmarcando las acciones de creación de conciencia en una estrategia de *ciberseguridad*, así como la implicación de los distintos sectores de la sociedad ejerciendo de actores para concienciar. La creación de conciencia es un proceso gradual que requiere tiempo y planificación. También resulta imprescindible adaptarse continuamente a la evolución de las amenazas.

Conclusiones

El ciberespacio es un nuevo dominio apto para la acción humana gracias a una gran ruptura tecnológica. Desde este punto de vista, se puede comparar a un nuevo territorio preparado para ser habitado, es decir, colonizado. A la sociedad, a escala global, le corresponde adaptarse a este hábitat como tantas otras veces ha sucedido a lo largo de la historia con la apertura de nuevos territorios o dominios. Para ello, las personas deben evolucionar para adaptarse a un nuevo entorno, adquiriendo nuevos hábitos y una nueva conciencia. Ello se realizará mediante la transmisión del conocimiento, característica esencial de la especie humana.

La creación de una conciencia ciudadana de *ciberseguridad* es un elemento esencial de la estrategia nacional. La Estrategia de Seguridad Nacional española incluye las *ciberamenazas* entre los riesgos y amenazas que afectan singularmente a la seguridad nacional. Así mismo, señala la concienciación de los ciudadanos como parte de una línea estratégica en el ámbito de actuación de la *ciberseguridad*.

Considerado como un nuevo dominio, se tiende a aplicar al ciberespacio una concepción geográfica derivada de la falta de adaptación y asimilación de sus características y focalizada en sus aspectos comunitarios. Sin embargo, el ciberespacio es un «no lugar»; es un medio más que un espacio y existe porque se producen flujos de información, esto es, relaciones.

A la hora de estudiar el ciberespacio, lo primero que se necesita es un modelo que nos permita describirlo y representar sus características. Hay que buscar el modelo más sencillo que se adapte a las características de este estudio. Por tanto, parece adecuado adoptar el modelo de Libicki, que consta solo de tres capas (física, sintáctica y semántica) y separa a los actores humanos, permitiendo mayor flexibilidad.

El ciberespacio no se debe asimilar directamente a Internet, lo que es un error común. Internet es solo una parte (aunque la más extensa) del ciberespacio, que contiene otras «regiones». Hay que prestar atención a estas regiones, ya que son, cada vez más, escenario de actividades de gran interés y, al tiempo, potencialmente peligrosas.

Se considera al ciberespacio como uno de los *global commons*. Es necesario preservar estos espacios ante agresiones como la contaminación. A veces, la contaminación del ciberespacio se produce por motivos técnicos, pero la mayor parte de las veces la contaminación tiene un origen humano. La eliminación de conductas contaminantes resulta de la mayor importancia para preservar el ciberespacio.

Las personas atesoran sus datos privados como el activo más importante del que disponen en el ciberespacio. La creciente cantidad y calidad de los datos personales aporta un enorme valor para la economía global. Una regulación adecuada de la protección de datos personales, la creación de un clima de confianza, la educación de las personas en relación con el control de su privacidad y una compensación equitativa pueden hacer sumamente provechosas las aplicaciones de los datos personales.

La identidad digital es el conjunto de todos los datos digitales disponibles relativos a una persona, independientemente de su validez, el formato que tengan o lo accesibles que sean. Las personas se preocupan por mantener su privacidad, por lo que se muestran poco dispuestas a comunicar más datos de los necesarios. Desde el punto de vista de la persona, las principales preocupaciones a la hora de comunicar o compartir su identidad digital son la confianza y la privacidad.

Las personas no son las únicas entidades que intervienen en las relaciones y transacciones en el ciberespacio. Los otros dos actores importantes son los Gobiernos y las corporaciones del sector privado. En este triángulo es donde se deben dar las condiciones necesarias para que el clima de confianza se cree y se mantenga. Para ello, resulta necesario un diálogo entre las distintas partes, el establecimiento de unos principios admitidos por todos, la implantación de normas firmes y flexibles y una continua experimentación sobre el terreno para discriminar lo que funciona de lo que no.

Las personas actúan en el ciberespacio con su identidad digital. Las posibilidades abiertas por la tecnología permiten asumir las responsabili-

dades de ciudadanos digitales del ciberespacio. La conciencia ciudadana digital se manifiesta en distintos grados. Hay varios elementos constitutivos de la ciudadanía digital: el respeto a la ley en nuestras acciones en el ciberespacio; el ejercicio de los derechos y deberes del ciudadano digital; la comunicación en el mundo digital; la conciencia de seguridad y su expresión en la conducta, y, finalmente, la responsabilidad como consumidor.

Los ciudadanos habitan, adaptándose a él, un nuevo entorno: necesitan seguridad, la cual se mide por el valor de lo que está en riesgo. Por tanto, la mejor manera de analizar la seguridad es centrase en los riesgos. El análisis centrado en los riesgos es una metodología muy extendida, y lo adaptamos para enfocarlo a los riesgos que corren las personas actuando individualmente en el ciberespacio.

Los factores que hay que considerar son: las víctimas, los orígenes de ataque o atacantes, los activos o bienes en riesgo y las amenazas o acciones contra los activos.

Los activos son un factor esencial, entendiendo como activo un elemento o atributo, material o inmaterial, que la persona posee y que tiene un determinado valor para ella, objetivo o subjetivo. El otro factor importante está constituido por las amenazas, que son sucesos que conducen a la pérdida o degradación de los activos. Determinando la posibilidad de ocurrencia de una amenaza sobre un activo sabremos cómo de vulnerable es. Determinar la cuantía del daño de cada amenaza sobre cada activo proporciona una medida del impacto que tiene esa amenaza al materializarse. De la relación vulnerabilidad/impacto obtendremos, para cada par amenaza/activo, una medida del riesgo: cuanto mayor sea la vulnerabilidad y más grande el impacto, mayor será el riesgo. El riesgo nulo no existe, por lo que deberemos aceptar un determinado nivel de riesgo. Es necesario reducir el riesgo a este nivel aceptable, ya sea minimizando la posibilidad de ocurrencia de las amenazas o mitigando su impacto, en caso de que se produzcan. La finalidad del análisis es deducir las medidas para reducir los riesgos.

En lo relativo a los atacantes, se puede decir que la persona debe estar atenta y precaverse contra tres orígenes genéricos de ataques: causas fortuitas, personas próximas y amenazas en la red.

En cuanto a las víctimas, fundamentalmente hay que considerar dos grupos: los menores y el resto. Los menores son un grupo especial porque se encuentran en una etapa muy importante del desarrollo de su personalidad y las acciones contra ellos pueden ver multiplicados sus efectos.

Los activos que se deben considerar son:

– Equipos físicos de cualquier tipo.

- Datos personales.
- Identidad digital e identidad personal.
- Integridad moral, derivada de la dignidad de la persona.
- Reputación personal y su contrapartida en el ciberespacio, la reputación digital.
- Patrimonio, activos reales materiales o inmateriales que poseen valor de cambio.
- Intimidad o control íntegro sobre los datos que atañen a la esfera más privada de la persona.
- Integridad legal o situación libre de responsabilidades judiciales o administrativas.

No se trata de elaborar un mero inventario de los activos, sino de establecer una jerarquía entre ellos y determinar las relaciones y dependencias existentes. En definitiva, se necesita establecer un «árbol de activos» en el que cada rama muestre cómo el daño o pérdida de uno de sus elementos influye en otros. A esto hay que añadir una valoración de los activos, y el criterio para realizar la valoración se basa, fundamentalmente, en medir su ausencia.

Entre las amenazas, se debe prestar atención a:

- Orígenes fortuitos, como accidentes, catástrofes, averías, etc.
- Acciones de personas próximas.
- Código dañino o *malware*, en sus muy variadas formas.
- Ingeniería social, con su variado despliegue de técnicas.
- Amenazas específicas sobre sistemas móviles.
- Desplazamiento de amenazas hacia medios sociales, especialmente, redes sociales.
- Ataques específicos contra menores y su integridad moral e intimidad.

Contra estas amenazas se definen las medidas que hay que aplicar para reducir los riesgos.

La conciencia de *ciberseguridad* resulta de extrema importancia para que la persona alcance un mayor valor en la cadena de seguridad. Por otra parte, favorece la conciencia de seguridad en otros ámbitos (empresa, Administración, etc.). La adaptación al ciberespacio requiere de la creación de esa conciencia. A fin de evitar al máximo los daños, es importante acelerar el proceso de creación de esa conciencia.

La conciencia de *ciberseguridad* se alcanza paulatinamente, según ciertos grados. No todas las personas pueden llegar a alcanzar el mismo

grado. Podemos establecer cuatro grados, de los que los tres primeros podrían ser alcanzados por una parte significativa de la población. Estos tres son: *ciberhigiene, ciberconciencia* y *ciberciudadanía*. El cuarto grado se refiere a los especialistas en *ciberseguridad,* elementos críticos y muy necesarios en la sociedad de la información.

En la creación de la conciencia de *ciberseguridad* hay que tener en cuenta cuatro factores:

- A quién: los sujetos sobre los que se desea crear esa conciencia de *ciberseguridad*.
- Quién: los actores de la creación de *ciberconciencia*, con protagonismo especial de los padres y docentes. Exige la intervención de la Administración, instituciones, asociaciones, corporaciones y otros muchos actores sociales.
- Qué: el objeto de la concienciación, o sobre lo que hay que crear conciencia. Se deduce del análisis centrado en el riesgo efectuado anteriormente, cuyo fin era determinar las medidas de reducción del riesgo.
- Cómo: los medios para crear la conciencia de *ciberseguridad*, que sigue varias vías, empezando por la educación, continuando en la enseñanza y completándose de forma continua por la concienciación. Los medios son muy variados y corresponde a los distintos actores aportarlos según su área de especialización.

Por último, hay que tener en cuenta dos consideraciones. En primer lugar, la temprana creación de una conciencia de *ciberseguridad,* empezando en el hogar y continuando en la escuela, permitirá identificar y orientar a las personas dotadas con las cualidades necesarias para llegar a ser *ciberespecialistas;* una de las mayores vulnerabilidades a las que se puede enfrentar una nación es la de no disponer de recursos humanos para cubrir todos los frentes existentes en el ciberespacio: defensa nacional, infraestructuras críticas, Administración, instituciones, corporaciones, empresas, etc. Los *ciberespecialistas* constituyen un recurso crítico cuya demanda inicial será muy elevada.

Por otra parte, los futuros líderes de la nación necesitan imperiosamente tener una visión acertada de las consecuencias que trae la adaptación al nuevo entorno del ciberespacio. Sin ser consciente de la naturaleza del ciberespacio y de los cambios que acarrea en la sociedad, no se podrá ejercer el liderazgo en ningún campo (político, empresarial, administrativo, etc.). La creación temprana de una conciencia de *ciberseguridad* y una política acertada a la hora de formar a aquellos destinados a ejercer el liderazgo facilitarán en gran medida que la sociedad en su conjunto se adapte al nuevo entorno con los menores traumas posibles.

Bibliografía

1. Departamento de Seguridad Nacional. *Estrategia de Seguridad Nacional.* España: Presidencia del Gobierno, mayo de 2013. NIPO 002130347.
2. JOYANES AGUILAR, Luis y otros. *Cuadernos de Estrategia 149: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Madrid:Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2010. ISBN 978-84-9781-622-9.
3. BUZAI, Gustavo D. «El ciberespacio desde la Geografía. Nuevos espacios de vigilancia y control global». *Meridiano. Revista de Geografía.* [En línea] 2012, n.º 1 [citado el 25 de febrero de 2013]. http://www.revistameridiano.org/.
4. United States Army Training and Doctrine Command. *TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe, VA: TRADOC Publications, 2010.
5. LIBICKI, Martin C. *Cyberdeterrence and cyberwar.* Santa Monica, CA: RAND Corporation, 2009. ISBN 978-0-8330-4734-2.
6. World Economic Forum y The Boston Consulting Group. *Rethinking Personal Data: Strengthening Trust.* Ginebra (Suiza): World Economic Forum, 2012.
7. DUDMAN, Jane. «Data is the new raw material of the 21st century». *The Guardian.* Edición electrónica, 18 de abril de 2012. [consultada el 11 de abril de 2013]. <www.guardian.co.uk/public-leaders-network/2012/apr/18/francis-maude-data-raw-material>.
8. REDING, Viviane. Conferencia de prensa: «Commission proposes a comprehensive reform of EU data protection rules». *European Commission Audiovisual Services.* Video en web, 25 de enero de 2012. <http://ec.europa.eu/avservices/video/player.cfm?ref=82655&sitelang=en>.
9. The Boston Consulting Group, Inc. *The value of our digital identity.* Liberty Global Inc., 2012. Documento electrónico. <http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf>.
10. ABELSON, Hal y LESSIG, Lawrence. *Digital Identity in Cyberspace, White Paper Submitted for 6.805/Law of Cyberspace: Social Protocols.* MIT's Computer Science and Artificial Intelligence Laboratory. [En línea] 10 de diciembre de 1998 [citado el: 17 de febrero de 2013]. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/linked-white-paper.html.
11. EGUILLOR, Marcos. *Social media.* 185, 2011, Bit, págs. 68-71.
12. RICHARDS, Reshan. «Digital Ctizenship and Web 2.0 Tools». [En línea] Merlot, junio de 2010, *Journal of Online Learning and Teaching,* vol. 6, n.º 2. <http://jolt.merlot.org/vol6no2/richards_0610.htm>.

13. *MAGERIT versión 3.* Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.
14. MUIR, Lawrence L. «The Case Against an International Cyber-Warfare Convention». *Wake Forest Law Review.* Winston-Salem, NC., EE. UU.: Wake Forest University School of Law, diciembre de 2011, vol. 2, n.º 5.
15. VAN HEERDEN, R. P., IRWIN, B. y BURKE, I. D. «Classifying network attack scenarios using an ontology». Seattle: University of Washington, 2012. *Proceedings of the 7th International Conference on Information Warfare and Security,* 22-23 de marzo de 2012, págs. 311-324.
16. SHELDON, John. *State of the Art: Attackers and Targets in Cyberspace.* 2012, *Journal of Military and Strategic Studies,* 2012, vol. 14, n.º 2.
17. ROUNDS, M. y PENDGRAFT, N. «Diversity in Network Attacker Motivation: A Literature Review». *CSE'09 International Conference.* Computational Science and Engineering, agosto de 2009, vol. 3, págs. 319-323.
18. MIRÓ LLINARES, Fernando. *El cibercrimen.* Madrid: Marcial Pons, 2012.
19. DESFORGUES, Alix. «Cyberterrorisme: quel périmètre?» *Fiche de l'Irsem n.°11.* [En línea] diciembre de 2011 [citado el 24 de febrero de 2013]. http://www.irsem.defense.gouv.fr.
20. MAIALEN, Garmendia, y otros. *Riesgos y seguridad en Internet: los menores españoles en el contexto europeo.* Universidad del País Vasco. Bilbao: EU Kids Online, 2011.
21. Equipo de Estudios del ONTSI. *Perfil sociodemográfico de los internautas, análisis de datos INE 2012.* Observatorio Nacional de las Tecnologías y de la Sociedad de la Información. 2013. ISSN 2172-9212.
22. EFE. «Un nuevo caso de "ciberacoso" se lleva por delante la vida de una chica de 15 años». *ABC,* 18 de octubre de 2012.
23. HEARN, Alison. *Structuring feeling: Web 2.0, online ranking and rating, and the digital «reputation» economy.* Ephemera, 2010, págs. 421-438.
24. AGRE, P. E. y ROTENBERG, M. *Technology and privacy: The new landscape.* Cambridge (MA): MIT Press., 1998. ISBN: 9780262511018.
25. KRAMER, Simon y BRADFIELD, Julian C. «A general definition of malware». *Journal in Computer Virology.* Springer-Verlag, 2010, vol. 6, n.º 2, págs. 105-114. Edición electrónica. ISSN 1772-9904.
26. Kindsight. *Kindsight Security Labs Malware Report - Q4 2012.* Kindsight Inc., 2012. [En línea]. <http://www.kindsight.net/sites/default/files/Kindsight_Security_Labs-Q412_*Malware*_Report-final.pdf>.
27. DANG, Hiep. «The origins of social Engineering». McAfee Security Journal. Santa Clara, CA (EE. UU.): McAfee Inc., otoño de 2008.
28. MITNICK, Kevin D. y SIMON, William L. *The art of Deception.* [Ed.] Carol Long. Indianapolis, IN: Wiley Publishing Inc., 2002. ISBN 0-471-23712-4.

29. CIALDINI, Robert B. *Influence.* [Ed.] Carolyn Merryll. Needham Heights, MA: Allynn & Bacon, 2001. ISBN 0-321-01147-3.
30. CIALDINI, Robert B. «The Science of Persuasion». Edición especial enero de 2004, *Scientific American special edition.* Edición especial enero de 2004, vol. 14, n.º 1, págs. 70-77.
31. *Symantec Intelligence Report: February 2013.* Symantec Corporation, 2013. <http://www.symanteccloud.com/es/es/mlireport/SYMCINT_2013_02_February_ES.pdf>.
32. Damballa. *Damballa Threat Report - First half 2011.* Damballa Inc., 2011. [En línea]. <https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf>.
33. «New firewall to safeguard against medical-device hacking». *Purdue University.* [En línea] 12 de abril de 2012 [citado el 14 de abril de 2013]. http://www.purdue.edu/newsroom/research/2012/120412RaghunathanHacking.html.
34. ISTTF. *Enhancing child safety and online technologies: final report of the Internet Safety Technical Task Force to the Multi-state Working Group on Social Networking of State Attorneys General of the United States.* Berkman Center for Internet & Society at Harvard University, 2008.
35. GOLDSTEIN, Emmanuel. *The Best of 2600, Collector's Edition: A hacker odyssey.* Indianapolis, IN: Wiley Publishing Inc., 2009. ISBN 97-0-470-45853-2.
36. MIZRACH, Steven. «Is there a Hacker Ethic for 90s Hackers?» *Old and New Hacker Ethics.* [En línea] 1997, [citado el 25 de febrero de 2013]. http://www2.fiu.edu/~mizrachs/hackethic.html.
37. Government Accountability Office. *Cyber Threats Facilitate Ability to Commit Economic Espionage.* Government Accountability Office. Washington: s.n., 2012. Testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives. GAO-12-876T.
38. POSTEL, J. RFC 801. *NCP/TCP Transition Plan.* [Electrónico]. Network Working Group, noviembre de 1981.
39. FALLIERE, Nicolas, MURCHU, Liam O. y CHIEN, Eric. *W32. Stuxnet Dossier. Version 1.4.* Symantec Coporation, 2011.
40. ZETTER, Kim. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.* [En línea], 11 de julio de 2011, Wired.com [citado el 24 de marzo de 2013]. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/.
41. ETSI. *TR 101 771V1.1.1. Service Independent requirements definition; Threat Analysis.* Sophia Antipolis, Francia: European Telecommunications Standards Institute, 2001-2004. Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

42. Department of Defense (DoD). MIL-STD-882E. *Standard Practice. System Safety.* EE. UU.: Department of Defense (DoD), 11 de mayo de 2012.
43. Ponemon Institute. *The Human Factor in Data Protection.* Ponemon Institute LLC, 2012. Patrocinado por Trend Micro.
44. LYNN, William J. *Defending a New Domain. The Pentagon's Cyberstrategy.* [En línea] Council on Foreign Relations, 1 de septiembre de 2010, Foreign Affairs [citado el 26 de marzo de 2013]. <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
45. NIST. *Special Publication 800-30. Guide for Conducting Risk Assessments.* Gaithersburg, MD: National Institute of Standards and Technology, 2012.
46. ISO. *ISO/IEC 27005: 2011 Information technology-Security techniques-Information security risk management.* ISO/IEC, 2011.
47. OIKARINEN, J. y REED, D. RFC 1459. *Internet Relay Chat Protocol.* [Electrónico] Network Working Group, mayo de 1993.
48. MARINO, Louis y SFAKIANAKIS, Andreas. *ENISA Threat Landscape. Responding to the Evolving Threat Environment.* European Network and Information Security Agency (ENISA). 2012.
49. KRYSIUK, Piotr y DOHERTY, Stephen. *The World of Financial Trojans.* Symantec Security Response. Mountain View, CA (EE. UU.): Symantec Corporation, 2013 [citado el 7 de abril de 2013]. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_world_of_financial_trojans.pdf>.
50. SHAH, Jimmy. «Los riesgos contra los datos confidenciales de los dispositivos móviles en el origen de las amenazas futuras». *McAfee Security Journal,* núm. 7. Santa Clara, CA (EE. UU.): McAfee Inc., 2011.
51. Blue Coat Systems. *2012 Web Security Report.* Blue Coat Systems Inc., 2013. <http://www.bluecoat.com/sites/default/files/documents/files/BC_2012_Security_Report-v1i-optimized.pdf>.
52. RIBBLE, Mike. *Digital Citizenship in Schools, 2.ª ed.* International Society for Technology in Education (ISTE), 2011. ISBN: 978-1564843012.
53. NAO. *The UK cyber security strategy: Landscape review.* Reino Unido, National Audit Office. 2013.

Concienciación[1] en las administraciones públicas

Por Luis Jiménez Muñoz

Capítulo tercero

Toma de conciencia y percepción del riesgo

El capítulo que se presenta analiza la problemática de la toma de conciencia[2] sobre los riesgos asociados al uso de las tecnologías de la información por parte del personal de las Administraciones Públicas, así como la importancia de su gestión en los marcos regulatorios del funcionamiento de la Administración.

El concepto de riesgo asociado al uso de las tecnologías de la información no difiere mucho del tradicional concepto de riesgo manejado por diversas disciplinas (1). En este sentido, el riesgo es un constructo social, dinámico y cambiante que requiere para su prevención y mitigación de dos herramientas básicas, el conocimiento y la comunicación (información y formación).

En el ámbito de las tecnologías de la información hace tiempo que se ha asumido la necesidad de convivir con un nivel de riesgo ya que la seguridad total o absoluta no existe. El grado de complejidad de las tecnologías de la información y las comunicaciones ha aumentado considerablemente y cada vez es más difícil de administrar el riesgo adecuadamente, y por tanto, de controlarlo.

[1] Concienciación: Acción y efecto de concienciar o concienciarse (Real Academia Española).

[2] Concienciar: Hacer que alguien sea consciente de algo. Adquirir conciencia de algo.

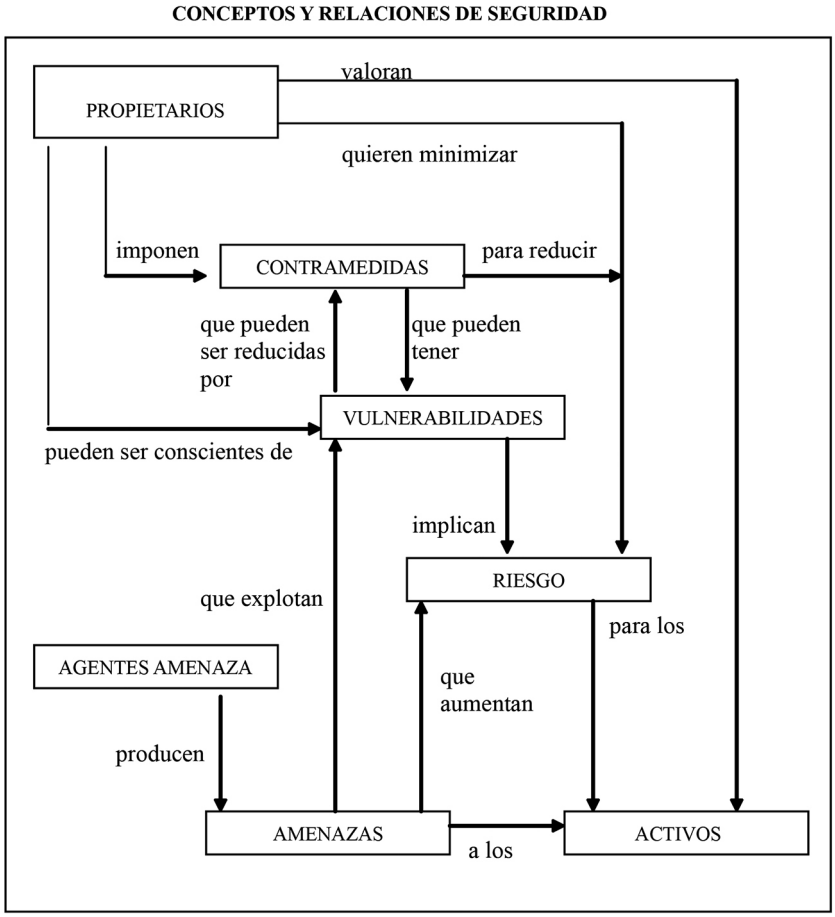


Figura 3.1: Conceptos y relaciones de seguridad en Common criteria ISO15408.

En las Administraciones Públicas, la gran mayoría de autores señalan que el nivel adecuado donde deben prevenirse los incidentes de seguridad es el nivel de usuario final del sistema de información, porque es allí donde se presupone que el eslabón más débil de la cadena existe y porque la experiencia ha demostrado que es donde ocurren la mayoría de violaciones, intencionadas o no, de la seguridad.

Sin embargo, aun siendo cierto lo anterior, la necesidad de comunicación y conocimiento (toma de conciencia) es mayor en los niveles jerárquicos superiores del personal de las Administraciones Públicas, incluido el nivel político, pues la toma de decisiones en relación con la *ciberseguridad* debe tener una buena ubicación para que las prioridades puedan ser adecuadas y el eterno equilibrio entre seguridad y eficacia pueda ser alcanzado.

La gestión del riesgo es para el experto en riesgos Lavell (2):

> *... no solo la reducción del riesgo, sino la comprensión que en términos sociales se requiere de la participación de los diversos estratos, sectores de interés y grupos representativos de conductas y modos de vida (incluso de ideologías y de perspectivas del mundo, la vida, la religión) para comprender cómo se construye un riesgo social, colectivo, con la concurrencia de los diversos sectores de una región, sociedad, comunidad o localidad concreta...*

Resulta interesante la idea expresada por el autor en cuanto al hecho de que la gestión del riesgo no consiste simplemente en disminuir la vulnerabilidad, sino en la búsqueda de acuerdos sociales para soportar o utilizar productivamente los impactos. Este acuerdo social al que hace referencia Lavell se manifiesta en el *principio de proporcionalidad* (3) que debe inspirar la toma de decisiones a la hora de implementar las medidas de seguridad en un sistema de información.

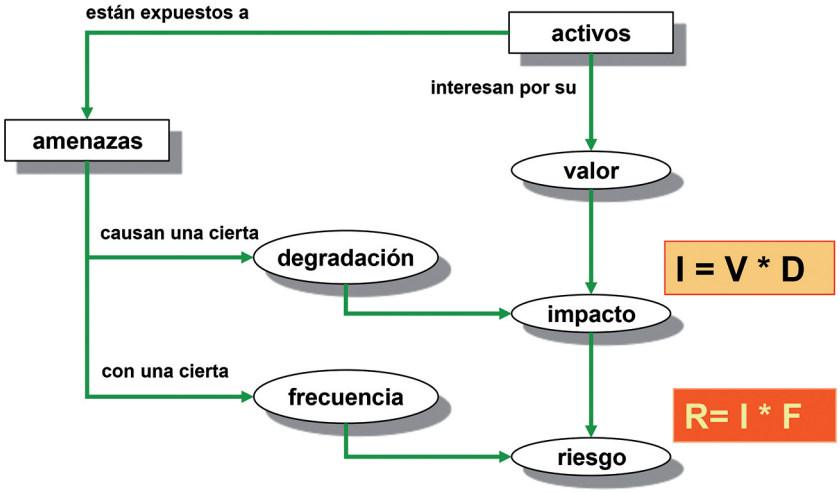


Figura 3.2. MAGERIT: Modelo conceptual de análisis de riesgos.

En tal sentido, resulta importante considerar que la gestión del riesgo no puede ser reducida a meras intervenciones tecnológicas, sino que debe estar referida al proceso a través del cual la sociedad, en sus diferentes niveles de estructuración:

> *...toma conciencia del riesgo, lo analiza y lo entiende, considera las opciones y prioridades en términos de su reducción, considera los recursos disponibles para asumirlo, diseña las estrategias e instrumentos necesarios para ello, negocia su aplicación y toma la decisión de hacerlo para finalmente implementar la solución más apropiada en términos del contexto concreto en que se produce o se puede producir el riesgo.*

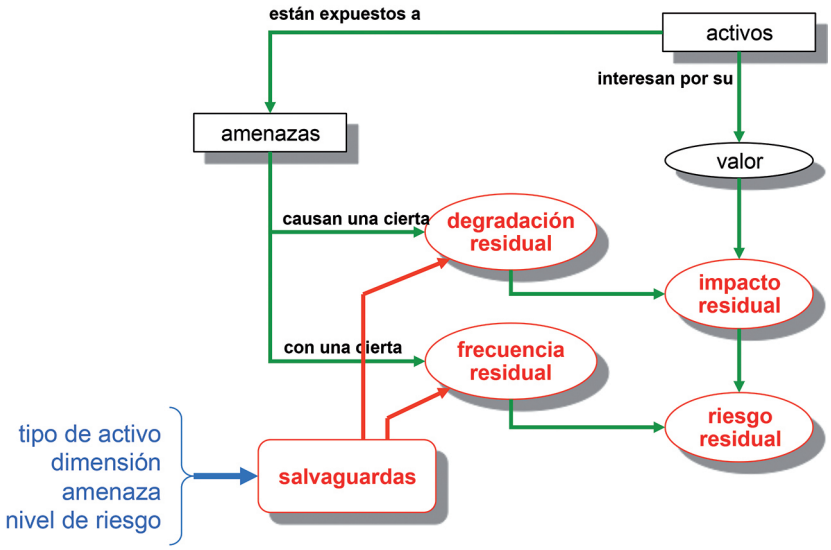


Figura 3.3. MAGERIT: Modelo conceptual de gestión de riesgos.

La gestión del riesgo es definida por Keipi, Bastidas y Mora (4) «... como el proceso que permite identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de las amenazas, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse...». Los autores señalan la importancia de desarrollar la capacidad preventiva y de respuesta, la que en numerosas ocasiones se ha visto inhibida por el conocimiento técnico insuficiente, el pobre desarrollo institucional y la aplicación incompleta de instrumentos preventivos, lo que ha condicionado una orientación mayormente dirigida hacia planes de contingencia con inspiración reactiva, los cuales se aplican a los efectos y no a las causas.

También podemos ver en otros especialistas de la gestión de riesgos el mismo planteamiento de la necesidad del conocimiento técnico suficiente y la información adecuada como factores imprescindibles para generar la capacidad preventiva de una organización ante los *ciberataques* (5).

Ante la «invisibilidad» de las amenazas que existe en el ámbito de las tecnologías de la información y las comunicaciones, es el saber lo que permite «reconocerlos» y «darles existencia». Sin embargo, el saber también puede negarlos o transformarlos, ya sea minimizándolos o dramatizándolos. Ideas similares se tienen en cuenta a la hora de diseñar el papel de la información y el conocimiento adecuado en la gestión de centros de operaciones de seguridad.

Las amenazas y vulnerabilidades que afectan a los sistemas de información han venido aumentando constantemente en los últimos años, llegan-

do incluso a incrementarse un 55% en los dos últimos años, según datos recogidos por el CCN-CERT (6). Respecto a los tipos de riesgos que estas vulnerabilidades implican para nuestros sistemas de información, según publica el CERT gubernamental, la mayoría de las amenazas recibidas constituyen casos de *cibercrimen* o *ciberdelincuencia.* Sin embargo, las más críticas han sido los casos de *ciberespionaje*, de tal forma que esta amenaza se ha convertido en una debilidad crítica en las naciones occidentales, máxime si tenemos en cuenta que estas amenazas evolucionan continuamente y a una velocidad cada vez mayor.

Dado que las amenazas cada vez son más complejas y, a veces, difíciles de detectar, se hace necesaria una formación del personal responsable de las TIC en todos los organismos de las Administraciones Públicas para luchar contra la ingenuidad, la ignorancia de buenas prácticas y la falta de concienciación existente sobre la necesidad de preservar la seguridad de la información. Una seguridad que debe estar orientada a garantizar o mantener tres cualidades propias de esta última: disponibilidad, integridad y confidencialidad. En algunos entornos, especialmente en los dedicados a la administración electrónica, interesan, además, otros aspectos muy importantes de las transacciones *on line* como son la autenticidad o la trazabilidad.

La Administración en su conjunto no puede ser ajena a este escenario y debe considerar el desarrollo, la adquisición, conservación y utilización segura de las TIC como algo imprescindible que garantice el funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

La Administración depende de los sistemas TIC para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los organismos deben aplicar un conjunto coherente y proporcionado de medidas de seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes organismos de la Administración deben «concienciarse» y cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad (7) (8) y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC.

La Administración debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes. Los organismos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar las medidas mínimas de seguridad determinadas por las políticas de seguridad que sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados (9).

Todos los empleados públicos, de todos los niveles, tienen la obligación legal, como se verá más adelante, de conocer y cumplir las políticas de seguridad de la información y la normativa de seguridad. La concienciación de los empleados públicos en materia de seguridad es una tarea imprescindible para el cumplimiento de esta obligación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC deben recibir formación para el manejo seguro de los

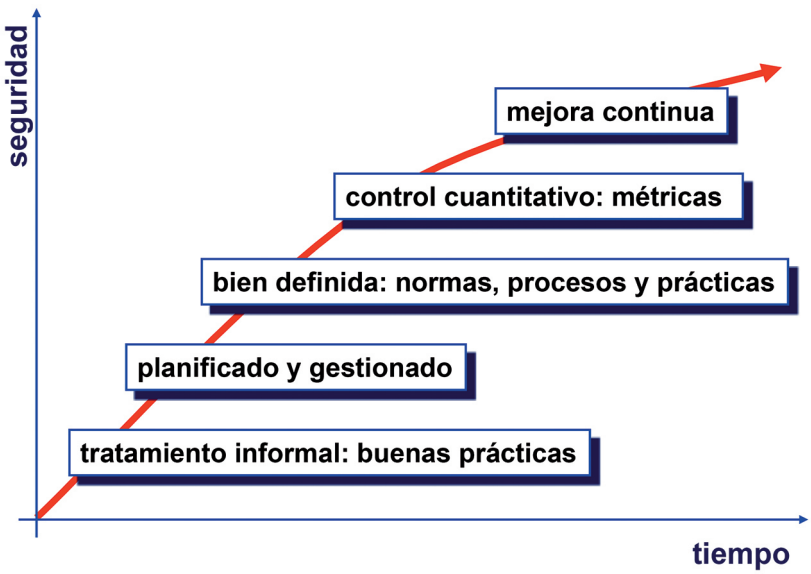


Figura 3.4. Niveles de madurez en la implantación de seguridad en una organización (International Systems Security Engineering Association).

sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo (10).

Las vulnerabilidades

Una vulnerabilidad (11) es una debilidad que puede ser aprovechada por una amenaza[3]. Solucionar las vulnerabilidades es la mejor forma de reducir el riesgo y, en consecuencia, disminuir la probabilidad de incidentes. Las vulnerabilidades aparecen por diversos factores: técnicos, humanos y de organización.

En general, una vulnerabilidad en un sistema se puede agrupar bajo uno de los siguientes apartados en función de su naturaleza:

- Vulnerabilidad debido al uso incorrecto del sistema por parte de usuarios autorizados.
- Vulnerabilidad debido a que no se controla el acceso al sistema.
- Vulnerabilidad generada por medidas de seguridad de procedimiento ineficaces.
- Vulnerabilidad generada por averías o por fallos en el hardware y software.
- Vulnerabilidad intrínseca de los sistemas debido a su complejidad y desconocimiento de sus posibilidades o limitaciones.

La última década ha sido testigo de un crecimiento muy importante en el descubrimiento y publicación de nuevas vulnerabilidades, alcanzándose su punto máximo en 2006 y 2007, para disminuir en los siguientes años e iniciar una nueva escalada, en la que nos encontramos.

El sistema CVSS *(Common Vulnerability Scoring System)* es un estándar, independiente de la plataforma, para la calificación de vulnerabilidades IT. El CVSS asigna un valor (entre 0 y 10) a las vulnerabilidades, atendiendo a su gravedad.

Las vulnerabilidades que conducen a incidentes provocados por factores humanos y organizativos son, en parte, el resultado de errores de los usuarios. Sin embargo, también pueden surgir debido a deficiencias en la organización y en la política y normativa de seguridad de instituciones y organismos.

Determinados estudios han señalado que las vulnerabilidades de aplicaciones web en el periodo considerado de 2012 no habían disminuido respecto de las de 2011.

[3] Definición dada por el Real Decreto 3/2010, de 8 de enero, *por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.*

1	Aplicaciones con insuficientes medidas de seguridad derivadas de una mala gestión de los usuarios o de los administradores. Este tipo de vulnerabilidades incluyen la conexión de sistemas a Internet con mecanismos de usuario-contraseña fáciles de adivinar.
2	Aplicaciones estándar tales como sistemas de gestión de contenidos, sin que se hayan instalado algunas de las actualizaciones de seguridad.
3	Errores de programación en desarrollos a medida para aplicaciones y páginas web.
4	Inyección SQL y Cross Site Scripting (XSS).

Figura 3.5. Vulnerabilidades más importantes detectadas en 2012.

Si bien las prácticas seguras de desarrollo han disminuido la presencia de vulnerabilidades en la producción de *software*, no parecen, sin embargo, estar ayudando significativamente en la reducción de las tasas de vulnerabilidades de aplicaciones *web*. De hecho, la enorme demanda de desarrolladores con experiencia en aplicaciones web, superior a la oferta, el modelo de amenazas en permanente evolución y la complejidad del *software* basado en web propician la aparición de nuevas vulnerabilidades, lo que provoca que las antedichas tasas no disminuyan.

Las vulnerabilidades que más se han reportado son las relativas a inyección SQL y *cross site scripting* (XSS). En segundo lugar, se encuentran las relativas a incidentes por denegación de servicio (DoS), *cross site request forgery* (CSRF) y *remote file include* (RFI).

En muchos casos, el acceso a aplicaciones web todavía se realiza mediante el par usuario-contraseña. Se ha evidenciado que este mecanismo puede burlarse con cierta facilidad, especialmente cuando se usan contraseñas débiles, fáciles de adivinar a través de mecanismos de *phishing* y *hacking*.

Otra de las vulnerabilidades importantes que se encuentra en los organismos e instituciones es la existencia de *software* sin actualizar. Un *software* es vulnerable antes de que el proveedor publique una actualización, y continuará siendo vulnerable hasta que esta actualización (o parche) ha sido adecuadamente implantada. Diferentes análisis han demostrado que, con frecuencia, las actualizaciones no se instalan con la suficiente rapidez o, incluso, no se instalan nunca.

Durante 2012, los atacantes siguieron explotando vulnerabilidades todavía no identificadas a través de los llamados *zero-days exploits.*

También los hábitos de navegación de los usuarios siguen siendo objetivo prioritario de los agentes maliciosos. Durante 2012, el organismo holandés National Cyber Security Centre (NCSC) realizó un estudio sobre 1.000 *websites,* detectando la presencia de 70 diferentes mecanismos de seguimiento ofrecidos por terceros[4]. La investigación también incluyó el uso de *cookies*. Estos trabajos de campo evidenciaron que el seguimiento también se utilizaba en las páginas web de ciertos hospitales, lo que hace especialmente delicado el ataque al afectar a datos de naturaleza personal.

Por otra parte, es preciso mencionar en este apartado de vulnerabilidades las asociadas al uso de los servicios en la nube. El pasado año 2012 los beneficios del uso de servicios en la nube atrajeron la atención de muchas organizaciones. Además de utilizar nubes públicas para los servicios menos comprometidos, las organizaciones han comenzado a invertir de manera más decidida en nubes privadas, construidas con tecnología de virtualización.

Los problemas de seguridad asociados a los servicios *cloud* pusieron de manifiesto, con el reconocimiento por parte de Dropbox, el hecho de que nombres de usuario y contraseñas robadas de otras webs habían sido utilizados para iniciar sesión en un cierto número de sus cuentas. Se adoptaron medidas de seguridad adicionales como la opción de autenticación de dos factores. En mayo de 2012, el Fraunhofer Institute for Securite Information Technology informó sobre las vulnerabilidades relacionadas con el registro, inicio de sesión, cifrado y compartición de datos de acceso en siete servicios de almacenamiento en la nube[5].

El incidente de Dropbox ha hecho aflorar cuestiones tales como: ¿cómo deben las organizaciones abordar la seguridad y la conformidad legal? ¿Autenticación de uno o dos factores? ¿Cómo se pueden manejar las fugas de información? ¿Cómo saber si los usuarios están transfiriendo información a terceros? ¿Cómo preservar el acceso del personal que ya no está en la organización? ¿Cómo seleccionar los proveedores adecuados? ¿Se están aplicando las mismas estrictas normas y requisitos contractuales que se exigen a otros socios críticos del negocio que tienen acceso a datos confidenciales o estratégicos? Y muchas otras.

Por último, hay que resaltar el nuevo escenario de vulnerabilidad que se abre con la implantación en las organizaciones del concepto denominado BYOD[6].

---

[4] http://www.alexa.com.

[5] *Fraunhofer Institute Finds Security Vulnerabilites in Cloud Storage Services. The H Security,* http://www.h-online.com/security/news/item/Fraunhofer-Institute-finds-security-vulnerabilites-in-cloud-storage-services-1575935.html.

[6] *Bring Your Own Device.*

BYOD es una modalidad de trabajo por la que las organizaciones permiten el uso de dispositivos personales (*smartphones* y *tablets,* habitualmente) para el tratamiento de los datos de la propia organización. En esta modalidad, cada usuario es responsable de sus propios dispositivos, que utiliza tanto para propósitos personales como corporativos. La llamada «consumerización» es una tendencia que está estrechamente ligada a BYOD. La consumerización significa que las TIC, cada vez más, se están desarrollando sobre la base de los requisitos de los propios consumidores y de sus dispositivos.

Recientes investigaciones muestran que casi el 75% de las organizaciones estudiadas permiten el acceso a activos de información a través de dispositivos que no están sujetos a la administración de seguridad corporativa[7].

Esta situación está impactando en la seguridad IT de las organizaciones, haciendo que sea necesario adoptar un nuevo enfoque que contemple cómo se accede a datos de negocio desde los puntos finales y cómo se custodiarán tales datos en los dispositivos de los usuarios. Estudios de 2012 muestran que, con frecuencia, la política de seguridad que se redacta y publica para tratar esta problemática es ignorada sistemáticamente por los empleados, cuya concienciación sobre los riesgos que se derivan de las fugas de datos es, todavía, baja[8].

Estas mismas fuentes señalaron que casi la mitad de las organizaciones ven una correlación entre el incremento de dispositivos móviles dentro del entorno corporativo y el incremento del número de incidentes de seguridad[9].

El nuevo enfoque en la gestión de riesgos

El análisis de riesgos es una actividad clásica que se requiere como base en múltiples ámbitos de la seguridad, desde certificaciones de sistemas de gestión de la seguridad (SGSI, ISO 27001) hasta la protección de los servicios de la administración electrónica (Esquema Nacional de Seguridad, Real Decreto 3/2010).

Clásicamente, el análisis de riesgos se ha venido realizando como una actividad de despacho para un análisis preventivo de las medidas de protección adecuadas y proporcionadas al valor de lo protegido frente a una caracterización del entorno hostil en que se encuentra, sea por incidentes externos, ataques deliberados o vulnerabilidades propias del sistema de información.

---

7 iPass (noviembre de 2011) *The iPass Mobile Enterprise Report:* http://info.ipass.com/forms/mobileenterprise-report.

8 PricewaterhouseCoopers (marzo de 2012): *Information Risk Maturity Index.*

9 Trend Micro (febrero de 2012) *Mobile Consumerization Trends&Perceptions:* http://www.trendmicro.com/cloud-content/us/pdfs/rpt_decisive- analytics_mobile_consumerization_trends_perceptions.pdf.

El análisis estático solo permite una gestión preventiva. Durante la ocurrencia de incidentes o ataques, es mero observador que aprende de lo ocurrido para el siguiente ciclo de despacho: revisión periódica. Pero no permite un análisis en tiempo real:

- Cuando descubrimos una vulnerabilidad en nuestro sistema (por ejemplo, un defecto de *software* o una deficiencia de fabricación o de ensamblaje o de gestión).
- Cuando un incidente o un ataque inutiliza parte de nuestras capas de defensa (por ejemplo, desastres naturales o *ciberataques*); en estos casos, el perímetro de seguridad cambia y el riesgo aumenta notablemente.
- Cuando un proveedor tiene problemas en su prestación de servicio con consecuencias sobre nuestra capacidad de operar.

En todos estos casos, lo que se requiere es revisar el análisis de riesgos del nuevo escenario y tomar rápidamente decisiones correctivas que mitiguen el impacto y permitan salir lo antes posible del escenario de crisis en que nos hemos visto envueltos.

Todo análisis necesita un modelo que defina los parámetros de entrada, el procesamiento y el significado de los resultados. En un análisis de riesgos, a veces es tanto o más importante el por qué del resultado porque si el riesgo es elevado la pregunta relevante es qué debemos hacer para reducirlo y, teniendo en cuenta que el entorno es el que es, normalmente lo que hay que mejorar es el sistema de protección propio para que de las mismas premisas se deriven situaciones de mejor riesgo. Eso implica entender cómo se traducen las amenazas en riesgos y cómo frenar las amenazas para que no lleguen a desgracias.

En el nuevo enfoque, los incidentes rara vez son atómicos (en el sentido académico del término: indivisibles) sino que usualmente siguen una ruta de avance desde donde se originan hasta donde hacen daño al sistema. Esto es muy gráfico en sistemas que disfrutan de capas de defensa, físicas y lógicas, de forma que un atacante tiene que ir progresando a través de varias etapas, a veces ayudado de forma inconsciente por problemas técnicos que debilitan alguna capa o por catástrofes naturales que destruyen o debilitan el esquema de capas.

Un modelo que dé respuestas debe incluir este concepto de progreso para poder entender:

- Qué capas debemos proteger preventivamente para impedir, dificultar o retrasar el progreso del incidente.
- Qué debemos hacer cuando una capa ha sido perforada y el atacante está más cerca de alcanzar su objetivo: esta es la parte más dinámica, pues supone conectar los detectores de intrusión al sistema

de análisis de riesgos para conocer el riesgo sobrevenido tras una intrusión.

En definitiva, el nuevo enfoque supone, por una parte, realizar los análisis de riesgos entendiendo los ataques posibles (tiempo, capacidad del atacante, progreso del ataque), y por otra parte, disponer de una capacidad de gestión que pueda informar adecuadamente a los que tienen que tomar decisiones preventivas y reactivas de forma que protejamos no los componentes, sino los servicios finales, sean relativos a la administración electrónica o a los servicios públicos esenciales que, a fin de cuentas, están fuertemente interrelacionados.

Toma de conciencia de lo que hay que proteger

Las políticas de seguridad de la información

La *Política de seguridad de la información* es un documento de alto nivel que define lo que significa «seguridad de la información» en una organización (12). El documento debe ser accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.

El Esquema Nacional de Seguridad (ENS) (13) se refiere en varios puntos a la existencia de una política de seguridad en los organismos públicos:

ENS. Artículo 11. Requisitos mínimos de seguridad:

> *Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.*
>
> *ENS. Artículo 12. Organización e implantación del proceso de seguridad.*
>
> *La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.*
>
> *ENS. Disposición transitoria. Adecuación de sistemas.*
>
> *Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.*
>
> *ENS. Anexo II: Medidas de seguridad.*
>
> *Marco organizativo [org].*

Política de seguridad [org.1].

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

Los objetivos o misión de la organización.

- *El marco legal y regulatorio en el que se desarrollarán las actividades.*
- *Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.*
- *La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.*
- *Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.*

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda (14).

La *Política de seguridad de la información* debe hacer referencia además a aquellas otras políticas de seguridad nacionales o internacionales que afecten al organismo público.

Principios de seguridad

En la toma de decisiones en materia de política de seguridad, se deben tener en cuenta una serie de principios básicos ampliamente aceptados en el ámbito de la seguridad y que están reflejados en los documentos de política de seguridad de la OTAN y de la Unión Europea (15) así como en los de otros países de nuestro entorno:

- Clasificación de la información.
- Habilitación/autorización de seguridad.
- Necesidad de conocer.
- Compartimentación de la información.
- Imputabilidad.
- Equilibrio entre seguridad y eficacia o garantía razonable.
- Segregación de las funciones de administración, administración de seguridad y supervisión de la seguridad.

Los anteriores principios son válidos para cualquier entorno de la seguridad, ya sea seguridad física, seguridad de personal, seguridad documental o seguridad TIC. Existen además otros principios de seguridad generalmente aceptados y directamente relacionados con los sistemas de información:

- Análisis y gestión del riesgo. Se realizarán aquellos procesos necesarios de análisis y gestión de riesgos que permitan monitorizar, reducir, eliminar, evitar o asumir los riesgos asociados al sistema.
- Mínima funcionalidad. Solo estarán disponibles las funciones, protocolos y servicios necesarios para cumplir el requisito operacional o funcional del sistema.
- Mínimo privilegio. Los usuarios de los sistemas que manejen información clasificada solo dispondrán de los privilegios y autorizaciones que se requieren para la realización de las obligaciones de su puesto de trabajo.
- Nodo autoprotegido. Cada sistema interconectado deberá, inicialmente, tratar al otro sistema como un entorno no confiable y deberá implementar medidas que controlen el intercambio de información con el otro sistema.
- Defensa en profundidad. Las medidas de protección deberán implementarse en la medida de lo posible en varios componentes, niveles o capas, y en la máxima extensión, de manera que no haya una única línea (o componente) de defensa.
- Control de configuración. Se debe mantener una configuración básica del equipamiento *hardware* y *software* en los sistemas clasificados. Establecer con carácter obligatorio la aplicación de configuraciones de seguridad en las diferentes tecnologías utilizadas en el sistema.
- Verificación de la seguridad. La aplicación de estos principios y su consecuente implementación en medidas de protección deberá ser inicial y periódicamente verificada.
- Respuesta ante incidentes. Se debe disponer de una capacidad de respuesta que permita una rápida reacción ante un incidente de seguridad.

Los principios de seguridad antes mencionados se materializan en los sistemas de información y comunicaciones identificando un conjunto de objetivos de seguridad:

- Identificar a las personas que acceden a la información manejada por un sistema o a los recursos del mismo.
- Autenticar a las personas que acceden a la información manejada por un sistema o a los recursos del mismo.

- Controlar el acceso a la información manejada por un sistema o a los recursos del mismo.
- Proporcionar confidencialidad a la información manejada por un sistema.
- Proporcionar integridad a la información manejada por un sistema o a los recursos del mismo.
- Mantener la disponibilidad de la información manejada por un sistema o de los recursos del mismo.
- No repudio. Proporcionar la prueba de que una determinada transmisión o recepción ha sido realizada, no pudiendo su receptor/transmisor negar que se haya producido.
- Trazabilidad. Proporcionar los controles que determinen en que en todo momento se podrá determinar quién hizo qué y en qué momento.

El ENS, por su parte, establece otros principios básicos:

- Seguridad Integral: la seguridad de la información en la Administración se plantea como un proceso integral que excluye tratamientos coyunturales. Se prestará especial atención a las personas, la organización y los procedimientos de seguridad.
- Gestión basada en riesgos: se analizarán los riesgos donde se deberán identificar y evaluar riesgos inherentes en todos los activos de información, incluyendo las personas y la infraestructura que invierten en su gestión. Este conocimiento de los riesgos servirá para gestionarlos mediante el despliegue de medidas de seguridad para mitigar su impacto.
- Prevención, reacción y recuperación: los sistemas de seguridad deben tener una orientación preventiva para evitar las amenazas. Los sistemas dispondrán de medidas de recuperación que permitan restaurar la información y los servicios, sin que se ponga en peligro la continuidad de los mismos.
- Establecimiento de barreras de defensa: deberá existir una estrategia de protección con diversas capas de seguridad y control.
- Evaluación periódica: a través de auditorías y sistemas de verificación de cumplimientos.
- Función diferenciada: Las diversas responsabilidades inherentes a la gestión de la seguridad deberán diferenciarse de las relativas a las de gestión de los sistemas de información.

Los principios de seguridad mencionados deben estar recogidos en la *Política de seguridad de la información,* la cual se desarrolla por medio de normativa de seguridad que afronta aspectos específicos. La normativa

de seguridad debe estar a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Dado que la *Política de seguridad de la información* está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello, se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes:

- Normas de seguridad *(security standards)*.
- Guías de seguridad *(security guides)*.
- Procedimientos de seguridad *(security procedures)*.

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios y suelen ser de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos (operativos) de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las organizaciones no siempre separan nítidamente estos diferentes tipos de herramientas, sino que a veces se generan manuales y reglamentos de seguridad que tienen un poco de todos los elementos anteriormente mencionados, buscando siempre una mayor efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que es política (abstracta) y su aplicación concreta. De esta forma, se es más flexible y se consigue una cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados.

El Esquema Nacional de Seguridad

El Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), *por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica,* regula el citado esquema previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Su finalidad es crear la confianza necesaria en el uso de la administración electrónica por parte de los ciudadanos y permitir el cumplimiento por parte de las administraciones de la obligación de prestar acceso electrónico y trámites públicos.

El ENS introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información.

En particular:

- Los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.
- Los requisitos mínimos que permitan una protección adecuada de la información.
- El mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información, el sistema y los servicios a proteger (16).

Se desarrolla teniendo en cuenta, entre otras, las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes, y la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos (17).

En su elaboración se han manejado, entre otros, referentes en materia de seguridad tales como directrices y guías de la OCDE (18), recomendaciones de la Unión Europea, normalización nacional e internacional (19) (20), normativa sobre administración electrónica, protección de datos de carácter personal (21), firma electrónica y Documento Nacional de Identidad Electrónico (22) (23), así como a referentes de otros países.

Sus objetivos principales son los siguientes:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por

los principios básicos y los requisitos mínimos para una protección adecuada de la información.

- Introducir los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones Públicas, así como la comunicación de los requisitos de seguridad de la información a la industria.

En el ENS se concibe la seguridad como una actividad integral en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

El ENS es de obligado cumplimiento para:

- Administración general del Estado (AGE): el conjunto de departamentos, entes, sociedades públicas, organismos y agencias estatales.
- La Administración de las comunidades autónomas (autonómica): los departamentos y consejerías, fundaciones públicas, institutos, agencias, sociedades públicas, universidades y otros entes de la Administración.
- La Administración local: ayuntamientos, diputaciones, mancomunidades y otras formas de organización de la Administración, fundaciones y patronatos, sociedades públicas y entes autónomos.
- Entidades de derecho público vinculadas o dependientes del conjunto de la Administración española.
- No obstante, no es obligatorio a aquellas administraciones que realicen sus actividades en régimen de derecho privado.

Para cumplir con el ENS, las administraciones deben cumplir al menos los siguientes puntos (24):

- Definir y aprobar formalmente la Política de seguridad por parte del titular responsable de la acción de gobierno, documento recopilatorio del marco de seguridad objetivo.
- Definir los tipos y niveles de información administrativa a efectos de seguridad y aprobar su estructura por el órgano de dirección.
- Crear y definir comités de seguridad, responsables de velar por la política de seguridad de la entidad.
- Designar la figura del responsable de seguridad por sistemas y/o departamentos.

- Definir la normativa de seguridad, indicando cómo y quién hace las distintas tareas y cómo se identifican y resuelven las incidencias que pudieran darse.
- Definir y escribir los procesos de autorización, formalizando autorizaciones que cubran todos los elementos de los sistemas de información: instalaciones, equipos, aplicaciones, medios de comunicación, accesos, soportes, etc.
- Establecer el cumplimiento técnico, con la revisión periódica de la normativa y los procedimientos por el personal técnico.
- Realizar auditorías bienales de seguridad en las que se revise la política de seguridad y su cumplimiento, así como el conjunto de riesgos, normativas, procedimientos y controles establecidos.
- Formar continuamente a todo el personal sobre la política, normativa y procedimientos de seguridad.

Están integrados en el ámbito del ENS todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información. De forma específica, se implementarán, gestionarán e integrarán para el cumplimiento del ENS los siguientes conceptos:

- Servicios, trámites y demás relaciones que se presten a ciudadanos electrónicamente.
- Las comunidades electrónicas relativas a la transmisión, almacenamiento y recepción de datos.
- Las sedes y registros electrónicos.
- Las notificaciones y publicaciones electrónicas.
- Los mecanismos de firma electrónica y certificados digitales.
- Las aplicaciones informáticas.
- Los ficheros con datos de terceros.
- La gestión de las copias de seguridad.
- Las herramientas de *hardware* y *software*, ya sean propias o provistas por terceros.
- La adquisición de nuevos componentes de los sistemas de información.
- La transmisión de datos entre distintas administraciones.
- El acceso y manejo de la información por el personal de las administraciones.
- Las redes, dispositivos periféricos, dispositivos móviles, etc.

– Procedimientos que aseguren la conservación y accesibilidad a largo plazo de los documentos electrónicos elaborados por las administraciones públicas.

El cumplimento del ENS engloba toda información que, estando en soporte físico, haya sido causa o consecuencia de la información electrónica, debiendo aplicarse las mismas medidas de seguridad conforme al soporte en el que se encuentre.

Para su implementación, se tiene que disponer de los siguientes elementos (25):

– Inventario de activos, recursos técnicos, organizativos, humanos y procedimentales sujetos al ENS.
– Catalogación de los tipos de información según su criticidad.
– Análisis de riesgos.
– Selección de medidas de protección en función de los tipos y niveles de la información.
– Elaboración de un marco organizativo de seguridad:
  • Documento de política de seguridad.
  • Documentos de normativa de seguridad.
  • Documentos de procedimientos de seguridad.
  • Documentos de autorización.
  • Documentos de cumplimiento técnico.
– Arquitectura de seguridad.
– Sistemas de registro, control y resolución de incidencias.
– Plan de continuidad de servicio.
– Plan de pruebas y monitorización del sistema.
– Medidas de protección.
– Plan de formación y sensibilización del personal.
– Actualización del sistema.
– Plan de auditoría bienal.

Respecto a su implantación, es de aplicación lo siguiente:

– Medidas de protección:
  • Protección de instalaciones e infraestructuras.
  • Gestión del personal.
  • Protección de equipos.
  • Protección de las comunicaciones.
  • Protección de soportes de información.

- Protección de aplicaciones.
- Protección de la información.
- Protección de los servicios.

– Categorización de los sistemas de información:

- Dimensiones de la seguridad: disponibilidad, autenticidad, integridad, confidencialidad, trazabilidad.
- Determinación de los niveles de seguridad por sistema: bajo, medio, alto.
- Relación entre tipos de información y dimensión de la confidencialidad.
- Determinación de categoría de cada sistema: básica, media, alta.

– Marco organizativo:

- Política de seguridad.
- Normativa de seguridad.
- Procedimientos de seguridad.
- Procesos de autorización.
- Órganos de gestión.
- Auditorías de seguridad: cumplimiento legal y cumplimiento técnico.

– Marco operacional:

- Planificación: análisis de riesgos, arquitecturas de seguridad, componentes, etc.
- Control de accesos.
- Explotación: inventario de activos, gestión de procesos, registros, sistemas de protección.

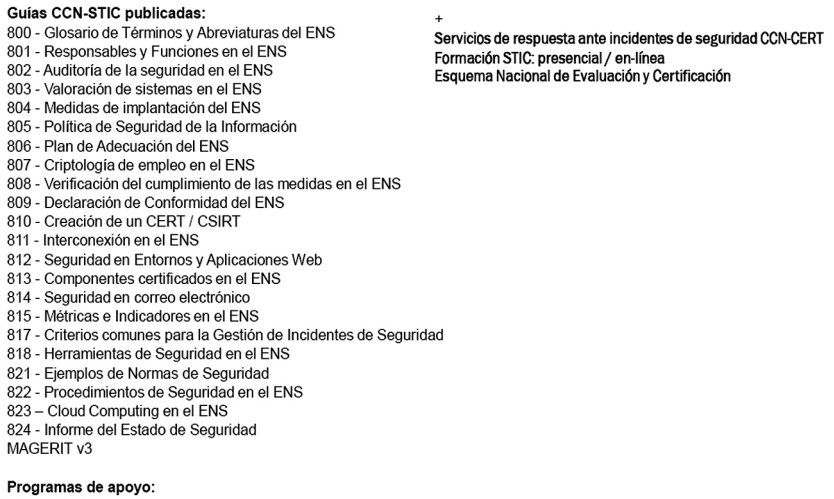


Figura 3.6. Instrumentos de apoyo a la implantación del ENS puestos a disposición de los organismos de las AA. PP. hasta 2012.

- Servicios externos.
- Continuidad del servicio.
- Monitorización del sistema.
- Acreditación de conocimientos de la vida laboral.

Las responsabilidades básicas del personal de la Administración

Las administraciones y entidades públicas de todo tipo deben contar con los factores organizativos que les permitan satisfacer el derecho de los ciudadanos a una buena Administración y contribuir al desarrollo económico y social. Entre esos factores el más importante es, sin duda, el personal al servicio de la Administración.

En general, la legislación básica de la función pública hace posible que existan los profesionales que la Administración necesita, estimula a los empleados para el cumplimiento eficiente de sus funciones y responsabilidades, les proporciona la formación adecuada y les brinda suficientes oportunidades de promoción profesional, al tiempo que facilita una gestión racional y objetiva, ágil y flexible del personal, atendiendo al continuo desarrollo de las nuevas tecnologías.

La Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (26) recoge los principios generales exigibles a quienes son empleados públicos así como los derechos básicos y comunes, distinguiendo entre los de carácter individual y los derechos colectivos. El Estatuto establece en nuestra legislación una regulación general de los deberes básicos de los empleados públicos fundada en principios éticos y reglas de comportamiento, que constituye un auténtico código de conducta.

En definitiva, la condición de empleado público no solo comporta derechos, sino también una especial responsabilidad y obligaciones específicas para con los ciudadanos, la propia Administración y las necesidades del servicio. Este, el servicio público, se asienta sobre un conjunto de valores propios, sobre una específica «cultura» de lo público que, lejos de ser incompatible con las demandas de mayor eficiencia y productividad, es preciso mantener y tutelar.

El Estatuto Básico también define las clases de empleados públicos –funcionarios de carrera e interinos, personal laboral, personal eventual– y la figura del personal directivo, factor decisivo de modernización administrativa, puesto que su gestión profesional se somete a criterios de eficacia y eficiencia, responsabilidad y control de resultados en función de los objetivos.

El capítulo VI del Estatuto recoge el «Código de conducta» de los empleados públicos. En él se establece (art. 52) que:

Los empleados públicos deberán desempeñar con diligencia las tareas que tengan asignadas y velar por los intereses generales con sujeción y observancia de la Constitución y del resto del ordenamiento jurídico, y deberán actuar con arreglo a los siguientes principios: objetividad, integridad, neutralidad, responsabilidad, imparcialidad, confidencialidad, dedicación al servicio público, transparencia, ejemplaridad, austeridad, accesibilidad, eficacia, honradez, promoción del entorno cultural y medioambiental y respeto a la igualdad entre mujeres y hombres, que inspiran el Código de Conducta de los empleados públicos configurado por los principios éticos y de conducta regulados en los artículos siguientes.

Los principios éticos (art. 53) recogen entre otros la necesidad de que los empleados públicos «respeten la Constitución y el resto de normas que integran el ordenamiento jurídico», y de que su actuación persiga «la satisfacción de los intereses generales de los ciudadanos y se fundamentará en consideraciones objetivas orientadas hacia la imparcialidad y el interés común, al margen de cualquier otro factor que exprese posiciones personales, familiares, corporativas, clientelares o cualesquiera otras que puedan colisionar con este principio». Ajustarán su actuación a los principios de lealtad y buena fe con la Administración en la que presten sus servicios, y con sus superiores, compañeros, subordinados y con los ciudadanos. Su conducta se basará en el respeto de los derechos fundamentales y libertades públicas y fundamentalmente actuarán de acuerdo con los principios de eficacia, economía y eficiencia, y vigilarán la consecución del interés general y el cumplimiento de los objetivos de la organización.

Además, y en relación con la necesidad de concienciación que aquí nos ocupa, los empleados públicos «cumplirán con diligencia las tareas que les correspondan o se les encomienden», «guardarán secreto de las materias clasificadas u otras cuya difusión esté prohibida legalmente», «garantizarán la constancia y permanencia de los documentos para su transmisión y entrega a sus posteriores responsables», «mantendrán actualizada su formación y cualificación» y «observarán las normas sobre seguridad y salud laboral».

Los aspectos de concienciación sobre los riesgos y de formación en seguridad pueden verse reflejados en los principios de conducta que establece la Ley 7/2007 relativos a la actuación diligente, eficaz, responsable, etc. Sin embargo, se echa de menos una expresión explícita a la observancia de las normas de seguridad informática tal como hace con las normas de seguridad y salud laboral.

La organización de seguridad

Los organismos de la Administración son entidades de distinta naturaleza, dimensión y sensibilidad y, sin entrar en casuísticas particulares,

está claro que el mantenimiento y gestión de la seguridad de las TIC va íntimamente ligada al establecimiento de una organización o estructura de seguridad dentro de los organismos (27).

Dicha «organización de seguridad» se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte. En general, la *Política de seguridad* debe establecer las funciones y responsabilidades, en materia STIC, del personal que constituye las diferentes estructuras de la organización. Por ejemplo, el artículo 10 del Esquema Nacional de Seguridad diferencia la responsabilidad de seguridad (responsable de seguridad) de la responsabilidad sobre la operación del servicio (responsable del sistema, ayudado por el administrador de seguridad), de forma que el responsable de seguridad supervisa la actividad operacional (28).

Como norma general, en la organización de seguridad de un organismo público se encontrarán definidas las figuras que se citan a continuación. Hay que tener en cuenta que estas figuras son un modelo de referencia que sirve de orientación en el desarrollo de la estructura de seguridad de cualquier organización, donde las necesidades de personal y recursos disponibles son determinantes.

La responsabilidad del éxito de una organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades y la política de seguridad del organismo y de facilitar los recursos adecuados para alcanzar los objetivos propuestos. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas. En una organización pueden coexistir diferentes informaciones y servicios, debiendo identificarse al responsable (o propietario) de cada uno de ellos. Una misma persona puede aunar varias responsabilidades. Por ejemplo, en el ENS dos figuras son especialmente relevantes:

- El responsable de la información que establece las necesidades de seguridad de la información que se maneja.
- El responsable del servicio que establece las necesidades de seguridad del servicio que se presta.

El ENS habla del «responsable de la información» como la persona que tiene la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la persona que determina los niveles de seguridad de la información. Aunque la aprobación formal de los niveles corresponda al responsable de la información, se puede recabar una propuesta al responsable de seguridad y conviene que se escuche la opinión del responsable del sistema.

El ENS habla del «responsable del servicio» como la persona que tiene la potestad de establecer los requisitos del servicio en materia de seguri-

dad. O, en terminología del ENS, la persona que determina los niveles de seguridad de los servicios.

En todos los organismos públicos debería existir también un «responsable de seguridad» o persona específicamente designada por el organismo, según procedimiento descrito en su política de seguridad, con un conjunto más o menos concreto de las siguientes responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación STIC dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema (ver sección 9).
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.

Esta figura de «responsable de seguridad» aparece con otras denominaciones en diferentes documentos de política de seguridad, como por ejemplo:

- NIST: Computer Security Program Manager [SP 800-12] (29).
- Unión Europea: Autoridad INFOSEC (ASTIC) [2001/264/CE].
- CCN: Autoridad de Seguridad de las Tecnologías de la Información y Comunicación (ASTIC) [CCN-STIC 201].
- Ministerio de Defensa: Autoridad INFOSEC (AI) [OM 76/2002] (30).

Otros roles especialmente importantes desde el punto de vista de la seguridad son aquellos directamente relacionados con la operación o explotación de los sistemas TIC. En este sentido, en los organismos públicos debería también existir un «responsable del sistema», persona designada por el propietario del sistema en la correspondiente documentación de seguridad con un conjunto de responsabilidades como las siguientes:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del sistema y cerciorarse de que estas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema.
- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Velar por el cumplimiento de las obligaciones del administrador de seguridad del sistema.
- Investigar los incidentes de seguridad que afecten al sistema y, en su caso, comunicación al responsable de seguridad o a quien este determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

La figura de responsable del sistema recibe también otras denominaciones tales como:

- NIST: Program and functional managers / application owners [SP 800-12].

- Unión Europea: Autoridad Operativa del Sistema de Tecnología de la Información (AOSTI) [2001/264/CE] (15).
- CCN: Autoridad Operacional del Sistema de las Tecnologías de la Información y Comunicación (AOSTIC) [CCN-STIC 201].
- Ministerio de Defensa: Autoridad Operacional del Sistema (AOS) [OM 76/2002].

En estrecha colaboración con el responsable del sistema, debería existir la figura de administrador de la seguridad del sistema. Esta persona debe ser designada por el propietario del sistema con las responsabilidades de gestión, configuración y actualización, en su caso, del *hardware* y *software* en los que se basan los mecanismos y servicios de seguridad, la implementación, gestión y mantenimiento de las medidas de seguridad y la supervisión de las instalaciones de *hardware* y *software*, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.

El administrador de seguridad del sistema es figura clave en la prevención, detección y respuesta ante los *ciberataques*. Como resultado de su trabajo y buen hacer, la organización garantiza que los controles de seguridad establecidos son cumplidos estrictamente, que se aplican los procedimientos aprobados para manejo del sistema y que se realiza la trazabilidad, la auditoría y el registro y análisis de eventos de seguridad.

El administrador de seguridad es el responsable, además, de iniciar el proceso de respuesta ante incidentes que se produzcan en el sistema bajo su responsabilidad, informando y colaborando con el responsable de seguridad en la investigación de los mismos.

Otras denominaciones de esta figura son:

- NIST: Security officer [SP 800-12].
- Unión Europea: Agente de Seguridad INFOSEC [2001/264/CE].
- CCN: Administrador de Seguridad del Sistema (ASS) [CCN-STIC-201].
- Ministerio de Defensa: Administrador de Seguridad del Sistema (ASS) [OM 76/2002].

En cada sistema, además, tienen cabida otras figuras tales como el administrador del sistema, el administrador de red, operadores, etc., y, finalmente, los usuarios del sistema, que es el conjunto de personas autorizado para acceder al sistema utilizando las posibilidades que les ofrece el mismo.

Como ya se ha mencionado, los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del sistema, por tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio sistema.

Deberes y obligaciones (mp.per.2):

1. Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

a) Se especificarán las medidas disciplinarias a que haya lugar.

b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto como las obligaciones en caso de término de la asignación o traslado a otro puesto de trabajo.

c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo como posteriormente a su terminación.

2. En caso de personal contratado a través de un tercero:

a) Se establecerán los deberes y obligaciones del personal.

b) Se establecerán los deberes y obligaciones de cada parte.

c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Figura 3.7. Medidas de seguridad (mp.per.2) del ENS en relación con las responsabilidades.

Administradores y operadores deben estar debidamente informados de sus obligaciones y responsabilidades, así como haber sido instruidos para la labor que desempeñan. Administradores y operadores del sistema son responsables, entre otras cosas, de leer, comprender y seguir los procedimientos operativos de seguridad (POS) relativos a su sistema y de asegurarse de que están preparados adecuadamente para llevar a cabo operaciones en el sistema, en particular las correspondientes a la gestión de mecanismos de identificación y al procedimiento de gestión de incidentes.

«La seguridad como función diferenciada» exige que el responsable del sistema no sea la misma persona que el responsable de seguridad. Además, de acuerdo con el *principio de jerarquía* que rige en las administraciones públicas españolas, en caso de conflicto este deberá ser resuelto por el superior jerárquico. Esto debería concretarse para el caso de cada organización, acorde con la normativa que sea de aplicación. El mecanismo concreto debe figurar en la *Política de seguridad.*

Las responsabilidades y los riesgos

La gestión de los riesgos es una tarea que debe realizarse de manera continua sobre el sistema, y se deben orientar todas las demás actividades de acuerdo a los principios de «gestión de riesgos» y «reevaluación periódica»[10].

[10] Ver artículo 6, «Gestión de la seguridad basada en los riesgos», y artículo 9, «Reevaluación periódica», del ENS.

En el análisis de riesgos se debe tener en cuenta el principio de proporcionalidad entre el nivel de detalle del análisis y la importancia (categoría) del sistema. Es responsabilidad del responsable del sistema que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

Por su parte, el responsable de la seguridad es responsable de que el análisis de riesgos se ejecute en tiempo y forma, así como de identificar carencias y debilidades y ponerlas en conocimiento de los responsables de la información, del servicio y del sistema.

En todo organismo público debería quedar claro que el responsable de la información es el dueño de los riesgos sobre la información, del mismo modo que el responsable del servicio es el dueño de los riesgos sobre los servicios.

En este sentido, el dueño de un riesgo debe ser informado (¡y tener conciencia!) de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente dueño.

Una buena praxis en los organismos públicos sería establecer indicadores del estado de los riesgos críticos (KRI, *Key Risk Indicators*). Estos indicadores son propuestos por el responsable de seguridad; su definición debería ser acordada por el responsable de seguridad y el dueño del riesgo.

La definición de los indicadores contendrá expresamente en qué medidas se basan, cuál es el algoritmo de cálculo, la periodicidad de evaluación y los umbrales de aviso y alarma (atención urgente), y los umbrales de riesgo en los que es preciso informar al responsable correspondiente. Todo ello, además, debería estar a disposición de los auditores.

En definitiva, la responsabilidad de monitorizar un riesgo recae en su dueño, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

Existen numerosos puntos de concurrencia entre los roles y responsabilidades aquí mencionados, el Esquema Nacional de Seguridad y el Reglamento de Protección de Datos de Carácter Personal. En algunos puntos hay coincidencia, y en otros diferencias.

El RD 1720/2007 de Protección de Datos de Carácter Personal identifica varios responsables y encargados, pormenorizando las funciones y tareas que cada uno debe realizar. Los siguientes párrafos muestran cómo conviven con las tareas y funciones marcadas por el Esquema Nacional de Seguridad.

Todos los roles determinados en uno y otro ordenamiento deberán ser identificados y estar formalmente asignados, sin perjuicio de que algunas figuras puedan concurrir en la misma persona, según se desarrolla a continuación.

El artículo 5 del RD 1720/1997 establece que el responsable del fichero o del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Asimismo establece que el responsable de seguridad es la persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

En cierta medida, pueden coincidir las figuras de «responsable de la información» con el «responsable del fichero». Hay que tener en cuenta que la determinación del carácter personal de los datos viene regulada por la normativa y matizada por una amplia jurisprudencia, acotando el margen de discrecionalidad del responsable de la información. En general, si las funciones no coinciden en la misma persona, el responsable de la información que se maneja estará supeditado al responsable del fichero.

El responsable del sistema debe aunar los requisitos sobre los datos de carácter personal que se manejen en el sistema de su competencia, tanto si son propios del organismo propietario del sistema como si son datos cedidos por un tercero.

No cabe esperar que se produzcan conflictos entre los responsables de la información y de los servicios por una parte y los responsables del fichero y del tratamiento por otra. En caso de discrepancia, los datos de carácter personal constituyen un objeto protegido de mayor rango y marcarán la pauta a seguir.

La figura del «responsable de seguridad» aparece en ambas normativas con un papel muy similar como persona que vela porque los sistemas efectivamente respondan a los requisitos establecidos. Los organismos públicos harán bien en hacer coincidir estas responsabilidades en una única figura, recopilando todas las funciones en la *Política de seguridad.*

Por último, no cabe esperar que se produzcan conflictos entre las obligaciones del responsable de seguridad derivadas de una u otra normativa, pues siempre deberá cumplirse la mayor de las exigencias derivadas de uno u otro.

Las normas y los procedimientos

La Administración Pública, en el desarrollo de sus funciones de servicio, policía o fomento, está sometida a diferentes normativas, de carácter estatal, autonómico o local. La particularidad de la actuación administrativa realiza-

da por medios electrónicos viene requiriendo, en los mismos tres niveles, la existencia de normas asimismo específicas, al objeto de acomodar aquellas funciones originarias a los condicionantes y medios electrónicos.

En este sentido, la LAECSP ha supuesto el punto de partida de un extenso compendio de regulaciones que vienen completando nuestro moderno ordenamiento jurídico administrativo-electrónico, entre las que cabe destacar: el Real Decreto 1671/2009, de 6 de septiembre, de desarrollo parcial de la LAECSP; el Real Decreto 3/2010, de 8 de enero, *por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica*, y el Real Decreto 4/2010, de de enero, *por el que se regula el Esquema Nacional de Interoperabilidad,* entre otras.

Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de la LAECSP, el ENS insta a los organismos de las AA. PP. a desarrollar, publicar y hacer valer normas de carácter interno a los propios organismos, tendentes a mejorar el nivel de seguridad de las informaciones que manejan y los servicios que prestan.

La necesidad de completar el marco normativo aparece explícitamente en muchos de los preceptos del ENS. Por ejemplo, en los artículos 14 («Gestión del personal»), 18 («Adquisición de productos de seguridad»), 21 («Protección de información almacenada y en tránsito»), 23 («Registro de actividad»), 34 («Auditoría de la seguridad»), 37 («Prestación de servicios de respuesta a incidentes de seguridad en las Administraciones Públicas»), Disposición adicional tercera («Comité de Seguridad de la Información de las Administraciones Públicas»), etc.

En concreto, en el anexo II del ENS («Medidas de seguridad») se encuentra la medida [org.2], que señala:

> *Normativa de seguridad [org.2].*
>
> *Se dispondrá de una serie de documentos que describan:*
>
> *a) El uso correcto de equipos, servicios e instalaciones.*
>
> *b) Lo que se considerará uso indebido.*
>
> *c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.*

Y en relación con los procedimientos de seguridad, nos encontramos también en el anexo II del ENS («Medidas de seguridad») la medida [org.3], que señala:

> *Procedimientos de seguridad [org.3].*
>
> *Se dispondrá de una serie de documentos que detallen de forma clara y precisa:*

a) *Cómo llevar a cabo las tareas habituales.*

b) *Quién debe hacer cada tarea.*

c) *Cómo identificar y reportar comportamientos anómalos.*

Esta habilitación a los organismos de las AA. PP. para que promuevan su propia normativa interna y de relación con terceros se alienta en varias medidas de seguridad del ENS: requisitos de acceso [op.acc.2], deberes y obligaciones [mp.per.2], concienciación [mp.per.3], formación [mp.per.4], protección del correo electrónico *(e-mail)* [mp.s.1], etc.

De acuerdo con lo previsto en el artículo 37 del ENS, el CCN-CERT investigará y divulgará las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones Públicas. Con esta finalidad, las series de documentos CCN-STIC, elaboradas por el Centro Criptológico Nacional, ofrecen normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de información en la Administración.

Se suele decir que lo que no se mide no puede gobernarse adecuadamente (31). Este aserto es igualmente predicable de la presencia y grado de cumplimiento de las normas de seguridad en los organismos públicos, razón por la cual conviene determinar qué métricas (32) habrán de proporcionar los indicadores adecuados que permitan a la dirección del organismo gestionar debidamente la influencia de las antedichas normas en la seguridad de la información y de los servicios prestados[11].

En relación con la normativa de seguridad, pueden utilizarse los siguientes indicadores clásicos:

- Proporción de normas implantadas sobre normas previstas.
- Número de violaciones graves de la normativa de seguridad reportadas.
- Encuesta de legibilidad percibida por los usuarios.
- Encuesta de utilidad percibida por los usuarios.

Como acabamos de mencionar, la normativa de seguridad podrá ser evaluada atendiendo a dos cualidades:

Legibilidad de la normativa: regularmente se puede preguntar a los usuarios a los que va dirigida la normativa de seguridad por la facilidad con la que se entienden los textos proporcionados. Las respuestas podrán valorarse en una escala de 1 a 5, de la siguiente forma: se interpreta perfectamente, se interpreta con cierta dificultad, puede generar inseguridad, no se entiende nada o genera confusión.

[11] Véase *Guía CCN-STIC 815: Métricas e indicadores en el ENS.*

Para calcular la legibilidad de un documento a partir de un conjunto de encuestas, pueden usarse los estadísticos mediana y desviación estándar de las puntuaciones obtenidas. Si la media o la mediana están por debajo de 3, debería revisarse la documentación, reescribiéndola de forma más clara para los lectores previstos. Por otra parte, si la desviación estándar es elevada, debería revisarse el colectivo al que va destinada pues puede que sea en sí heterogéneo y la documentación deba fraccionarse en partes o incluso redactarse de varias formas para que llegue a cada colectivo específico.

Utilidad de la normativa: regularmente se puede preguntar a los usuarios a los que va dirigida la normativa de seguridad por la utilidad que obtiene de los textos proporcionados. Las respuestas podrán valorarse en una escala de 1 a 5, de la siguiente forma: se encuentra rápidamente respuesta a lo que se necesita, aunque cuesta trabajo; leyéndolo con cuidado y detenimiento, se consigue; no está claro a qué caso se aplica cada cosa; da muchas cosas por sobreentendidas, o no sirve.

También en este caso, para calcular la utilidad de un documento a partir de un conjunto de encuestas, se usarán los estadísticos mediana y desviación estándar de las puntuaciones obtenidas. Si la media o la mediana están por debajo de 3, debería revisarse la documentación para ajustarla a los casos de uso previstos; si la desviación estándar es elevada, deberían revisarse los escenarios a los que se pretende aplicar pues puede que sean en sí heterogéneos y la documentación deba fraccionarse en partes o incluso redactarse de varias formas para que se adapte a cada caso de aplicación y los lectores sepan cuándo aplica cada cosa que se dice.

Ejemplo del contenido de una norma general de utilización de los recursos y sistemas de información de un organismo de la Administración

1. Introducción. Ámbito de aplicación.
2. Vigencia, Revisión y evaluación.
3. Referencias.
4. Utilización del equipamiento informático y de comunicaciones.
   - 4.1. Normas generales.
   - 4.2. Usos específicamente prohibidos.
   - 4.3. Normas específicas para el almacenamiento de información.
   - 4.4. Normas específicas para equipos portátiles y móviles.
   - 4.5. Uso de memorias/lápices USB (*pendrives*).

4.6. Grabación de CD y DVD.

4.7. Copias de seguridad.

4.8. Borrado y eliminación de soportes informáticos.

4.9. Impresoras en red, fotocopiadoras y faxes.

4.10. Digitalización de documentos.

4.11. Cuidado y protección de la documentación impresa.

4.12. Pizarras y *flipcharts.*

4.13. Protección de la propiedad intelectual.

4.14. Protección de la dignidad de las personas.

5. Uso eficiente de equipos y recursos informáticos.
6. Instalación de *software.*
7. Acceso a los sistemas de información y a los datos tratados.
8. Identificación y autenticación.
9. Acceso y permanencia de terceros en los edificios, instalaciones y dependencias del organismo.

   9.1. Normas.

   9.2. Modelo de protocolo de firma.

   9.3. Modelo de autorizaciones y habilitaciones personales.
10. Confidencialidad de la información.
11. Protección de datos de carácter personal y deber de secreto.
12. Tratamiento de la información.
13. Salidas de información.
14. Copias de seguridad.
15. Conexión de dispositivos a las redes de comunicaciones.
16. Uso del correo electrónico corporativo (33).

    16.1. Normas generales.

    16.2. Usos especialmente prohibidos.

    16.3. Recomendaciones adicionales.
17. Acceso a Internet y otras herramientas de colaboración.

    17.1. Normas generales.

    17.2. Usos específicamente prohibidos.

18. Incidencias de seguridad.
19. Compromisos de los usuarios.
20. Control de actuaciones sobre las bases de datos del organismo.
21. Uso abusivo de los sistemas de información.
    21.1. Uso abusivo del acceso a Internet.
    21.2. Uso abusivo del correo electrónico.
    21.3. Uso abusivo de otros servicios y sistemas del organismo.
22. Monitorización y aplicación de esta normativa.
23. Incumplimiento de la normativa.
24. Modelo de aceptación y compromiso de cumplimiento.
25. Compendio de normas.

Información y concienciación

Tradicionalmente, se ha visto la seguridad como una materia del entorno corporativo de las TIC, y no del entorno de la función o el «negocio» de la organización, y ha sido responsabilidad del departamento TIC. Todavía se puede apreciar en muchos organismos de la Administración que los procesos relacionados con la función del organismo son independientes de los procedimientos de seguridad y en la mayoría de los casos el criterio de la seguridad no se ha tenido en cuenta a la hora de diseñar los procesos relacionados con la función. Sin embargo, la seguridad de los sistemas de los organismos puede ser mejorada aumentando la concienciación, mejorando las habilidades y desarrollando una estrecha relación entre funcionalidad y seguridad.

La necesidad de concienciación ha sido reconocida en la Estrategia de Seguridad Nacional recientemente aprobada, la cual tiene entre sus líneas estratégicas relacionadas con la *ciberseguridad* «la implantación de una cultura de *ciberseguridad* sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento» (34).

La concienciación y la formación ayudan a desarrollar una estrecha relación de trabajo entre las áreas y unidades de los organismos y los departamentos TIC, proporcionando un lenguaje y procesos comunes que se pueden utilizar para desarrollar una protección efectiva de los activos de la organización. Aumentar la concienciación es potencialmente la acción más valiosa en la tarea continua de la seguridad. Aumentar la concienciación consigue que todo el personal pertinente tenga suficiente

conocimiento de los riesgos y del impacto potencial en el negocio o función de los fallos de seguridad. El personal necesita saber qué hacer para prevenir los ataques y qué hacer en caso de un incidente.

Numerosos sitios web y recursos de información sirven de ayuda a usuarios finales y al personal de la Administración para proteger los sistemas de información, aunque muy pocos abordan o explican de manera específica la naturaleza y el alcance de los diferentes tipos de *ciberataques*. En ocasiones, además, el número de recursos disponibles y la información que contienen puede resultar aplastante para el usuario, ya que la información y orientación pueden variar entre las diferentes entidades. Del mismo modo, algunos consejos son inconsistentes e incluso inadecuados para hacer frente a la naturaleza rápidamente cambiante de esta amenaza, como, por ejemplo, los consejos que afirman que la única contramedida necesaria es mantener actualizados los sistemas operativos y los programas antivirus.

Los esfuerzos de concienciación deberían seguir haciendo hincapié en la disponibilidad de información clara que pueda ser entendida por todos los participantes y, en especial, por aquellos que carecen o poseen mínimos conocimientos técnicos. Dada la constante naturaleza cambiante del *malware*, las actividades de concienciación deberían ser revisadas o actualizadas regularmente para que sigan siendo efectivas, lo que ayudaría a mejorar la conducta y prácticas *online* de usuarios así como su capacidad para protegerse de los *ciberataques*.

Una campaña de concienciación orientada a los empleados debe tener presente los diferentes aspectos del problema de la seguridad informática. Aunque cualquier acción es positiva, es realmente necesario que se planifiquen y detallen los objetivos a conseguir.

Los programas de «concienciación» no solo deben concienciar a las personas sino también formarlas y mostrar suficientes casos prácticos en los que se pueda apreciar la realidad.

El fin último de dichos programas es que el empleado público sepa identificar las situaciones de riesgo en el uso de las TIC y que adquiera hábitos de uso seguro de las mismas. Para ello, será imprescindible que alcance un cierto nivel de conocimiento sobre los motivos para llevar a cabo dichas conductas.

Los mensajes de concienciación de seguridad necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes, que se han recibido y entendido, se debe tener en cuenta las particularidades de cada organización y su entorno de trabajo. Aumentar la concienciación no es un ejercicio único, es un proceso continuo que provoca un cambio cultural que con el tiempo se irá integrando en el día a día del organismo.

El enfoque puede diferir de una organización a otra, pues la forma más eficaz de aumentar la concienciación en una organización dependerá de la cultura de la organización. En cualquier caso, para que un programa de concienciación en seguridad tenga éxito, hay dos elementos clave que son necesarios: la participación de la dirección y el establecimiento de objetivos claros y medibles.

La seguridad TIC puede llegar a ser complicada, abarca tecnologías y conceptos en general desconocidos y, en consecuencia, los mensajes claros deben formar parte de un programa de concienciación. Al determinar los mensajes de concienciación, es importante darse cuenta de que aumentar la concienciación e integrarla en el organismo es un proceso a largo plazo, no un esfuerzo de una vez (35) (36).

Es esencial que cualquier programa de concienciación de seguridad en un organismo esté correctamente planificado, ya que una sucesión de intentos mal planificados y mal ejecutados pueden obstaculizar los programas de seguridad. Para garantizar que un programa de concienciación está bien dirigido y ejecutado hay una serie de aspectos que deben considerarse y dar respuesta a las siguientes preguntas:

- ¿Cuál es el objetivo de concienciación de seguridad?
- ¿Cuál es el público objetivo?
- ¿Cómo funcionan las comunicaciones dentro de la organización?
- ¿Qué conocimientos existen en la organización con anterioridad?
- ¿Qué temas de concienciación necesitan tratarse?
- ¿Qué métodos de concienciación pueden usarse para transmitir el mensaje?
- ¿Cómo puede integrarse la concienciación de seguridad en la organización?
- ¿Cómo de bien es comprendido el mensaje?

Tener un objetivo específico de concienciación centrará los esfuerzos de difusión del mensaje clave en el público apropiado y permitirá medir el éxito del programa. Integrar la seguridad en cualquier organización lleva tiempo y el mejor enfoque es centrarse en los mensajes clave y construir lentamente y en profundidad la concienciación.

La formación del personal de la Administración

El nivel de formación necesario varía en función de los individuos y, en general, en los organismos públicos existen programas específicos de formación que combinan una serie de temas que pueden ser considerados para distintos públicos:

- Políticas y normas: se centra en las normas y la legislación.
- Procedimientos: detalla los procedimientos y cómo se relacionan con las políticas y las normas.
- Respuesta a incidentes: cubre lo que se debe hacer en caso de incidente.
- Arquitectura: cubre cómo los distintos sistemas están conectados entre sí y configurados, y será un tema con una fuerte componente técnica pero también procedimental, ya que esta actividad de formación deberá exponer claramente los flujos de información autorizados del organismo.
- Formación técnica detallada: cubre normalmente la seguridad TIC general.

En la Administración Pública española hay comparativamente pocos recursos diseñados específicamente para la formación en seguridad. De los cursos de seguridad TIC disponibles, encontrar cuál proporcionará un nivel adecuado de comprensión puede ser proceso difícil y largo. El análisis de las necesidades de formación es de gran ayuda en este ámbito y seleccionar cursos organizados por empresas y organizaciones profesionales reconocidas puede garantizar que se cumplan las necesidades de formación. Sin embargo, es poco probable que se oferte todo lo que se necesita y es probable que sea necesaria una mezcla de distintas actividades formativas. Los métodos típicos que se suelen utilizar son:

- Formación interna: las sesiones organizadas internamente a menudo proporcionan la formación más relevante, ya que se ocupan de temas específicos del organismo y pueden poner en contexto los conocimientos adquiridos externamente. Sin embargo, pueden consumir una gran cantidad de tiempo y valiosos recursos en su planificación y ejecución.
- Cursos de formación externos y formación aprobada de colaboradores: ya sea proporcionada por proveedores o por profesionales de la seguridad, son de carácter técnico y a veces difícil de relacionar con cuestiones específicas del puesto de trabajo. Hay una variedad de empresas y organismos profesionales que prestan certificaciones de seguridad tales como «Certificado CISA de Auditor de Sistemas de Información», «Certificación CISM de Director de Seguridad de la Información», «Certificado CISSP de Profesional de Seguridad de los Sistemas de Información (CISSP)», «Certificado GIAC de Garantía Global de la Información[12]», etc.

[12] Certified Information Systems Auditor (CISA), www.isaca.org; Certified Information Systems Security Professional (CISSP), www.isc2.org, y Global Information Assurance Certification (GIAC), www.giac.org.

- Formación *online* y seminarios web: se puede utilizar para formación de individuos y equipos con un coste relativamente bajo.
- Conferencias y talleres: asistir a conferencias es una buena manera de aprender acerca de la seguridad y muchos organismos que organizan conferencias suelen tener talleres de formación como parte del evento.
- Cursos de actualización: la formación no es algo puntual, se deben buscar cursos para garantizar que el personal se mantiene actualizado en los cambios, en las amenazas y en la tecnología y para mantener su nivel de destreza.
- Sesiones personales: se trata de una valiosa herramienta para los principales interesados, permitiendo que esas personas aprendan rápidamente y que el mensaje se entienda.
- Cursos de formación estructurados: pueden ser tanto externos como internos, y se centran en un tema u objetivo específico (p. ej., instalación y configuración de cortafuegos).
- Autoevaluación: la autoevaluación es una valiosa herramienta que permite a una organización obtener resultados de la formación en seguridad y medir el éxito de los planes de mitigación.
- Talleres multidisciplinares: reunir a diferentes partes interesadas de la organización para debatir las mejoras de la seguridad permite que se apliquen una amplia gama de experiencias y conocimientos a un problema, y puede poner de relieve las deficiencias que requieran ayuda externa.

Con independencia de las actividades de formación interna de los diferentes organismos, apoyadas o no por empresas especializadas, la Administración tiene instituciones propias para la formación de sus empleados públicos en el campo de la seguridad.

Instituto Nacional de Administración Pública

El Instituto Nacional de Administración Pública (INAP) tiene encomendadas las tareas de selección de los funcionarios de los cuerpos generales de la Administración General del Estado, la formación de directivos públicos y del resto de las personas que componen las organizaciones administrativas, así como la reflexión sobre las principales líneas de actuación de la Administración española.

El INAP es un organismo autónomo adscrito al Ministerio de Hacienda y Administraciones Públicas a través de la Dirección General de la Función Pública. Sus orígenes se remontan al Instituto de Estudios de Administración Local (IEAL), creado en 1940.

La misión del INAP es:

> *...crear conocimiento transformador en el sector público en beneficio de la sociedad, con el fin de propiciar la cohesión social y una democracia de alta calidad. Para alcanzar sus objetivos, el INAP cuenta con equipos transversales capaces de atraer ideas, personas y proyectos innovadores a los procesos de investigación, selección y formación, y actúa de acuerdo con los principios y valores de eficacia, aprendizaje en equipo, orientación al ciudadano, transparencia, ejemplaridad, autonomía y responsabilidad.*

El presupuesto total del INAP en 2011 fue de 146.071.100 €, de los cuales 18.375.400 € correspondieron a los gastos derivados de actividades propias del organismo y el resto, 127.695.700 €, correspondieron a créditos destinados a Formación para el Empleo de las Administraciones Públicas.

Las funciones principales que desarrolla el INAP se distribuyen en cuatro áreas de actividad: selección de funcionarios; formación y perfeccionamiento de empleados públicos; estudios y publicaciones, y relaciones internacionales. Además, organiza una amplia variedad de actividades docentes y académicas, de cooperación interadministrativa y de difusión en materia de Administración y políticas públicas, a través de jornadas, conferencias, encuentros y seminarios.

Actualmente, las cuatro grandes áreas de actividad del INAP son:

– Formación. La actividad formativa desarrollada por el INAP se ordena en torno a seis grandes programas formativos:

  - Directivos públicos: el INAP ha diseñado un programa para directivos que pretende ofrecer una formación de calidad para la mejora de la dirección pública. Las actividades formativas de este programa están dirigidas a los funcionarios de cuerpos y escalas del subgrupo A1, y al personal laboral fijo asimilado de las Administraciones Públicas.
  - Empleados públicos en funciones de gestión, de administración y auxiliares: el INAP ofrece actividades formativas que versan, dentro de estas funciones, sobre la organización, la actividad y el procedimiento administrativo, la gestión de los recursos humanos, la administración económica, la administración electrónica, las políticas públicas y las habilidades profesionales.
  - Administración local: una formación dirigida a los empleados públicos locales con el objetivo de adquirir los conocimientos y habilidades necesarias para una gestión de calidad de los servicios públicos locales.
  - Administración electrónica: el INAP incluye una amplia oferta de actividades formativas para todos los empleados públicos, como respuesta a la demanda y las necesidades de formación existente en administración electrónica.

- Idiomas y lenguas cooficiales: el INAP incorpora, en su oferta formativa, cursos de inglés, francés y alemán. Asimismo incluye, entre sus actividades formativas, la enseñanza de la lengua cooficial correspondiente a los funcionarios de la Administración General del Estado destinados en las comunidades autónomas bilingües.
- Cursos selectivos para funcionarios en prácticas: tienen como finalidad primordial la adquisición de conocimientos en orden a la preparación específica, para el ejercicio de sus funciones, de los aspirantes que han superado las pruebas selectivas.

– Selección:

- El INAP, a través de la Comisión Permanente de Selección, es responsable de la gestión de los procesos selectivos de los funcionarios de los cuerpos y escalas adscritos al Ministerio de Hacienda y Administraciones Públicas.
- También presta apoyo administrativo y técnico a los tribunales de los cuerpos y escalas del subgrupo A1.

– Estudios, publicaciones e investigación:

- El INAP dispone de una biblioteca especializada en Ciencia de la Administración y Derecho Público. Cuenta con más de 230.000 volúmenes y publicaciones periódicas. Posee, además, un fondo antiguo que integra más de 9.000 obras de los últimos cinco siglos.
- El INAP, desde su creación, mantiene una importante actividad editorial en sus materias de referencia y ha publicado más de 700 obras. Todas ellas se encuentran digitalizadas y disponibles para el público.
- Actualmente, el INAP publica las siguientes revistas: *Revista de Estudios de la Administración Local y Autonómica* (REALA), *Gestión y Análisis de Políticas Públicas* (GAPP), *Documentación Administrativa* (DA) y *Cuadernos de Derecho Público* (CDP)
- La actividad investigadora del INAP se realiza a través de la constitución de grupos de investigación, la convocatoria de premios y becas de formación y la realización de jornadas y seminarios de debate.

– Relaciones internacionales:

- El INAP desarrolla una amplia actividad de relaciones internacionales a través de la formación de empleados públicos extranjeros –principalmente iberoamericanos– en colaboración con otras instituciones, la participación en organizaciones y organismos internacionales especializados en el campo de la Administración Pública y las relaciones bilaterales con escuelas e institutos de formación extranjeros.

La formación ofrecida por el INAP en materia de seguridad de las tecnologías de la información y comunicaciones cuenta con la colaboración del Centro Criptológico Nacional (CCN-CNI). Tal colaboración fue formalizada

por convenio, suscrito el 5 de julio de 2011, entre la Secretaría de Estado para la Función Pública, el Centro Criptológico Nacional y el INAP.

Federación Española de Municipios y Provincias

La Federación Española de Municipios y Provincias (FEMP) es la asociación de entidades locales de ámbito estatal con mayor implantación, que agrupa ayuntamientos, diputaciones, consejos y cabildos insulares, en total 7.324, que representan más del 90% de los Gobiernos locales españoles.

Constituida al amparo de lo dispuesto en la disposición adicional quinta de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, fue declarada como asociación de utilidad pública mediante acuerdo de Consejo de Ministros de 26 de junio de 1985.

La Subdirección de Formación de la Dirección General de Estudios y Formación es la encargada de la elaboración del Plan de Formación Continua.

El Plan de Formación Continua que la FEMP elabora cada año está dirigido fundamentalmente al personal de las corporaciones locales, con una clara intención de formar en cuestiones muy especializadas y que tengan impacto directo en el futuro del municipalismo. Las necesidades formativas se detectan como una actividad más de las comisiones sectoriales que trabajan en la FEMP y a partir de las novedades normativas y legislativas que se van produciendo. Asimismo están alineadas con el plan estratégico de la organización.

El objetivo del Plan es «la modernización y el desarrollo en la Administración local y por lo tanto la mejora en los servicios proporcionados a los ciudadanos, mediante el aumento de la cualificación y la mejora de las competencias de los empleados públicos locales».

Todos los empleados públicos locales pueden tener acceso a los cursos del Plan FEMP, con independencia de su relación laboral o el nivel de su puesto. Los cursos de formación continua son completamente gratuitos y el criterio de selección principal de los asistentes es la relación entre sus funciones y el perfil definido para el curso.

La FEMP cuenta además con una plataforma *online* para su actividad formativa en la página http://www.goblonet.es/formacion.

Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN) es un organismo, adscrito al Centro Nacional de Inteligencia (CNI), creado en el año 2004 con el fin de garantizar la seguridad TIC en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

Su ámbito de competencia está definido por el siguiente marco normativo:

- Ley 11/2002, 6 de mayo, Reguladora del Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN) y que tiene entre otras misiones actuar contra el *ciberespionaje*, neutralizando las actividades de contrainteligencia y la seguridad de los sistemas de información del país, y protegiendo el patrimonio tecnológico de España.
- Real Decreto 421/2004, 12 de marzo, que regula y define el ámbito y funciones del Centro Criptológico Nacional (CCN).
- Orden del Ministerio de la Presidencia PRE/2740/2007, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, y que confiere al CCN la capacidad de actuar como organismo de certificación (OC) de dicho Esquema.
- Real Decreto 03/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad, en el que se establecen los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte del CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos. Así mismo, en sus artículos 36 y 37 articula en torno al CCN-CERT la capacidad de respuesta ante incidentes en las Administraciones Públicas.
- Comisión Delegada del Gobierno para Asuntos de Inteligencia, que define anualmente los objetivos del CNI mediante la Directiva de Inteligencia, que marca la actividad del Centro.

Desde su creación en el año 2004, el Centro Criptológico Nacional ha ido adecuándose y, en la medida de lo posible, adelantándose a una realidad cambiante en donde las *ciberamenazas* se incrementan día a día, varían (en función de la motivación de los atacantes o sus objetivos), se modifican los métodos de ataque, aparecen nuevas vulnerabilidades o se renuevan los dispositivos de los usuarios, los servicios ofrecidos a través de Internet o la tecnología empleada.

En esta evolución constante, y a medida que las amenazas y los riesgos cobran mayor importancia y alcanzan una mayor repercusión en todas las capas de la sociedad, la creación de la Capacidad de Respuesta a Incidentes, CCN-CERT, (y sus múltiples servicios orientados a una defensa preventiva frente a los *ciberataques* a las Administraciones Públicas y empresas estratégicas) y del Organismo de Certificación (OC) son la respuesta más importante en los últimos años al desafío planteado.

Dentro de esta actualización constante, y en virtud de las funciones asignadas al CCN, en los últimos diez años se han ido elaborando normas,

instrucciones, guías y recomendaciones para mejorar el grado de *ciberseguridad* en España. De este modo, a finales del año 2012 existían 223 documentos enmarcados en la serie CCN-STIC, con normas, procedimientos y directrices técnicas para optimizar la seguridad de las tecnologías de la información en nuestro país. De ellas, 73 se han elaborado o actualizado en los dos últimos años y abarcan todo tipo de aspectos de la seguridad, siendo algunas de difusión limitada para el personal de la Administración Pública y empresas estratégicas, y otras de difusión abierta para todos los usuarios que accedan al portal del CCN-CERT (www.ccn-cert.cni.es). Entre estas, se encuentran toda la serie CCN-STIC 800, elaboradas en colaboración con el Ministerio de Hacienda y Administraciones Públicas, de desarrollo del Real Decreto 3/2010, de 8 de enero, *por el que se regula el Esquema Nacional de Seguridad.* También son públicas las guías de la herramienta PILAR (versión 5.2 de 2012) y las destinadas a la seguridad de los dispositivos móviles (iPhone, Android o iPad).

Todos los documentos de la serie CCN-STIC son actualizados periódicamente y enviados a más de 300 organismos diferentes de la Administración (aparte de contar todos ellos con acceso a la parte privada del portal del CCN-CERT donde se encuentran).

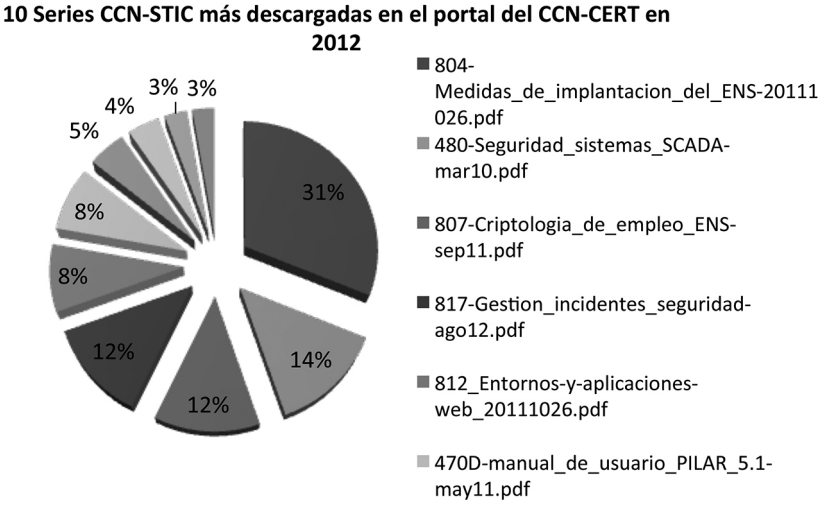


Figura 3.8. Los diez documentos de la serie CCN-STIC más descargados en el portal del CCN en 2012.

Disponer de personal cualificado en todos los niveles de la Administración (dirección, gestión e implantación) es considerado por el CCN un aspecto fundamental para proteger los sistemas de las *ciberamenazas*. De ahí que una de las funciones principales a lo largo de sus casi diez años de historia haya sido formar al personal de la Administración a través de

un amplio programa, en el que se incluyen los cursos STIC (presenciales, a distancia y *online*), jornadas de sensibilización, participación en ponencias y mesas redondas, etc.

Evolución de la oferta formativa del CCN

	2008	2009	2010	2011	2012	TOTAL
Alumnos	380	450	510	500	500	2.340
Cursos presenciales	17	18	17	14	14	80
Horas lectivas	1.200	1.400	1.200	900	900	5.600
Cursos *online*	-	1	3	5	6	15
Jornadas de sensibilización	2	4	3	6	7	22
Participación en mesas redondas/jornadas	8	10	15	15	40	88

Contenido de la oferta formativa del CCN en 2011-2012

- Cursos informativos y de concienciación en seguridad.
  - IX Curso de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) (con fase *online*).
- Cursos básicos de seguridad.
  - VII Curso Básico STIC - Infraestructura de Red.
  - VII Curso Básico STIC - Base de Datos.
- Cursos específicos de gestión de seguridad.
  - IV Curso *Common Criteria*.
  - IX Curso de Gestión STIC - Implantación del ENS (fase *online*).
  - XXIII Curso de Especialidades Criptológicas (fase por correspondencia).
- Cursos de especialización en seguridad.
  - VII Curso STIC - Seguridad en Redes Inalámbricas.
  - I Curso STIC - Seguridad en Dispositivos Móviles (nuevo en 2012).
  - IV Curso STIC - Seguridad en Aplicaciones Web.
  - VIII Curso STIC - Cortafuegos.
  - VIII Curso STIC - Detección de Intrusos.
  - IX Curso Acreditación STIC - Entornos Windows.
  - V Curso STIC - Búsqueda de Evidencias.
  - VII Curso STIC - Inspecciones de Seguridad.
  - III Curso STIC - Herramienta PILAR (fase *online*).

Todos estos cursos están accesibles en la parte privada del portal del CCN-CERT (www.ccn-cert.cni.es).

Además, en estos dos últimos años, el Centro Criptológico Nacional ha ido ampliando su oferta formativa, adaptándose a las necesidades de muchos usuarios y facilitando, a través de un método de *e-learning*, algunos de sus cursos más demandados. De esta forma, a finales de 2012, estaban disponibles en el portal del CCN-CERT los siguientes cursos:

- Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones STIC.
- Curso PILAR (Manejo de herramienta / Funciones más usadas).
- Curso Básico de Seguridad. Entorno Windows.
- Curso Básico de Seguridad. Entorno Linux.
- Curso del Esquema Nacional de Seguridad (acceso público).
- Curso de Análisis y Gestión de Riesgos de los Sistemas de Información (acceso público).

En apenas tres años desde la puesta en funcionamiento del primero de los cursos, se ha conseguido un total de 1.887 alumnos y más de 30.000 accesos al apartado del portal web.

Evolución de los cursos on-line (www.ccn-cert.cni.es)

Mes	2010	2011	2012	TOTAL
Número de accesos a los cursos *online*	5.430	13.876	11.735	30.681
Número de alumnos inscritos	891	1.511	1.887	4.289

Bibliografía

1. ISO Guide 73. *Risk management: Vocabulary.* 2009.
2. LAVELL, Allan. *Sobre la gestión del riesgo: apuntes hacía una Definición.* [En línea] http://www.bvsde.paho.org/bvsacd/cd29/riesgo-apuntes.pdf.
3. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. MAGERIT, versión 3.0. *Metodología de análisis y gestión de riesgos de los sistemas de información.* Secretaría General Técnica, Ministerio de Hacienda y Administraciones Públicas, 2012. NIPO: 630-12-171-8.
4. KEIPI, Juhani, MORA CASTRO, Sergio y BASTIDAS, Pedro. *Gestión de riesgo derivado de amenazas naturales en proyectos de desarrollo.* Banco Interamericano de Desarrollo, 2005.
5. NIST SP 800-30. *Risk Management Guide for Information Technology Systems.*
6. Centro Criptológico Nacional. *CCN-CERT. Informe. Ciberamenazas 2012 y tendencias 2013.* Mayo de 2013. www.ccn-cert.cni.es. CCN-CERT IA 09/13.

7. Guía CCN-STIC 301. *Requisitos de seguridad de las TIC.*
8. FIPS 200. *Minimum Security Requirements for Federal Information and Information Systems.* Marzo de 2006.
9. Guía CCN-STIC 400. *Manual de seguridad de las tecnologías de la información y comunicaciones.*
10. Guía CCN-STIC 402. *Organización y gestión para la seguridad de los sistemas TIC.*
11. Real Decreto 3/2010, de 8 de enero, *por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.*
12. Guía CCN-STIC 805. *ENS. Política de seguridad.*
13. Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
14. Real Decreto 1720/2007, de 21 de diciembre, *por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
15. Decisión del Consejo 2001/264/CE, de 19 de marzo de 2001, *por la que se adoptan las normas de seguridad del Consejo.*
16. Guía CCN-STIC 803. *ENS. Valoración de los Sistemas.*
17. Real Decreto 1671/2009, de 6 de septiembre, *de desarrollo parcial de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.*
18. OECD. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* París: s. n., 2002.
19. UNE - ISO/IEC 27002:2005. *Código de buenas prácticas para la gestión de la seguridad de la información.*
20. UNE - ISO/IEC 27001:2007. *Especificaciones para los sistemas de gestión de la seguridad de la información.*
21. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
22. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
23. Real Decreto 1553/2005, de 23 de diciembre, *por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.*
24. Guía CCN-STIC 804. *ENS. Guía de implantación.*
25. Guía CCN-STIC 806. *ENS. Plan de adecuación.*
26. Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
27. Guía CCN-STIC 201. *Estructura de seguridad.*
28. Guía CCN-STIC 801. *ENS. Responsables y funciones.*
29. NIST SP 800-12. *An Introduction to Computer Security: The NIST Handbook.*
30. Orden Ministerial 76/2002, de 18 de abril, *por la que se establece la política de seguridad para la protección de la información del Ministerio*

de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones. BOE de 29 de abril de 2002.

31. Guía CCN-STIC 807. *ENS. Inspección de las medidas de seguridad.*
32. Guía CCN-STIC 815. *Métricas e indicadores en el ENS.*
33. Guía CCN-STIC 814. *Seguridad en correo electrónico.*
34. ESN. *Estrategia de Seguridad Nacional 2013. Un proyecto compartido.* Mayo de 2013.
35. NIST SP 800-100. *Information Security Handbook: A Guide for Managers.*
36. NIST SP 800-53. *Recommended Security Controls for Federal Information Systems and Organizations.*

La conciencia de *ciberseguridad* en las empresas

Por Oscar Pastor Acosta

Capítulo cuarto

«Quien piensa que la tecnología puede solucionar sus problemas de seguridad, está claro que ni entiende los problemas ni entiende la tecnología.»

Bruce Schneier (1963-...)

Introducción

No cabe duda de que el extraordinario desarrollo experimentado por las tecnologías de la información y las comunicaciones (TIC) ha convertido al ciberespacio en un recurso vital para el normal desarrollo de la sociedad actual, ya que favorece y simplifica la relación entre ciudadanos, Administraciones Públicas y empresas, constituyendo una pieza básica para la prestación de servicios esenciales para la comunidad. Su creciente nivel de importancia ha suscitado desde hace tiempo el interés de organismos internacionales del máximo nivel, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), que considera Internet como un «elemento fundamental para impulsar el desarrollo económico y el bienestar social, así como para fortalecer la capacidad de las sociedades para mejorar la calidad de vida de sus ciudadanos» (1).

Sin embargo, estos beneficios tienen como contrapartida una dependencia cada vez mayor del ciberespacio, lo que también supone un aumento del nivel de exposición a sus amenazas y vulnerabilidades. Por tanto, la relevancia de las redes de comunicaciones en el mundo actual lleva asociada, de manera inseparable, la necesidad de protegerlas ante los incidentes de cualquier naturaleza que puedan alterar su operación, ya que las consecuencias de la interrupción o alteración de las redes de comunicaciones podrían afectar gravemente a funciones sociales fundamentales, tal y como reconoce la recientemente aprobada Estrategia de Seguridad Nacional (2):

> *España está expuesta a los ciberataques, que no solo generan elevados costes económicos, sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad.*

Esto se ha reflejado a nivel internacional en las correspondientes estrategias nacionales de *ciberseguridad*, entre las que cabe mencionar los documentos elaborados por los Gobiernos de Estados Unidos (3), Canadá (4), Japón (5), Reino Unido (6), Alemania (7), Francia (8) y Holanda (9). Así, por ejemplo, en la Estrategia de Ciberseguridad del Reino Unido –*Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space* (6)–, publicada en junio de 2009, ya se afirmaba que «el coste medio de un incidente de seguridad de la información para una PYME era de entre 10.000 y 20.000 libras y para una gran empresa, con más de 500 empleados, podía llegar a ser de entre un millón y dos millones».

En su posterior revisión de noviembre de 2011 –*The UK Cyber Security Strategy Protecting and Promoting the UK in a digital world* (10)–, se indicaba que «el coste para el Reino Unido de los delitos cibernéticos podrían llegar a ser del orden de 27.000 millones de libras al año». Este dato provenía de un informe (11) realizado conjuntamente con la Cabinet Office[1], en el que se desglosaban dichos costes indicando que los debidos a robos de la propiedad intelectual ascendían a más 9.000 millones de libras al año, mientras que los que tienen su origen en el espionaje industrial se elevaban a casi 8.000 millones de libras al año.

Resulta, por tanto, evidente la importancia que para el buen desarrollo de las empresas supone un apropiado conocimiento de su *ciberseguridad,* es decir, una concienciación adecuada de su situación en el ciberespacio y de las amenazas que este conlleva para su normal desarrollo en este nuevo medio.

[1] Oficina del Gabinete, que apoya al primer ministro y al viceprimer ministro para garantizar el funcionamiento eficaz del Gobierno británico. Es la sede corporativa del Gobierno, en colaboración con el Ministerio de Hacienda, y constituye un departamento ministerial con el apoyo de 19 agencias y organismos públicos. https://www.gov.uk/government/organisations/cabinet-office.

Contenido

El presente capítulo abordará los aspectos más importantes que las empresas deben considerar para alcanzar una adecuada concienciación de su *ciberseguridad.* Para ello, se revisarán cada uno de los grupos conceptuales que todo buen análisis de riesgos debe abordar, esto es, los activos de las empresas, como elementos que aportan valor a las mismas; sus amenazas y vulnerabilidades, que pueden ocasionar impactos negativos en los anteriores, así como las salvaguardas, que pueden reducir el riesgo de que dichos impactos negativos se materialicen finalmente.

El presente análisis no pretende realizar una descripción exhaustiva ni una clasificación pormenorizada de los anteriores conceptos, que ya han sido abordados con más detalle en capítulos anteriores del presente documento, pero sí pararse a revisar con detenimiento aquellos elementos que son de especial significación para la *ciberseguridad* de las empresas.

Así, al abordar los principales activos que las empresas exponen en el ciberespacio, se analizarán sus activos intangibles, como son la propiedad intelectual, la reputación o la imagen de marca, y el creciente valor que estos elementos están tomando en el conjunto de activos de las empresas, frente a los activos materiales tradicionales como son edificios, materiales, existencias de productos, etc. También se revisarán las infraestructuras críticas como activos cuya propiedad recae mayoritariamente en empresas privadas, pero cuya protección se ha convertido en una cuestión de Seguridad Nacional, dado que un impacto negativo sobre los mismos podría afectar no solo a la empresa que los opera sino a la sociedad en su conjunto.

A continuación, se abordarán las amenazas provenientes del ciberespacio a las que se enfrentan los activos de las empresas previamente analizados. Se revisarán los ataques reales o potenciales de los que son o pueden ser objeto los citados elementos, su finalidad y sus principales características, pues solo así las empresas pueden alcanzar una conciencia de su situación en el ciberespacio que les permita mejorar su *ciberseguridad*.

También se examinarán las principales vulnerabilidades que las tecnologías más avanzadas del ciberespacio suponen para las empresas. Las organizaciones del siglo XXI, si quieren garantizar su eficiencia y perdurar en el tiempo, no pueden prescindir de los servicios y funcionalidades que estas tecnologías proporcionan. Sin embargo, deben implementarlas con el conocimiento suficiente de los riesgos intrínsecos que conllevan para mejor gestionar su exposición a los mismos. En este capítulo, se abordará el análisis de nuevas funcionalidades y servicios como el *cloud computing*[2]

[2] «Computación en la nube», o simplemente «la nube», es un nuevo paradigma en los sistemas de información que permite ofrecer capacidades de computación a través de redes de comunicaciones en forma de servicios.

y el *big data*[3]; la «consumerización»[4] de los terminales de usuario y su movilidad en las redes empresariales, o lo que se ha denominado con el acrónimo anglosajón BYOD[5], así como las redes sociales como lugar donde hacer negocios, en las que la presencia empresarial es cada vez mayor.

Vistos los elementos que conjuntamente colaboran a conformar los riesgos a los que las empresas se enfrentan en el ciberespacio, posteriormente se analizarán las principales herramientas de que disponen las empresas para gestionar dichos riesgos hasta limitarlos a niveles aceptables. En este apartado se revisarán las buenas prácticas de *ciberseguridad,* entre las que se incluyen el uso de productos certificados y el establecimiento de sistemas de gestión de la seguridad de la información.

Por último, para concluir el presente capítulo, se analizará cómo se podría abordar en las empresas un adecuado programa de concienciación de *ciberseguridad* como herramienta mediante la que difundir a lo largo de la organización los conceptos de *ciberseguridad* analizados en el presente capítulo, asegurando que los diferentes miembros disponen del conocimiento adecuado, según su rol y responsabilidad, para asegurar una adecuada conciencia de la situación de la empresa en el ciberespacio que permita a esta garantizar su éxito en este nuevo medio.

Las empresas en el ciberespacio

Activos de las empresas en el ciberespacio

Activos intangibles: propiedad intelectual, reputación y marca

Desde hace mucho tiempo, las empresas reconocen la importancia de los elementos intangibles como el conocimiento, la propiedad intelectual, la

[3] Que podría traducirse como «grandes datos», hace referencia a los sistemas de información que manipulan grandes volúmenes de datos, que superan la capacidad del *software* habitual para ser capturados, gestionados y procesados en un tiempo razonable.

[4] Término proveniente del inglés *consumerization,* todavía no recogido en el Diccionario de la Real Academia Española, pero ya de amplio uso en los foros y congresos tecnológicos, expresa la creciente tendencia de las empresas de nuevas tecnologías de la información a abordar en primer lugar el mercado de consumo y posteriormente el de las organizaciones empresariales y gubernamentales. El surgimiento de los mercados de consumo como el principal impulsor de la innovación tecnológica de la información supone un cambio radical en la industria de TI, donde las grandes empresas y las organizaciones gubernamentales dominaron las primeras décadas del desarrollo y uso de los sistemas de información y comunicaciones.

[5] Acrónimo de «*Bring Your Own Device*», que puede traducirse como «trae tu propio dispositivo», y hace referencia a las políticas empresariales en las que los empleados pueden llevar sus propios dispositivos informáticos (portátiles, móviles, tabletas, etc.) a su lugar de trabajo para tener acceso a recursos empresariales, tales como correos electrónicos, bases de datos y archivos en servidores corporativos, al tiempo que son usados con aplicaciones personales.

reputación, la imagen corporativa, la imagen de marca o la responsabilidad social corporativa como elementos críticos para alcanzar los objetivos del negocio manteniendo los niveles de competitividad adecuados.

En la actualidad, las empresas se enfrentan a continuos cambios y a una creciente complejidad en las sociedades con las que interactúan (12). Estas transformaciones del medio afectan a las relaciones de la empresa con su entorno, en las que se empiezan a tener en cuenta aspectos que anteriormente no se consideraban y que van desde su imagen o cómo se proyecta su actitud social hasta cómo contaminan o sus comportamientos solidarios.

Estas nuevas categorías han influido en la forma de pensar de las organizaciones, que se encuentran condicionadas por el marco institucional que les rodea. Todo esto pone de manifiesto que las empresas se encuentran en un proceso dinámico por el cual buscan establecer su aceptación, evolucionando de forma acompasada con los cambios en las normas, creencias, valores y definiciones sociales (13). Por tanto, las organizaciones, en general, y las empresas, más en concreto, están en un progresivo cambio de comportamientos y actitudes en consonancia con las continuas transformaciones de su entorno. Esta sincronización les va a repercutir en una constante aceptación por parte tanto de aquellos elementos vinculados directamente con la empresa como de la sociedad en general.

Tradicionalmente, el valor de una empresa estaba fundamentado en su capacidad de hacer. Su competitividad se asociaba a los recursos materiales y su valor dependía de esos elementos asociados principalmente a lo tangible y lo material. Desde hace años, y de forma creciente, ese valor se basa en el saber hacer y cómo se transmite dicho saber. La competitividad es fruto del conocimiento que la empresa atesora y de cómo lo explota.

Desde hace tiempo, se vienen realizando estudios e investigaciones en universidades norteamericanas sobre la generación de valor en las empresas (14), viniendo a confirmar que, al menos en los Estados Unidos, se ha invertido la relación entre el valor de los activos tangibles e intangibles de las empresas entre 1929 y 1999, pasando de una relación de porcentajes del 70% tangible y el 30% intangible, a justo la contraria, un 70% intangible y un 30% tangible. En algunos de estos mismos estudios se augura incluso que el valor de los intangibles empresariales alcanzará en un futuro hasta el 85% del valor total de algunas empresas de los Estados Unidos.

Varios estudios del profesor Kaplan (15), creador de una de las herramientas más exitosas para la gestión integral de las empresas como son los cuadros de mando, corroboran los datos anteriores, indicando que el valor de los intangibles de una organización puede llegar a alcanzar hasta el 75% del valor de la misma.

Un claro ejemplo de esta situación se evidencia en la valoración de las marcas que realiza la empresa Interbrand[6]. Así, por ejemplo, en su *ranking* anual de las marcas más importantes de 2011, la empresa Coca-Cola está valorada en 71.861 millones de dólares. Lo más relevante de esta valoración es que, según expertos en temas bursátiles, los activos de la marca no superan el 10% de su valor intangible (16).

Si revisamos con más detenimiento el significado de «activo intangible», podemos ver que, para el IASB[7] (Internacional Accounting Standards Board), solo se puede hablar de activos intangibles cuando la empresa espera obtener de ese activo beneficios económicos futuros y, además, es un recurso controlado por dicha empresa, ya que de no existir tal control no puede hablarse de activo como tal.

En la figura 4.1 se muestra una posible clasificación de los activos intangibles de una compañía (17).

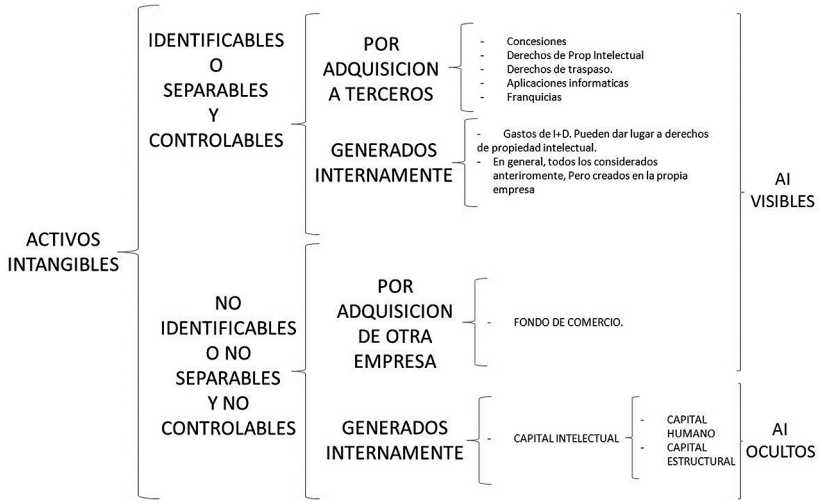


Figura 4.1: Clasificación de los activos intangibles de una compañía (fuente: D. Nevado Peña, 2002).

Partiendo de esta clasificación inicial, conviene establecer una definición de cada uno de los diferentes activos intangibles, como son la imagen corporativa y de marca, la reputación, el conocimiento y la propiedad intelectual, así como la responsabilidad social corporativa, para entender mejor qué comprenden.

En lo que se refiere a los conceptos de imagen, marca y reputación, algunos autores (18) establecen las siguientes definiciones:

[6] http://www.interbrand.com/.
[7] http://www.ifrs.org/Pages/default.aspx.

- Identidad corporativa: consiste en los atributos que definen a una compañía, tales como su personal, sus productos y sus servicios.
- Identidad de marca: elemento distintivo que se extiende por toda una empresa (que también puede tener otras «marcas» asociadas a múltiples productos). Pretende trasmitir las expectativas de lo que la compañía ofrecerá en términos de productos, servicios y experiencias.
- Imagen: es un reflejo de la identidad corporativa y su identidad de marca; cómo se proyecta la organización en su entorno (clientes, inversores, empleados...). Una organización puede tener diferentes imágenes.
- Reputación: la representación colectiva de las múltiples imágenes de una compañía, construida con el tiempo y basada en los programas de desarrollo de reputación de la organización.

Respecto al conocimiento, son varios los autores (19) que lo definen como el material intelectual –la información, la propiedad intelectual y la experiencia–, que puede utilizarse para crear valor, constituyéndose así como el capital intelectual de las compañías. Sería, por tanto, la fuerza cerebral colectiva. Tiene como característica su dificultad para ser identificado y, aún más, para ser distribuido eficazmente. Sin embargo, aquellas empresas que lo encuentran y explotan tienen garantizado su triunfo. Por tanto, en nuestra actual sociedad de la información, la riqueza es producto principalmente del conocimiento; este se ha convertido en la materia prima fundamental de la economía actual y genera sus productos más importantes.

Por otro lado, en el campo de la comunicación empresarial, se ha producido en los últimos años un cambio radical (20). Tradicionalmente, la comunicación de las empresas tenía dos expresiones casi exclusivas: las relaciones informativas y la comunicación de *marketing* o de producto, cuya expresión más genuina fue siempre la publicidad.

Esta situación se mantuvo hasta los primeros años 90, período en el que las dificultades de la industria publicitaria pusieron en entredicho la eficacia de la publicidad como elemento creador de valor, sumiendo al sector en una profunda crisis que ha arrastrado durante más de una década. En ese momento emerge con fuerza el concepto de imagen corporativa y el inicio de lo que se ha venido a denominar la emergencia de los intangibles empresariales y, muy especialmente, de la reputación corporativa.

Es por ello que, a los anteriores elementos intangibles, debemos añadirles el de responsabilidad social corporativa (RSC) por la importancia que está tomando en los últimos años. Fue incorporada en 2001 en el Libro Verde de la Comisión Europea (21) como consecuencia del mandato del Consejo Europeo celebrado en marzo del 2000 en Lisboa, en el que se afirma que se trata esencialmente de «un concepto con arreglo

al cual las empresas deciden voluntariamente contribuir al logro de una sociedad mejor y un medio ambiente más limpio», y se define como «la integración voluntaria por parte de las empresas de las preocupaciones sociales y medioambientales en sus operaciones comerciales y sus relaciones con sus interlocutores».

La razón de incorporar este elemento intangible es la importancia que el cumplimiento de esta función por parte de las organizaciones tiene para la sociedad, así como los graves perjuicios que el incumplimiento de la misma puede acarrear en términos de afectación a la reputación y a los resultados de las organizaciones. Valgan como ejemplo los recientes accidentes producidos en fábricas textiles en Bangladesh (22) y cómo la puesta en conocimiento del público de las condiciones de trabajo del personal de esas factorías ha afectado directamente a la reputación, imagen y ventas de las marcas que fabricaban en esas factorías. Todo esto ha promovido un acuerdo de cinco grandes grupos textiles, entre ellos el español Inditex (23), sobre seguridad y contra incendios para evitar tragedias como la ocurrida en Bangladesh el pasado 24 de abril de 2013.

En el marco de la gestión directa de las organizaciones, se debe tener en cuenta, además, que en el año 2005 entraron en vigor las Normas Internacionales de Contabilidad (NIC), de obligado cumplimiento para todas las empresas cotizadas de la Unión Europea, así como las Financial Accounting Standards, que son las normas de contabilidad financiera en Estados Unidos y Canadá, entre otros países, y exigen a las empresas una estimación del valor económico financiero de sus activos intangibles. Esta estimación se hace difícil: primero, porque no hay consenso sobre lo que se entiende por activo intangible, y, en segundo lugar, porque tampoco existe dicho consenso sobre cómo estimar el valor económico de este tipo de activos.

En este sentido, las propias normas NIC incluyen tanto las definiciones como los criterios necesarios para que cualquier «recurso» intangible pueda considerarse un «activo» y, en definitiva, pueda ser capitalizado (24). La NIC 38 define un activo intangible como todo aquel «activo identificable, de carácter no monetario y sin apariencia física». La propia definición recoge las primeras dos condiciones que deben cumplirse para que un recurso intangible, adquirido o generado internamente por la empresa, sea reconocido en el balance empresarial: que el recurso intangible cumpla con la definición de «activo» del marco conceptual; y que sea identificable.

Junto a estas condiciones, la NIC 38 incluye dos más, en línea con los requisitos generales de reconocimiento de cualquier activo, recogidos en el marco conceptual: que sea «probable» que los beneficios económicos futuros que se han atribuido al activo fluyan a la entidad, y que el coste del activo pueda medirse de forma «fiable». Para evaluar el grado de cumpli-

miento de estos dos últimos requisitos, la empresa recurrirá a «hipótesis razonables y fundadas» que representen de la mejor forma posible los beneficios económicos que se esperan obtener del activo.

A raíz de esta aplicación, las empresas se enfrentan a la necesidad de emitir información financiera completa del valor de los intangibles. La mayoría de las técnicas de los expertos en el tema se pueden agrupar en cuatro categorías (25) de metodologías de medición de este tipo de elementos:

- Métodos directos de capital intelectual: calculan el importe del valor de los activos intangibles mediante la identificación de sus diversos componentes. Una vez que dichos componentes han sido identificados, pueden ser directamente valorados, ya sea de forma individual o como un coeficiente agregado.
- Métodos de capitalización de mercado: calculan la diferencia entre la capitalización de mercado de la empresa y su capital contable como el valor de su capital intelectual, o bien de sus activos intangibles.
- Métodos de retorno sobre los activos: a través de estas técnicas se obtiene una utilidad promedio del año para los activos intangibles. Dividiendo el mencionado promedio de activos intangibles entre el costo de capital promedio de la compañía o por una tasa de interés, se puede obtener un valor estimado de sus activos intangibles o capital intelectual.
- Métodos de cuadros de mando: los diversos componentes de los activos intangibles o capital intelectual son identificados y se generan indicadores que se reportan gráficamente.

En lo referente a la evaluación de la reputación de las organizaciones, se encuentran en la actualidad una variedad significativa de índices de reputación, entre los que se pueden citar el *World's Most Admired Companies* de la revista *Fortune*[8], el *World's most respected companies* de la revista *Barron's*[9], el MERCO[10] (Monitor empresarial de reputación corporativa) o el iRON (Índice de reputación *online*), ampliamente usado en el sector turístico, entre muchos otros.

Cada uno de esos índices se elabora sustentado en diversos atributos y los criterios de evaluación dependen directamente de los elaboradores. Sin embargo, hay autores (26) que no creen que la reputación corporativa pueda ser evaluada en lo empresarial, ya que entienden que no cumplen los requisitos ya definidos para los activos intangibles, como el de ser identificables o estar controlados por la organización.

8 http://money.cnn.com/magazines/fortune/most-admired/.
9 http://online.barrons.com/.
10 http://www.merco.info/.

Infraestructuras críticas

Los servicios esenciales y las infraestructuras críticas

Los actuales Estados disfrutan de una serie de servicios básicos para sus sociedades que se sustentan sobre un conjunto de complejas infraestructuras, en su mayoría operadas y propiedad de empresas privadas. Estas infraestructuras, cuya función puede tener un alcance más o menos localizado, dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general.

La creciente preocupación por el impacto que un ataque contra una o varias de estas infraestructuras podría suponer, incluso a nivel supranacional, ha llevado al desarrollo de un conjunto de normativas tanto nacionales como internacionales que se encargan de establecer los principios para la identificación de las infraestructuras de mayor criticidad y su adecuada protección.

Los antecedentes sobre la protección de infraestructuras críticas (IC) en Europa se remontan al Libro Verde de 17 de noviembre de 2005 sobre un Programa Europeo para la Protección de Infraestructuras Críticas (27), que presentaba las opciones para una respuesta de la Comisión a la solicitud del Consejo de establecer el Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC[11]) y la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN[12]).

El 12 de diciembre de 2006, la Comisión aprueba la comunicación sobre el PEPIC por el que se establecía un marco legislativo para las actividades de protección de las infraestructuras críticas en la Unión Europea (UE) y, posteriormente, la Directiva 2008/114/CE del Consejo (28) establecía un procedimiento de identificación y designación de infraestructuras críticas europeas[13] (ICE), y un planteamiento común para evaluar dichas infraestructuras con el fin de mejorar y, así, proteger las necesidades de la población.

En España, y como trasposición de la citada directiva, la Ley 8/2011, *por la que se establecen medidas para la protección de las infraestructuras críticas,* define 12 sectores estratégicos, definidos como «cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país» (29). Los sectores que establece la Ley 8/2011 son: Administración; espacio; industria nuclear;

[11] En inglés EPCIP, European Programme for Critical Infrastructure Protection.

[12] Critical Infrastructure Warning Information Network.

[13] Son aquellas infraestructuras críticas situadas en algún estado miembro de la Unión Europea cuya perturbación o destrucción afectaría gravemente al menos a dos estados miembro.

industria química; instalaciones de investigación; agua; energía; salud; tecnologías de la información y las comunicaciones (TIC); transporte; alimentación, y sistema financiero y tributario, aunque en algunos casos estos sectores se subdividen en ámbitos o subsectores.

Dentro de cada uno de estos sectores existen infraestructuras, denominadas infraestructuras estratégicas (IE[14]), de cuyo funcionamiento dependen los servicios esenciales, definidos como «el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas». Aquellas IE indispensables para el correcto funcionamiento del servicio esencial son denominadas infraestructuras críticas (IC[15]).

En la Ley 8/2011 se establece el sistema de protección de IC (PIC), compuesto por una serie de instituciones, órganos y empresas procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos, haciendo especial hincapié en la necesidad de considerar la seguridad desde una perspectiva integral. Con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la citada ley, se publica el Real Decreto 704/2011(30), *por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.*

Como ya se ha indicado anteriormente, el sistema PIC queda integrado por los diferentes agentes con responsabilidad en el correcto funcionamiento de los servicios esenciales. Incluye, por tanto, diferentes departamentos ministeriales, en particular el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad y del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC[16]), adscrito a esta, así como Administraciones Públicas (nacionales, regionales o locales), Fuerzas y Cuerpos de Seguridad del Estado, comisiones y grupos de trabajo.

A la lista anterior se añaden los denominados operadores críticos, es decir, todas aquellas empresas y organismos que gestionan al menos una IC. Sobre ellos recae, entre otras, la responsabilidad de definir los oportunos planes de seguridad para proteger adecuadamente los activos de las IC bajo su control.

La gestión del *Catálogo nacional de infraestructuras estratégicas,* conformado por unas 3.700 (31), entre las cuales figuran las identificadas como

[14] Son aquellas instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

[15] Son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

[16] http://www.cnpic.es/.

IC, corresponde a la Secretaría de Estado de Seguridad, quedando su conocimiento restringido al ser calificado como *secreto,* conforme al Real Decreto 704/2011. Sin embargo, el propio Ministerio del Interior estima que el 80% de las IC españolas quedarían en manos de empresas del sector privado (32), frente al 20% restante que serían gestionadas por operadores del sector público.

La necesidad de integrar dentro del sistema PIC a tal cantidad de actores, privados y públicos, hace que resulte fundamental el fomento de la colaboración público-privada, así como una fuerte implicación desde las empresas del sector privado. En este contexto, el CNPIC juega un papel fundamental, ya que los operadores críticos tienen en él su punto directo de interlocución con el Ministerio del Interior en lo relativo a responsabilidades, funciones y obligaciones.

Ciberdependencia de las infraestructuras críticas

Uno de los aspectos clave en la PIC es la estrecha interrelación existente entre IC, lo que puede conducir a que una perturbación en el funcionamiento de una provoque la alteración de otra que inevitablemente requiere del servicio de la primera para funcionar y proporcionar a su vez su servicio esencial. Por tanto, las perturbaciones en los servicios esenciales pueden transmitirse a otros servicios, incluso de diferentes sectores estratégicos, pudiendo generar un efecto cascada.

En este contexto, las IC de la información, dentro del sector TIC, proporcionan servicios esenciales al resto de sectores (33), soportando fundamentalmente las comunicaciones y la operación remota de instalaciones. Por otra parte, las IC de los diferentes sectores hacen a su vez un uso intensivo de las TIC, ya que en gran medida recurren a sistemas de monitorización en tiempo real para el control y supervisión de sus infraestructuras propias.

Desde hace décadas, se vienen aplicando por las empresas las tecnologías TIC para gestionar la automatización de procesos o para controlarlos remotamente en el ámbito industrial, normalmente en entornos completamente aislados y sin conectividad alguna con el exterior. En función de sus características y particularidades, se puede establecer una difusa categorización (34) de los sistemas de monitorización y control en tiempo real, o sistemas de control industrial (ICS[17]), que englobarían a: los sistemas de control de supervisión y adquisición de datos (SCADA[18]); los sistemas de control distribuido (DCS[19]), y los sistemas basados en controladores lógicos programables (PLC[20]).

17 *Industrial Control System.*
18 *Supervisory Control And Data Acquisition.*
19 *Distributed Control System.*
20 *Programmable Logic Controllers.*

Esta presencia de redes y equipamientos TIC utilizados para la gestión y la operación de los procesos industriales es lo que se conoce como *ciberdependencia* de las IC (35), concepto que describe la posibilidad de que una perturbación de los activos cibernéticos que soportan a las IC tenga importantes impactos negativos en el funcionamiento de estas (36), así como en la provisión de los respectivos servicios esenciales que soportan.

La *ciberdependencia* de las IC pone de manifiesto la exposición, para bien o para mal, de estos activos a los efectos del ciberespacio. De hecho, la propia Ley 8/2011 incluye como definición de IC a las redes, los sistemas y los equipos de tecnologías de la información, considerando a estos como activos sobre los que descansa el funcionamiento de los servicios esenciales.

Las TIC de las IC fueron diseñadas en su origen primando los criterios de funcionalidad, pero se han visto sometidas a importantes alteraciones en su concepto de operación, de modo que se han introducido cambios en las tecnologías, arquitecturas y entornos de trabajo que han ido más allá de los requisitos de seguridad para los que habían sido diseñadas originalmente. Seguramente, el cambio más importante ha sido el de interconectar las TIC de las IC con redes abiertas, como Internet, para ganar en interoperabilidad y reducir costes, lo que ha supuesto un gran impacto en su seguridad.

En general, los sistemas de monitorización y control en tiempo real de las IC, generalmente referidos bajo el término SCADA, tienen una estructura (37) que se compone de:

- Centros de control: alojan los componentes centrales desde los que gestionar los procesos, así como el personal encargado de supervisarlos y operarlos, dando las órdenes oportunas que se transmitirán a las posiciones a través de los diferentes mecanismos de comunicación disponibles.
- Posiciones de campo: son los elementos encargados de transmitir las órdenes recibidas del centro de control a los actuadores finales, es decir, los dispositivos que físicamente controlan un proceso (tales como válvulas, sensores, bombas, etc.), así como de recopilar la información de monitorización de los mismos para hacérsela llegar al centro de control.
- Redes de comunicación: normalmente de área extensa (WAN[21]), que permiten la transferencia de información entre los dos anteriores.

Aunque la ubicación física de estos sistemas puede condicionar su arquitectura, sin embargo, la creciente exposición lógica de las IC al ciberespacio es consecuencia fundamentalmente de dos aspectos:

21 *Wide Area Network.*

– De la cada vez mayor conectividad con otras redes empresariales, o externas, con el fin de alimentar a diferentes procesos de negocio y de soporte, redes que a su vez están expuestas, de una u otra forma, a Internet.

– De la tendencia a integrar tecnologías hardware y software comerciales de consumo (ordenadores personales, comunicaciones *Wifi*[22], sistemas operativos no específicos o bases de datos de propósito general) que permiten una mayor flexibilidad y facilidad en el mantenimiento y configuración del sistema, en detrimento de los antiguos productos específicos utilizados.

Esta exposición de redes y sistemas de control industrial, potencialmente consideradas como IC, es patente en todo el mundo y en muchos casos su localización en Internet se convierte en algo trivial mediante herramientas de libre distribución, tal y como alerta el DHS[23] estadounidense (38).

Si bien cabe considerar a los sistemas SCADA directamente relacionados con el control de las IC destinadas a proveer el servicio esencial como el activo más importante por su criticidad, también existe la posibilidad de que haya otros activos de apoyo que se encuentren expuestos al ciberespacio, tales como:

– Sistemas de soporte: que permitan la provisión y funcionamiento adecuado de suministros, dispositivos mecánicos (como escaleras y ascensores), climatización, ventilación, etc., que podrían ser necesarios para la correcta operación de los sistemas e infraestructuras.

– Sistemas de seguridad: con los que se controla la protección de las IC, ya sean dedicados a la detección, alerta, retardo o respuesta frente a incidentes de seguridad, como son los sistemas de videovigilancia, el control de acceso, la detección de intrusión, el sistema antiincendios o las comunicaciones de seguridad.

Amenazas a las empresas desde el ciberespacio

Amenazas a la propiedad intelectual

Los albores del siglo XXI están siendo dominados por los avances de las TIC, que nos proporcionan servicios avanzados como las redes sociales, los teléfonos inteligentes o la computación distribuida. La digitalización de la sociedad en general también ha afectado a las empresas, haciendo

[22] *Wireless Fidelity*, en castellano «fidelidad inalámbrica». Es una marca de la Wi-Fi Alliance, que persigue una idea similar a la de Hi-Fi, *High Fidelity* (término para describir la calidad en la grabación de sonido). Hace referencia a la tecnología de comunicación inalámbrica de calidad entre dispositivos.

[23] *Department of Homeland Security.*

que su información tome un valor preponderante frente a otros activos más tradicionales, convirtiéndose en objetivo muy deseado por colectivos que actúan al margen de la ley.

En esta situación, las organizaciones criminales, así como otros actores relevantes de este contexto (naciones-estado, empresas competidoras, etc.), analizan las tendencias y monitorizan los cambios en la sociedad digital en busca de una oportunidad que les permita comprometer la información sensible de sus objetivos.

La propiedad intelectual de las empresas se encuentra actualmente comprometida debido al creciente número de ataques informáticos (39) que han sufrido grandes compañías como, por ejemplo, Google, RSA o Apple, entre otras muchas.

Como ya se ha mencionado, la propiedad intelectual es uno de los activos más valiosos para las empresas (40), pues es el factor habilitante que permite la actividad innovadora. Las empresas, usando las distintas formas de la propiedad intelectual (patentes, diseños industriales, *copyright,* etc.), se hacen más competitivas al obtener ventajas exclusivas sobre el invento, modelo de utilidad, marca u objeto protegido, consiguiendo un título de propiedad que puede ser objeto de toda clase de negocios jurídicos-mercantiles y pasando a formar parte del capital de bienes inmateriales en una empresa (41). Ese es precisamente el objetivo del espionaje industrial, conseguir por cualquier medio la información estratégica, modelo de utilidad y/o patente en poder de la empresa objeto del ataque.

Según diferentes autores (42), las áreas de mayor impacto que producen los robos de propiedad intelectual sobre el negocio de las empresas serían las siguientes:

- Recursos estratégicos: como, por ejemplo, los planos y diseños industriales de los productos que se desarrollan o los acuerdos y/o contratos con otras empresas.
- Innovación: como son los resultados de las pruebas de un nuevo producto o los estudios sobre las nuevas tendencias en el mercado tecnológico.
- Posicionamiento en los mercados: a través de documentación y manuales de los productos en desarrollo o listas de correos de clientes y usuarios.
- Operacional: como, por ejemplo, los procesos de desarrollo o los procedimientos de distribución y logística.

La figura 4.2 muestra gráficamente un cuadro resumen con varios ejemplos de elementos que constituyen la propiedad intelectual, así como el impacto en la empresa (a nivel estratégico, de innovación, de mercado u operacional) que supone el robo de dichos activos de propiedad intelectual.

		Business Impact			
Example Properties		Strategic	Innovation	Market	Operational
Product Development	Test Results		✓		
	System Designs	✓			✓
	Product Manuals			✓	
	Parts Lists		✓		
	Simulation Technologies		✓		
Manufacturing Procedures	Proprietary Processes		✓		
	Standards				✓
	Supplier Sourcing Arrangements	✓			✓
	Quality Testing Results				
Business Plans	Contract Negotiation	✓		✓	
	Product Pricing	✓		✓	
	Legal Events			✓	
	Mergers / Joint Ventures	✓		✓	
Policy Positions	White Papers		✓	✓	
	Board Minutes	✓			
	Executive Emails	✓	✓	✓	✓
	Recruiting	✓			✓

Figura 4.2: Cuadro de impactos del robo de propiedad intelectual en la empresa. (Fuente: Morgan Franklin Consulting, 2012).

Grupos *hacktivistas*[24], empresas competidoras, organizaciones criminales, agencias de inteligencia o Gobiernos de naciones rivales están detrás de los principales *ciberataques* sufridos recientemente por las empresas, que en el año 2012 ascendieron a alrededor de 30.000 (44). El objetivo principal de estos ataques es la información sensible (propiedad intelectual) en poder de la empresa. Esta será utilizada para realizar transacciones monetarias en el mercado negro o para conseguir una ventaja comercial, económica y/o estratégica sobre un sector, Gobierno o empresa.

Los países occidentales, en especial Estados Unidos y los miembros de la Unión Europea, se enfrentan a un grave desafío para su seguridad y estabilidad económica, debido al incremento progresivo de los *ciberataques* recibidos. Así, por ejemplo, la empresa Mandiant publicó en el pasado mes de febrero un polémico informe (45) en el que se relaciona al Gobierno de la República Popular China con los ataques informáticos recibidos por empresas e instituciones de los países occidentales durante los últimos años. Según este informe, posiblemente *hackers* chinos están detrás de los miles de *ciberataques* que sufren a diario las empresas y organis-

[24] *Hacktivismo* es un término que proviene de la unión de las palabras *hacker* y activismo. Algunos autores (43) lo entienden como «la utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de *software*».

mos occidentales, entre ellos los de EE. UU. Además, el citado informe afirma que dichos *hackers* contaban con el apoyo de una unidad especial del Ejército Popular Chino, que denomina Unidad 61398 o APT1.

Más recientemente, en mayo de 2013, el Pentágono hizo público un informe al Congreso de los Estados Unidos en el que se acusa formalmente a China de llevar a cabo *ciberataques* contra los intereses de los Estados Unidos (46).

Hasta hace pocos años, los *ciberataques* eran atribuidos, en su mayoría, a personas que jugaban a ser *hackers,* los denominados *script kiddies*[25], y no representaban un riesgo serio para las empresas. En esos momentos, la líneas tradicionales de defensa perimetral, basadas en cortafuegos y antivirus, parecían resistir estoicamente dichas amenazas. Sin embargo, hoy en día, las personas que se encuentran detrás de los *ciberataques* ya no son simples aprendices de *hackers*, sino grupos bien organizados con un perfil técnico especialista en seguridad de la información.

Por otro lado, según diversas fuentes (47), la mayoría de los robos de información de propiedad intelectual se producen mediante técnicas de ingeniería social, errores en la utilización de los recursos o técnicas de intrusión avanzada, explotando lo que se conocen como vulnerabilidades de día cero (*zero-day*[26]).

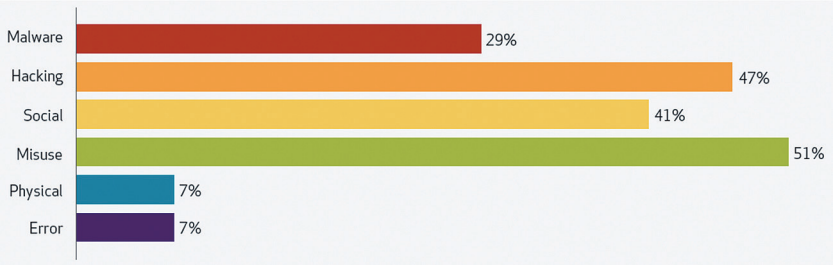


Figura 4.3. Porcentaje de las categorías de amenazas en el robo de propiedad intelectual (fuente: Verizon, 2012).

En el actual contexto del ciberespacio, el NIST[27] norteamericano establece que las nuevas amenazas sobre los sistemas de Información de las empresas son (48):

– La seguridad de las aplicaciones.

[25] Es un término utilizado para describir a personas, normalmente muy jóvenes, que utilizan programas desarrollados por otros para atacar sistemas y redes. Se asume que son personas sin capacidad para programar sus propios *exploits* y que su objetivo es intentar impresionar o ganar reputación entre sus amigos.

[26] Vulnerabilidades que son desconocidas para el fabricante del producto, lo que supone que aún no existen parches o soluciones provisionales que las resuelvan.

[27] National Institute of Standards and Technology.

– La integridad de los sistemas operativos de elementos *hardware* (*firmware*[28]).

– Las amenazas avanzadas y persistentes (APT[29]), es decir, el *software* malicioso o *malware*[30], personalizado y sofisticado, especialmente desarrollado para una organización, empresa o Gobierno.

– La gestión de la privacidad de los datos.

Así, por ejemplo, en el caso de la operación Aurora (49), que apareció publicado en 2010, estaban implicadas varias empresas de nivel internacional, entre las que se pueden citar Google, Adobe o Juniper entre otras, que sufrieron un ataque masivo con el único objetivo de robar información de propiedad intelectual y, además, conseguir información de interés sobre activistas de derechos humanos en China, así como cuentas de usuarios de Google. El origen de este ataque también fue atribuido a China.

El método utilizado para realizar el ataque fue la propagación de un *malware* sofisticado (APT) a través de correos electrónicos. Cada correo electrónico era enviado con un archivo PDF[31], que explotaba una vulnerabilidad no conocida (*zero-day*) del navegador web por defecto, que en la mayoría de los equipos basados en el sistema operativo Windows[32] es el Internet Explorer[33] en sus versiones 6, 7 y 8.

En el caso Aurora, los ataques se llevaron a cabo mediante la combinación de varias técnicas:

– Ingeniería social: basada en explotar la curiosidad innata en los seres humanos. Se enviaron correos electrónicos con el suficiente nivel de conocimiento sobre los destinatarios que consiguieron captar la

[28] Se trata de instrucciones en código máquina para propósitos específicos, almacenados en una memoria normalmente de lectura/escritura (ROM, EEPROM, *flash*...), que establece la lógica de más bajo nivel para controlar un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, pues es el *software* que interactúa directamente con el *hardware*.

[29] Advanced Persisten Threat.

[30] Proviene del inglés *malicious software*.

[31] *Portable Document Format*, lo que puede traducirse como «formato de documento portátil». Se trata de un formato de almacenamiento de documentos digitales independiente de plataformas de *software* o *hardware*, que fue inicialmente desarrollado por la empresa Adobe Systems.

[32] Microsoft Windows es el nombre de una familia de sistemas operativos desarrollados y comercializados por la compañía Microsoft.

[33] Internet Explorer es un navegador web desarrollado en 1995 por Microsoft para el sistema operativo Microsoft Windows. Ha sido el navegador web más utilizado de Internet desde 1999, con un pico máximo de cuota de utilización del 95% entre el 2002 y 2003. Dicha cuota de mercado ha disminuido paulatinamente con los años debido a una renovada competencia por parte de otros navegadores, logrando aproximadamente entre el 30% y 54% en 2012.

atención y ganar la confianza de los mismos, hasta el punto de que los destinatarios consideraron legítimos dichos correos electrónicos.

– Una vez lograda la confianza y establecida la legitimidad de los correos, adjuntaron a los mismos un archivo PDF que contenía un código especial en su interior *(exploit)* para aprovecharse de una vulnerabilidad no conocida *(zero-day)* en una de las aplicaciones de escritorio más utilizada, el Internet Explorer.

El archivo PDF era un simple contenedor del *exploit,* es decir, un medio para transportar el código malicioso hasta su destino. Mediante esta combinación de ataques, los *ciberdelincuentes* consiguieron introducirse en el sistema de dichas corporaciones a principios de 2009 y permanecer ocultos en ellas hasta que se hizo público el informe en 2010.

Durante el tiempo que permanece un código malicioso (*malware*) oculto, este suele llevar a cabo operaciones tales como:

– Obtención de información sobre la infraestructura y sistema donde se encuentra ubicado el *malware*.

– Localización y recuperación de todo tipo de información a la que tenga acceso.

– Comunicación del *malware* con el centro de control (C&C[34]) para enviar la información obtenida y recibir nuevas instrucciones.

Todo ello sin el conocimiento del usuario ni del equipo de seguridad de la corporación. El ataque permaneció oculto en la infraestructura de la corporación hasta que la actividad del *malware* se hizo demasiado patente y los sistemas de seguridad detectaron la intrusión. Sin embargo, se supone que pudo estar oculto en el sistema durante al menos un año, lo que pone de manifiesto el alto grado de exposición de la información y el alto riesgo de sustracción de Información a la que estuvo expuesta la corporación.

Existen muchos otros ataques sofisticados similares a la operación Aurora, como Night Dragon (50), RSA SecureID (51), etc. Todos ellos tienen como denominador común el uso de vulnerabilidades *zero-day* y las técnicas de ingeniería social.

Amenazas a la reputación y marca

Existen varias razones por las que la reputación o imagen corporativa de la empresa pueden verse amenazadas y atacadas, desde la filtración de información comprometedora por un empleo desleal hasta la acusación de actividades ilegales relacionadas o atribuibles a la misma. Pero, si se

[34] *Command and Control.*

limita el ámbito de actuación al ciberespacio, son los *ciberataques* dirigidos contra la imagen y reputación de una empresa sobre los que se debe prestar especial atención.

Determinadas acciones pueden repercutir negativamente en la imagen corporativa o en la reputación de la misma. Este fue el caso del anteriormente referido ataque RSA SecureID (52), que propició una importante brecha de seguridad y un robo de información a la empresa RSA[35] en el 2011 que supuso unos costes directos de 66,3 millones de dólares (53), incluyendo la investigación del ataque, los costes para reconfigurar la infraestructura TIC comprometida, el soporte y la sustitución parcial de los dispositivos a clientes, pero excluyendo el impacto en la reputación y la imagen de RSA.

Por tanto, además de un ataque contra la propiedad intelectual, este incidente supuso un enorme ataque a la reputación e imagen de la propia empresa. Esto se debía a que el principal negocio de la compañía es la seguridad de la información, que se había visto comprometido durante el ataque, lo que dejaba a la empresa en una delicada situación frente a sus clientes. Tanto es así que tras el ataque se vio obligada a sustituir, sin coste algunos para sus usuarios, millones de dispositivos SecureID en todo el mundo (54).

El *ciberataque* se inició con una campaña de *phishing* a un reducido grupo de empleados de la empresa RSA (55), a quienes enviaron correos electrónicos con títulos sugerentes como *2011 recruitment plan*[36]. Todos esos correos electrónicos llevarían adjunto un documento Excel[37], que incluía un código dañino listo para explotar la vulnerabilidad de tipo *zero-day* en Adobe Flash[38] que había sido descubierta recientemente.

En tan solo cinco pasos, los *ciberatacantes* habían conseguido hacerse con el control de algunos equipos dentro de la organización y sustraer informaciones tales como las credenciales de los equipos comprometidos, el nombre de los usuarios, las cuentas de administrador, la información sobre los grupos del dominio, la información sobre la infraestructura, su ubicación, el perfil del usuario víctima, sus direcciones IP, el nombre de servidores, etc.

[35] Originalmente, RSA dio nombre a un sistema criptográfico de clave pública desarrollado en 1977. Tomaba el nombre de las iniciales de sus creadores: Rivest, Shamir y Adleman. Desde el 14 de septiembre de 2006, RSA constituye la División de Seguridad de la empresa EMC Corporation, y organiza anualmente el famoso evento de *ciberseguridad* RSA Conference. De sus productos, destacan las bibliotecas criptográficas B-SAFE, los mecanismos de autenticación SecureID y el propio algoritmo criptográfico RSA.

[36] Plan de contrataciones para el 2011.

[37] Microsoft Excel es una aplicación para hojas de cálculo comercializada por Microsoft dentro de su familia de productos Office.

[38] Adobe Flash Player es una aplicación en forma de reproductor multimedia creado inicialmente por Macromedia y actualmente comercializado por la compañía Adobe Systems que permite reproducir archivos multimedia. Si estos archivos se reproducen en un navegador, su formato es el de un *plug-in*.

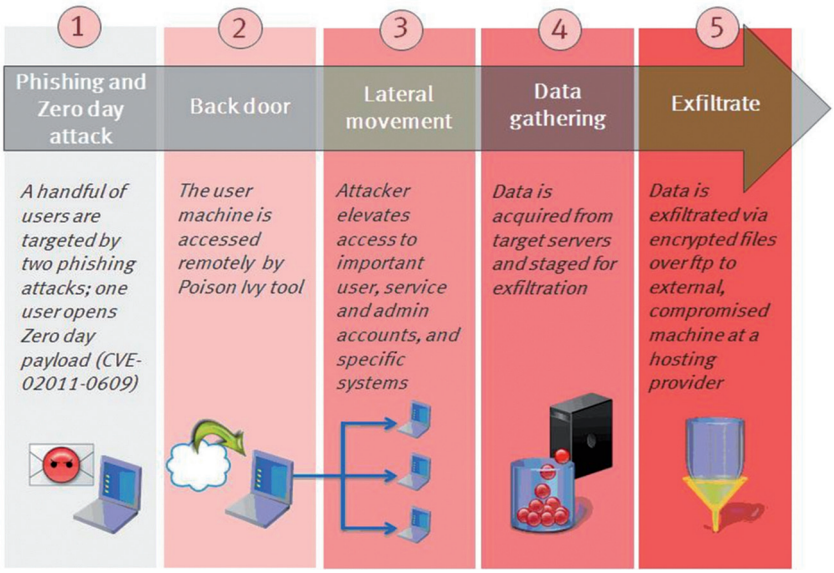


Figura 4.4. Fases del ataque sufrido por RSA (fuente: RSA, 2011).

Además, los atacantes instalaron una puerta trasera en el equipo, quedando este completamente comprometido y bajo el control del atacante.

Tal y como se ha venido comentando en los apartados anteriores, la principal vía de ataque (vector de ataque[39]) es la combinación de una vulnerabilidad, preferentemente desconocida, unido a una campaña de ingeniería social sobre los usuarios potencialmente objetivos. Una vez infiltrados, el APT se comunicará con el centro mando y de control para recibir instrucciones y enviar toda la información posible antes de ser detectado por los sistemas de seguridad.

Para dañar la imagen o reputación de una empresa, además de a través del robo de información sensible o de propiedad intelectual, se puede conseguir el mismo efecto mediante los siguientes tipos de ataques:

- Ataque de denegación de servicio (DoS[40]).
- Modificación o manipulación del comportamiento normal de una página web (*defacement*[41]).

[39] Un vector de ataque es la vía que se utiliza para obtener información o acceso no autorizado a un determinado sistema.

[40] *Denial of Service*. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente, provoca la pérdida de la conectividad por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

[41] Palabra inglesa que significa «desfiguración». Es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página *web* por un atacante.

– Filtración de información sensible y/o comprometedora de la empresa.
– Robo de información como consecuencia de una intrusión en los sistemas TIC corporativos.

Por supuesto, el efecto sobre la imagen y la reputación de la empresa vendrá determinado por la actividad de esta, así como el alcance que tenga el incidente de seguridad dentro de la misma. Si en el caso RSA, el incidente de seguridad en sus sistemas ponía en tela de juicio su fiabilidad (reputación) como empresa de seguridad, en el incidente que afectó a la empresa Sony (56), la filtración de millones de cuentas de usuarios, incluidas tarjetas de crédito, en su plataforma de juegos *online* PlayStation Network (PSN) supondría un duro golpe a su reputación e imagen corporativa, así como el coste derivado de contener y reparar el daño causado por el *ciberataque*. Si en el ataque RSA consiguieron infiltrarse en los sistemas con un ataque de ingeniería social, en el caso de Sony el procedimiento fue más lento y elaborado.

El ataque comenzó en enero de 2011, cuando un conocido *hacker* asociado al mundo de la PlayStation consiguió acceder a las claves de cifrado que utiliza el sistema PS3[42] para protegerse y evitar la ejecución de juegos no autorizados en su plataforma.

Tras la publicación (57) del proceso para realizar el desbloqueo del sistema de seguridad de Sony en la consola de juegos PS3, la compañía inicia una serie de acciones legales contra el *hacker* en cuestión. Estas acciones obtienen como respuesta un *ciberataque* a gran escala, fechado el 3 de abril de 2011, contra varias páginas web de Sony realizado por el grupo de *hacktivistas* Anonymous (58). Este boicot contra Sony por parte de Anonymous duró al menos diez días, pero no fue hasta el 19 de abril de 2011 cuando se detecta una actividad no autorizada en los servidores de la plataforma de juegos *online* (PSN), obligando a Sony a apagar sus servidores de juego *online* lo que provoca la indignación de los millones (más de 70) de usuarios en todo el mundo.

Hasta el 30 de abril de ese mismo año, Sony (59) no decide hacer un comunicado oficial informando de lo sucedido. A continuación, se lanza una actualización del *firmware* y se reanuda el funcionamiento habitual del servicio, después de un mes de la confirmación del incidente de seguridad en sus sistemas (60).

En esta ocasión, los atacantes aprovecharon el ruido generado por la publicación de las claves de cifrado y el *ciberataque* del grupo Anonymous para llevar a cabo su intrusión al sistema. No hay un comunicado oficial de Sony donde se comente la técnica utilizada por los atacantes, pero existen informes de empresas de seguridad (61) que exponen una serie

[42] PlayStation 3.

de teorías sobre el método y técnicas de ataque utilizadas para vulnerar la seguridad de la plataforma PlayStation Network.

Según dichas investigaciones, es posible que una vulnerabilidad del tipo «SQL injection»[43] en una de las aplicaciones de PlayStation Network o en una base de datos públicamente accesible fuese la causa principal de la intrusión. No obstante, al no existir ninguna confirmación oficial sobre el incidente, solo se puede especular sobre el ataque.

Las consecuencias del ataque informático no solo afectaron a la reputación e imagen de Sony, sino que causaron unas pérdidas de unos 130 millones de euros según fuentes de la propia compañía (62). Esto incluyó la necesidad de establecer una estrategia de compensación a los usuarios que consistía en obsequiarlos con un juego gratuito, variando este según la zona o región de pertenencia de los mismos.

Sin embargo, los casos más sencillos de ataques a la reputación y a la imagen corporativa de una empresa son los ataques de denegación de servicio (DoS) o cambiar el aspecto del servicio *Web* (*defacement*), en particular para empresas que ofrecen un servicio *online*.

Uno de los casos más recientes es el que se ha producido durante la disputa mantenida por dos empresas a través de Internet, que como efecto secundario ha provocado una ralentización de la velocidad de navegación *web* en todo el mundo; incluso algunos expertos han llegado a catalogar el incidente como el mayor ataque de denegación de servicio distribuido (DDoS[44]) nunca antes visto (63).

Esto sucedió cuando la empresa holandesa Cyberbunker[45] lazó un ataque masivo de *spam*[46] y denegación de servicio contra Spamhaus[47], firma suiza que se dedica a la seguridad informática, en particular a sistema *antispam*. La empresa Cyberbunker es conocida por su largo historial de ataques de denegación de servicio (DDoS) y sus laxas políticas de alojamiento *web*, que permiten prácticamente todo tipo de contenido salvo pornografía infantil y terrorismo. Fruto de dicha política, Spamhaus

[43] Inyección SQL. Es un método de introducción de código malicioso que se vale de una vulnerabilidad informática presente en el nivel de validación de las entradas para realizar consultas a una base de datos. El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL.

[44] *Distributed Denial of Service*. Es una ampliación del ataque DoS que se lleva a cabo generando un gran flujo de información desde varios puntos de la red. La forma más común de realizar un DDoS es a través de una *botnet.*

[45] http://www.cyberbunker.com/.

[46] O correo basura, constituido por los mensajes no solicitados, no deseados o de remitentes no conocidos, habitualmente de tipo publicitario. Generalmente es enviado en grandes cantidades, lo que perjudica seriamente al receptor.

[47] http://www.spamhaus.org/.

incluyó a Cyberbunker en su lista negra de envío de correo no deseado (*spam*). Como represalia, el pasado mes de marzo de 2013 la empresa Cyberbunker decidió llevar a cabo un ataque de DDoS contra Spamhaus que no solo provocó la caída del servicio de la empresa, sino que además provocó efectos secundarios en todo Internet.

Según diversos autores (64), estos efectos se deben, en gran parte, a la técnica empleada por la empresa Cyberbunker para ejecutar el ataque. Este consiste en explotar una vulnerabilidad de los servidores DNS[48], lo que genera múltiples paquetes de respuesta a peticiones falsas desde dichos servidores DNS hacia el sitio web atacado, en este caso el de Spamhaus. Este ataque es conocido como *DNS amplification attacks* (65).

Uno de los efectos secundarios del ataque sobre Spamhaus fue la caída del servicio Netflix[49] en diversas zonas del mundo, sobre todo en Alemania, pues los usuarios no lograron establecer conexión con los servidores de *streaming*[50] mientras duró el ataque, lo que supuso importantes pérdidas económicas para la empresa proveedora del servicio.

Independientemente de quién esté detrás de los ataques contra la reputación y la imagen corporativa (empresas competidoras, *hacktivistas* empleados descontentos, agencias de inteligencia o el crimen organizado), no cabe duda de que estos constituyen una seria amenaza para la seguridad de la empresa, con un coste económico considerable, y que puede provocar una crisis de confianza que, en determinadas ocasiones, puede llegar a ser insalvable.

Este es el caso de la empresa de seguridad DigiNotar (66) tras sufrir un grave incidente de seguridad en el que se robaron varios centenares de certificados digitales utilizados para autenticar conexiones seguras SSL[51] en multitud de aplicaciones, entre ellas las ventas por Internet. Fue declarada en bancarrota en septiembre de 2011, poco después de que el Gobierno holandés hubiese tomado el control sobre las operaciones de los sistemas informáticos de la compañía tras confirmar la brecha en sus sistemas de seguridad.

[48] *Domain Name System*, en español «sistema de nombres de dominio». Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet. Su función más importante es traducir nombres de dominio inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar estos equipos en todo el mundo.

[49] Plataforma de vídeo que ofrece la distribución de contenido multimedia, como películas y series de televisión, a cambio de una cuota de suscripción mensual.

[50] Servicio de distribución de contenidos multimedia a través de una red de ordenadores de manera que el usuario consume el contenido al mismo tiempo que se va descargando.

[51] *Secure Sockets Layer*. Es un protocolo criptográfico que permite comunicaciones seguras por una red TCP/IP, comúnmente Internet.

Amenazas a las infraestructuras críticas

En el ciberespacio, la separación entre lo físico y lo lógico está cada vez más difuminada. Un ataque «virtual» podría tener repercusiones serias en el mundo físico. En este contexto, las infraestructuras críticas (IC) se han convertido en objetivos de especial interés para los países adversarios, así como para organizaciones terroristas que buscan conseguir sus objetivos mediante la fuerza y el terror.

En el caso de las IC, el objetivo de los *ciberataques* son los actos de sabotaje contra dichas infraestructuras (67). Estos precisan contar, además de con importantes recursos materiales, con personal que disponga de la cualificación técnica adecuada, hasta tal punto de que la mayoría de los expertos consideran que esto solo puede alcanzarse por parte de actores muy organizados y con recursos suficientes, como son los propios Estados.

Una de las primeras ocasiones en las que se realizó un sabotaje masivo de las infraestructuras de toda una nación a través de *ciberataques* tuvo lugar en 2007, durante la crisis entre Estonia y Rusia motivada por el traslado de símbolos soviéticos en la ciudad de Tallin. Los ataques informáticos contra empresas e instituciones de Estonia llegaron a tal punto que se vieron obligados a desconectar temporalmente el país de Internet e, incluso, a solicitar ayuda a la OTAN, al considerar los *ciberataques* como una acción terrorista a gran escala por el daño y las consecuencias que ocasionaron (68).

Pero no fue hasta el año 2010, con la aparición del *malware* denominado Stuxnet, cuando se hizo patente la posibilidad de afectar a las infraestructuras del mundo físico por medio de un código malicioso, proveniente por tanto del mundo virtual pero capaz de provocar, de forma indeseada, una respuesta física real.

Como ya hemos visto, tradicionalmente siempre se ha considerado que los sistemas ICS que controlan las infraestructuras estratégicas se encuentran en redes aisladas, por lo que estas no podrían ser atacadas a través de redes públicas como Internet. Pero nada más lejos de la realidad: en 2010 apareció la primera referencia al mencionado Stuxnet, cuya sofisticación no había sido vista anteriormente y que posteriormente fue catalogado como la primera arma cibernética (69).

Este *malware* fue descubierto por casualidad durante un rutinario procedimiento de actualización de algunos de los componentes de un sistema de control de las centrifugadoras de enriquecimiento de uranio de una central nuclear. El procedimiento presentó diversos errores y el ingeniero decidió llevarse parte del trabajo a casa. Una vez allí, conectó su ordenador con Internet y comprobó que este estaba infectado con un virus y que utilizó dicha conexión para propagarse más allá de la zona de

actuación para la que había sido programado inicialmente. Esto acabaría siendo detectado posteriormente por diferentes laboratorios de seguridad y equipos de investigación (70).

Como ya se ha mencionado anteriormente, los sistemas ICS se componen principalmente de elementos o sistemas tales como (71):

- Sistemas SCADA, que permiten controlar los procesos industriales a distancia mediante el despliegue de sensores y actuadores en el sistema industrial.
- Sistemas DCS, para la localización de productos y elementos durante el proceso industrial.
- Controladores PLC, utilizados en los procesos industriales para automatizar tareas con controles electromecánicos.

Con la información que gestionan y administran los sistemas de control, se puede percibir la importancia y criticidad que algunos de estos sistemas puede suponer, en particular, si estuvieran presentes en infraestructuras catalogadas como críticas.

Según diversas fuentes (72), Stuxnet fue programado para atacar los sistemas de control utilizados en plantas nucleares de enriquecimiento de uranio en Irán, y el desarrollo de este *malware* se atribuye a EE. UU.

Lo más identificativo de este virus es que explotaba hasta cuatro vulnerabilidades *zero-day* diferentes. Como sabemos, para este tipo de vulnerabilidades no existen contramedidas; ni temporales, mediante inhibición por alguna técnica como podría ser la detección por un antivirus que evitara que actuase, ni definitivas, por medio de un parche que corrigiera la vulnerabilidad del sistema y así dejara de ser explotable de forma permanente. El que el *malware* usara hasta cuatro de estas vulnerabilidades da idea de la virulencia con la que era capaz de penetrar los sistemas objetivo, pero, sobre todo, de la capacidad técnica y económica del equipo que lo desarrolló.

Utilizando la ventaja que supone disponer de vulnerabilidades *zero-day,* el *malware* permanecía oculto en el sistema anfitrión esperando la oportunidad de propagarse, principalmente a través de los dispositivos USB[52]. Al ser un *software* malicioso diseñado para redes que se encuentran aisladas (sin conexión a Internet), este tenía la capacidad de ser autónomo, limitando al mínimo la necesidad de comunicarse con sus centros de mando y control.

Según diversos estudios (73), existe una tendencia a descuidar la seguridad del *firmware* incrustado en los elementos *hardware*. Esto, unido a

[52] *Universal Serial Bus*. Es un estándar que define los protocolos usados en un bus de datos para conectar, comunicar y proveer de alimentación eléctrica a periféricos desde un ordenador.

la popularidad e importancia que ha adquirido este tipo de *software*, lo convierte en una amenaza a tener muy en cuenta. En general, el *firmware* está diseñado para llevar a cabo una función de control específica, dentro de un sistema mayor y más complejo. Por ello, cada vez con más frecuencia, los desarrolladores de código dañino crean agentes *software* que atacan a estos componentes al ser mucho más simples que los sistemas operativos.

En concreto, Stuxnet estaba programado para atacar un PLC específico de la compañía Siemens[53] encargado de hacer funcionar a la frecuencia adecuada los motores para bombas y centrifugadoras utilizadas en instalaciones industriales. La infección del PLC se realizaría tras comprometer el sistema operativo del ordenador que ejecutaba el *software* de gestión del PLC, que en este caso se trataba de un sistema Windows.

Para alcanzar los sistemas de control industrial, no basta con crear código dañino especializado en el *hardware* y su *firmware*, sino que deben utilizar a los usuarios, en especial a los administradores de sistemas, para llegar a sus objetivos. Para ello se diseñan ataques muy elaborados, utilizando código malicioso muy sofisticado –las ya referidas APT– que, a diferencia de los virus clásicos, tienen objetivos específicos y bien determinados y son incluso capaces de propagarse desde un sistema conectado a Internet a un sistema aislado. Para lograr esto, los atacantes utilizan todos los recursos a su alcance, como por ejemplo:

- Ingeniería social (*phishing, mailing*, etc.).
- Vulnerabilidades a través de las páginas *web* corporativas.
- Gusanos, troyanos, virus, etc.

Con el denominador común de que estos ataques van acompañados de la existencia de vulnerabilidades de día cero. Según informes especializados (74), existe un mercado negro donde se ponen a la venta vulnerabilidades *zero-day* por valor que puede oscilar entre los 80.000 € y los 500.000 €, según la sofisticación de la misma, lo que da una idea de los beneficios que puede reportar este tipo de actividades.

Sin embargo, en la actual sociedad de la información, es la unión de la ingeniería social y estas vulnerabilidades de día cero lo que se está convirtiendo en el vector de ataque más utilizado. Las redes sociales y la creciente falta de control en la privacidad de los datos personales están permitiendo a los *ciberatacantes* recopilar enormes cantidades de información sobre sus potenciales víctimas y, así, poder desarrollar campañas de ingeniería social con mensajes muy personalizados.

[53] http://www.siemens.com/.

Principales vulnerabilidades para las empresas de las tecnologías del ciberespacio

«Cloud computing»

Tal y como referencian diferentes autores, existen numerosas definiciones del término *cloud computing*, o «computación en la nube» en castellano, pero una que podría agrupar la mayoría de los aspectos recogidos en todas ellas sería la siguiente (75):

> *Las nubes son un gran conjunto de recursos virtualizados, fácilmente utilizables y accesibles (como «hardware», plataformas de desarrollo y/o servicios). Estos recursos pueden ser reconfigurados dinámicamente para adaptarse a una carga variable, capacitándolos también para una utilización óptima de los recursos. Este conjunto de recursos suele ser explotado por un modelo de pago por uso, en el que las garantías son ofrecidas por el proveedor de infraestructura a través de acuerdos del nivel de servicio (SLA[54]) personalizados y acordados.*

Otros autores (76) prefieren destacar otros aspectos en sus definiciones, como por ejemplo la que indica que la computación en la nube

> *...es una tendencia reciente de los sistemas TI[55] que desplaza el proceso y los datos desde los PC de escritorio y portátiles hacia grandes centros de proceso. El término hace referencia tanto a las aplicaciones, suministradas como un servicio a través de Internet, como a la infraestructura real, es decir, las computadoras y los sistemas «software» de los grandes centros de proceso que proporcionan dichos servicios.*

Finalmente, el NIST[56] norteamericano define la computación en la nube como (77):

> *...un modelo para facilitar el acceso a red, ubicuo, conveniente y bajo demanda, a un conjunto de recursos de computación configurables (v. g. redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden provisionar y liberar rápidamente, con un mínimo esfuerzo de gestión o interacción del proveedor del servicio.*

En resumen, desde un punto de vista empresarial, el *cloud computing*, o simplemente *cloud* o nube para abreviar, es básicamente un nuevo modelo de negocio que se basa en ofrecer un servicio que permite la gestión y explotación de información digital, que se encuentra almacenada en servidores remotos, accediendo a ella a través de redes de telecomunicaciones públicas o privadas.

---

54 *Service Level Agreements.*

55 Tecnologías de la Información.

56 *National Institute of Standards and Technology.* http://www.nist.gov/.

Si bien es cierto que las tecnologías de base que soportan este nuevo servicio existen hace muchos años, el aumento de la capacidad de cómputo y almacenamiento de los ordenadores, las mejoras en los anchos de banda de las redes de telecomunicaciones y el crecimiento exponencial del número de usuarios particulares y empresas conectados a Internet han propiciado el auge de este nuevo modelo de negocio.

El funcionamiento de la nube, independientemente de su tipo y del uso que se le vaya a dar, se sustenta en cinco pilares fundamentales:

- Autoservicio bajo demanda. El usuario puede, unilateralmente y en cualquier momento, modificar las capacidades de computación que está utilizando, tales como el tiempo del servidor o el espacio de almacenamiento, de manera automática y sin necesidad de requerir la interacción humana con su proveedor del servicio en cuestión.
- Acceso completo a la red. Todas las prestaciones del servicio están disponibles a través de la red, a las que se puede acceder mediante los dispositivos más comúnmente utilizados (p. ej. *smartphones*, tabletas, portátiles, estaciones de trabajo, etc.).
- Agrupación de recursos. Los recursos del proveedor del servicio están agrupados para servir a múltiples usuarios, con diferentes recursos físicos y virtuales, asignados y reasignados dinámicamente en función de la demanda de los usuarios. Existe una cierta sensación de independencia de la ubicación que siente el usuario debido al escaso control y conocimiento que tiene este sobre la ubicación exacta de los recursos utilizados. No obstante, en función del proveedor de servicios y el SLA del que se disponga, el usuario puede ser capaz de especificar la ubicación de dichos recursos con cierto nivel de abstracción (por ejemplo, país, comunidad o centro de datos).
- Rápida elasticidad. Los recursos pueden ser reservados y/o liberados elásticamente, en algunos casos automáticamente, para escalar rápidamente un sistema o aplicación acorde a la demanda, dando a veces la sensación al usuario de que dispone de recursos ilimitados.
- Servicio a medida. La infraestructura de la nube controla y optimiza automáticamente el uso de los recursos mediante la medición continua de dicho uso, acorde al tipo de servicio que se esté prestando (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuarios activas). El uso de los recursos puede ser monitorizado y controlado de forma transparente tanto para el usuario como para el proveedor del servicio.

En función del modelo de implantación, es decir, de quién presta el servicio y quién es el usuario del mismo, existen diferentes tipos de nubes (78): la «nube privada», la «nube comunitaria», la «nube pública» y la «nube híbrida».

En la *nube privada,* la infraestructura es proporcionada para su uso exclusivo por parte de una organización. Esta infraestructura puede pertenecer y ser gestionada o mantenida por una misma organización, por una empresa externa o por una combinación de ambas.

Dentro de la misma línea, se encuentra la *nube comunitaria,* cuya infraestructura es proporcionada para su uso exclusivo por parte de un grupo de organizaciones que forman una comunidad con principios e intereses similares, esto es, misión, requisitos de seguridad, políticas y cumplimientos normativos, etc. La infraestructura puede pertenecer, ser gestionada y mantenida por una o varias de las organizaciones dentro de dicha comunidad, por una empresa externa o por una combinación de estas. Se podría considerar una variante de la nube privada.

Por su parte, en la *nube pública,* la infraestructura es proporcionada para su uso por parte del público en general. Esta puede pertenecer, ser gestionada y mantenida por una empresa, escuelas, universidades, organismos públicos o alguna combinación de los anteriores.

Finalmente, existiría un cuarto tipo de nube, denominado *nube híbrida,* en la que pueden coexistir los modelos anteriores con distintos niveles de relación.

Según el NIST, existen tres modelos de servicios para la explotación de la nube:

- Infraestructura como servicio (IaaS[57]).
- Plataforma como servicio (PaaS[58]).
- *Software* como servicio (SaaS[59]).

La figura 4.5 muestra gráficamente los tres modelos de servicios *cloud,* así como el nivel de visibilidad o de abstracción que tienen los usuarios de dichos servicios (79).

En el modelo IaaS, se proporciona al usuario, bajo demanda, una infraestructura completa para el procesamiento de información donde este puede instalar y ejecutar las aplicaciones que considere pertinentes. El usuario no administra la infraestructura, pero sí tiene control sobre los sistemas operativos usados, el almacenamiento en disco y las aplicaciones instaladas. Del mismo modo, el usuario es el responsable de realizar las instalaciones y mantenimiento del *software* instalado, así como de proporcionar las correspondientes licencias que sean necesarias. Los proveedores de este modelo de servicio suelen ofrecerlo mediante la utilización de máquinas virtuales que permiten una rápida configuración

[57] *Infraestructure as a Service.*
[58] *Platform as a Service.*
[59] *Software as a Service.*

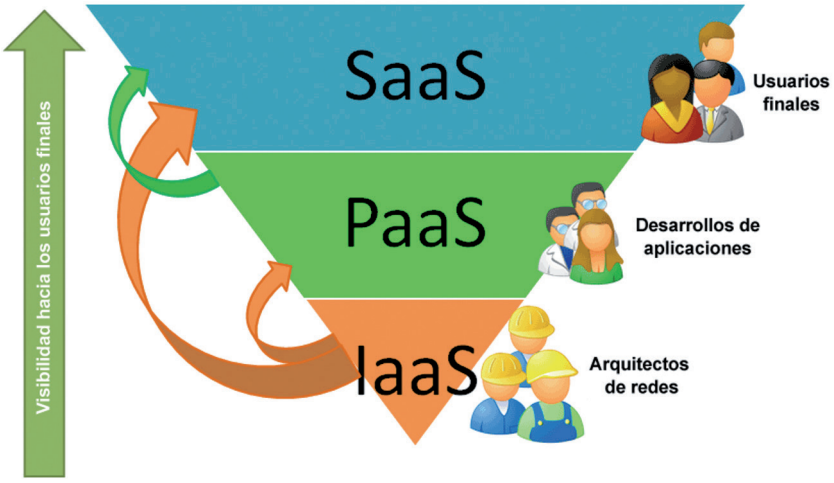


Figura 4.5. Modelos de servicio en la nube (fuente: Schuller, 2008).

por parte del usuario de elementos como el espacio en disco disponible o el número de procesadores, donde este solo paga en función de los recursos utilizados. Este modelo a veces es también denominado *hardware* como servicio (HaaS[60]) (80).

Por otra parte, en el modelo PaaS se proporciona al usuario una plataforma completa, plenamente funcional (*hardware* y *software*), en la que puede instalar y ejecutar sus propias aplicaciones; sin necesidad de tener que administrar el sistema. Un ejemplo son los típicos servidores *web* donde un usuario puede «subir» su propia aplicación y tan solo tiene que preocuparse de la administración y configuración de dicha aplicación particular.

Por último, en el modelo SaaS se proporciona al usuario el propio *software* como un servicio. En este caso, el usuario accede al *software* normalmente desde un navegador *web* (aunque no siempre tiene porque ser así), garantizando que accede a la última versión disponible de dicho *software* y sin necesidad de tenerlo instalado en su propio dispositivo (ordenador, *smartphone* o tableta). Un ejemplo de estos servicios son las versiones *online* de las *suites* ofimáticas (por ejemplo, Office 365) o los servicios de correo electrónico vía *web* (por ejemplo, Gmail).

Principales vulnerabilidades de la computación en la nube

Debido a la propia naturaleza de la nube, y a pesar de sus interesantes ventajas, estas conllevan como contrapartida un importante número de vulnerabilidades.

60 *Hardware as a Service.*

La Cloud Security Alliance[61] describe las que a su entender son las principales vulnerabilidades de la computación en la nube (81), entre las que se pueden destacar:

- Sencillez de acceso y anonimato de la nube. Los proveedores de IaaS y PaaS ofrecen a sus clientes la ilusión de disponer de unas capacidades de cómputo, de red y de almacenamiento ilimitadas, a menudo combinada con un simple proceso de registro, donde cualquiera con una tarjeta de crédito válida puede registrarse y empezar a usar inmediatamente los servicios de la nube. Mediante el abuso del relativo anonimato de este proceso de registro y el modelo de uso, los *ciberdelincuentes* son capaces de llevar a cabo sus actividades con relativa impunidad.
- Interfaces y API[62] poco seguras. Los proveedores de servicios en la nube suelen ofrecer una serie de interfaces y API que permiten a los usuarios controlar los recursos asignados. Así, toda la gestión, monitorización y provisión de los recursos se realiza a través de estas interfaces. Puesto que todas las operaciones (incluidas la autenticación y el cifrado de datos) se realizan con estos mecanismos, es necesario que dichas interfaces estén diseñadas y desarrolladas de forma segura para evitar cualquier posible incidente de seguridad, intencionado o accidental, lo que no siempre se garantiza.
- Tecnologías compartidas. En ocasiones, los componentes físicos utilizados por los proveedores de IaaS (memorias caché, CPU[63], etc.) no fueron diseñados para ser usadas en como partes de una arquitectura compartida entre múltiples usuarios, lo que puede facilitar que determinado *malware* acceda y se propague por estos recursos compartidos.
- Perfil de riesgo desconocido. Una de las grandes ventajas de la nube es la reducción del *software* y *hardware* que una empresa tiene que adquirir y mantener, permitiendo que destine más recursos en su negocio y se centre exclusivamente en él. Sin embargo, esta facilidad puede provocar el deterioro de la seguridad exigida y necesaria en la infraestructura utilizada por falta del conocimiento de la misma.

Además de las vulnerabilidades descritas anteriormente, existen otras asociadas a la propia naturaleza de la nube, entre las que se pueden citar:

[61] Asociación internacional sin ánimo de lucro, cuyo objetivo es promover las mejores prácticas de seguridad en la nube. https://cloudsecurityalliance.org/.

[62] *Application Programming Interface*, o «interfaz de programación de aplicaciones en español». Es el conjunto de funciones y procedimientos que ofrece cierta biblioteca *software* para ser utilizado por otro *software* como capa de abstracción.

[63] *Central Processing Unit*, o «unidad central de procesamiento» en español. Es el componente principal del ordenador y otros dispositivos programables, ya que interpreta las instrucciones contenidas en los programas y procesa los datos.

- Dependencia de la conectividad a la red. Si no existe conexión a la red, no hay acceso a la nube. Esta cuestión, que parece muy simple, hay que tenerla en consideración a la hora migrar determinados servicios a la nube, tanto como usuarios de dichos servicios como siendo los proveedores de los mismos. Este hecho tiene una especial importancia si se pretende utilizar la nube en operaciones consideradas como críticas (por ejemplo, centros de emergencias).
- Deslocalización. Si bien una de las características fundamentales de la nube es la independencia de la localización de los recursos, esto puede suponer un riesgo. Al desconocer el lugar físico real donde se almacena la información, se pierde el control de la misma. Incluso se puede perder el control sobre el número de copias existentes de una información determinada, debido a la replicación de datos que pueden realizar los proveedores de servicios, ya sea para mejorar el acceso a la misma o en labores de mantenimiento de sus sistemas. Por este motivo, hay que tener especial cuidado con qué servicios se utilizan y que información almacenamos y gestionamos con ellos, especialmente si se trata de información sometida al cumplimiento de legislaciones nacionales (de seguridad del Estado, privacidad, etc.) que no puede salir del país sin un consentimiento expreso. Es decir, hay que evaluar las posibilidades reales de trazabilidad de la información.
- Acceso global. Si bien es cierto que el acceso global a la nube facilita el acceso a la información a sus legítimos usuarios de una forma como no se había conocido nunca, también lo es que, por este mismo hecho, se amplía el número de potenciales atacantes o usuarios no autorizados que quieren acceder a dicha información. Puesto que el acceso es global, pudiendo acceder desde cualquier parte del mundo, se dificulta tanto la posible localización de dichos individuos como su posterior denuncia y enjuiciamiento si fuese necesario.
- Dependencia de terceras partes. Al externalizar todo o parte de los servicios que usa una empresa u organización, se añade una dependencia hacia una tercera parte. Esta dependencia es tal que si esta tercera parte proveedora de los servicios falla o incumple los términos del SLA, puede poner en grave riesgo la continuidad del negocio y la operativa de dicha entidad, de forma temporal o incluso permanente. Del mismo modo, al externalizar estos servicios, se le transfieren ciertas competencias a estas terceras partes como, por ejemplo, el almacenamiento de información de la entidad. Por todo ello, hay que garantizar, además de la operativa del servicio, la salvaguarda de la integridad y la confidencialidad de la información que pase a través de estas terceras partes mediante los apropiados acuerdos de confidencialidad.
- Propiedad de la información. En el caso de utilizar nubes públicas o híbridas, es necesario prestar mucha atención a las condiciones

del servicio prestado. En muchos de estos proveedores, se especifica abiertamente que el usuario cede los derechos de uso de la información «subida» por él a la nube, pudiéndola usar el proveedor del servicio para los fines que él considere oportunos. Este hecho se da especialmente en algunos servicios de almacenamiento en la nube que ofrecen un mínimo de capacidad gratuito.

– Privacidad de la información. Al igual que en el caso anterior, también hay que prestar especial atención en las condiciones del servicio prestado en lo referente a la privacidad y acceso a la información almacenada en la nube. En algunos de estos servicios, se especifica que se va a acceder a la información allí almacenada tanto para fines meramente estadísticos como para fines comerciales. Un ejemplo de esto son algunos servicios de correo electrónico gratuito en la nube que leen de forma automática el contenido de los correos para ofrecer al usuario publicidad en base al contenido de sus correos. Esto es especialmente importante cuando algunos de estos proveedores ya empiezan a ofrecer su servicio de correo en la nube a empresas.

– Error humano. El eslabón más débil de la seguridad en cualquier sistema es siempre el factor humano y la nube puede potenciar los efectos que dicha debilidad puede ocasionar. Hay que evitar que los usuarios dejen sus respectivos accesos a los servicios en la nube sin una contraseña mínimamente segura, que faciliten sus credenciales de acceso a terceras personas, que dejen sus sesiones abiertas, etc. Del mismo modo, aunque se pueda acceder a la información de manera global, no todas las ubicaciones son las más apropiadas para acceder a según qué tipo de información. Para ello, nada mejor que una adecuada concienciación del personal implicado, así como un apropiado seguimiento y monitorización periódica del cumplimiento estricto de las políticas de seguridad estipuladas.

– Suplantación de identidad. En relación con el punto anterior, hay que tener mucho cuidado con los robos y suplantaciones de identidad. Puesto que en la nube se accede a los servicios de forma remota, basta con conseguir las credenciales de acceso (certificado, usuario y clave de acceso, etc.) de un usuario legítimo para acceder a la nube como si se tratase de él mismo. A efectos del sistema y del resto de usuarios, no habrá ninguna constancia ni evidencia de que se trata de otro usuario que ha suplantado su identidad.

– Dispositivos móviles. El auge de los dispositivos móviles, sumado a la mejora en el acceso a la redes a través de los mismos (*WiFi*, 3G, etc.), hace posible que un usuario pueda estar permanente conectado a los distintos servicios en la nube. Dadas las características propias de estos dispositivos, así como las de las aplicaciones de acceso a dichos servicios en la nube, no es necesario introducir las credenciales

de acceso a los mismos cada vez que se quieran utilizar. Es decir, virtualmente se puede tener siempre una sesión abierta con uno o más servicios en la nube concretos, con lo que bastaría con tener acceso físico al dispositivo móvil durante tan solo unos instantes para poder acceder a información confidencial, modificar contraseñas de acceso, suplantar la identidad del propietario del dispositivo móvil, etc.

«Big data»

De forma intuitiva, se puede decir que el término *big data* hace referencia los grandes conjuntos de datos y las tecnologías necesarias para su análisis y explotación.

Algunos autores (82) definen *big data* como «un término técnico y de *marketing* que hace referencia a un activo valioso de la empresa, es decir, la información», y sobre su objetivo principal dicen: «analizar grandes conjuntos de datos es respaldar a las empresas en la toma de mejores decisiones de negocio».

Al igual que la nube, el *big data* representa una nueva tendencia tecnológica enfocada a cambiar el modo en el que se toman las decisiones en el mundo de los negocios y las empresas. De esta forma, las decisiones se tomarán en base a la información que se haya extraído de grandes volúmenes de datos, estructurados o no, y que difícilmente podrían ser tratados utilizando las herramientas convencionales de bases de datos.

Este volumen de datos puede venir de muy diversas fuentes, tales como redes sociales, transacciones comerciales, videos, etc., por lo que, para realizar esta labor de forma eficiente, es necesaria la utilización de *software* muy especializado ejecutándose en múltiples servidores.

Un aspecto relevante es la concepción de lo que es un «gran conjunto de datos». Para algunas empresas, un conjunto de estas características puede tener *petabytes*[64] y para otras solo cientos de *gigabytes*[65]. De forma general, el término *big data* se refiere a conjuntos de datos demasiado grandes y/o que cambian con demasiada rapidez (incluso en tiempo real) como para analizarlos con las herramientas convencionales.

Podríamos decir que los tres elementos más característicos del *big data* son:

- El grado de complejidad del conjunto de datos.
- La cantidad de valor o información que se pueden derivar usando las técnicas de análisis (tanto innovadoras como tradicionales).
- El uso de «datos longitudinales»[66], que complementa el análisis.

[64] Unidad de almacenamiento de información que equivale a 10^{15} *bytes*.
[65] Unidad de almacenamiento de información que equivale a 10^{9} *bytes*.
[66] Se refiere a datos que analizan el mismo tipo de información sobre los mismos temas en múltiples momentos a lo largo del tiempo.

En base a estos elementos, y debido al carácter no estructurado de gran parte de la información que se maneja dentro del *big data,* habitualmente se utilizan las denominadas bases de datos NoSQL[67] para almacenar los datos. Estas bases de datos se caracterizan principalmente por no tener la información estructurada en tablas y relaciones, como en las bases de datos convencionales (denominadas bases de datos relacionales), y no ser compatibles con el lenguaje SQL (utilizado de forma estándar para gestionar las bases de datos relacionales).

Estas bases de datos fueron originalmente creadas y utilizadas por grandes empresas tecnológicas como Google, Yahoo, Ebay o Facebook para almacenar la enorme cantidad de datos que manejaban, y cuyo volumen aumenta rápidamente y de forma exponencial. Algunos ejemplos de las técnicas de modelado de datos para gestionar este tipo de bases de datos serían (83): *key-value stores, bigtable, graph databases* o *document-stores.*

Entre sus principales ventajas, se encuentran las siguientes (84):

- Existe una amplia oferta de código abierto.
- Escalamiento sencillo.
- No generan cuellos de botella.
- Se pueden ejecutar en clústeres de máquinas baratas.
- Pueden manejar enormes cantidades de datos.

Principales vulnerabilidades del *big data*

Al igual que ocurre con la nube y con cualquier nueva tecnología, el *big data* no está exento de vulnerabilidades. Según la Cloud Security Alliance (85), los principales retos de seguridad a los que se enfrenta el *big data* debido a las vulnerabilidades inherentes que presenta son:

- Computación segura en *frameworks* de programación distribuidos. Los *frameworks* de programación distribuidos utilizan el paralelismo en la computación y en almacenamiento para procesar cantidades masivas de datos. Un ejemplo muy conocido es el framework MapReduce, que divide un archivo de datos en varios segmentos para su procesamiento distribuido. Como medidas de prevención, hay que garantizar la integridad tanto del archivo de datos como de los segmentos producidos y asegurar que no existen segmentos indeseados o extraños.
- Usar las mejores prácticas de seguridad en bases de datos no relacionales. Las bases de datos no relacionales más extendidas son las NoSQL. A pesar de que su uso está muy extendido, todavía está evo-

[67] *Not only* SQL.

lucionando la infraestructura de seguridad de las mismas. Por ejemplo, todavía no hay soluciones robustas y maduras para el «NoSQL injection». Dado que existen distintos tipos de bases de datos NoSQL, que utilizan conceptos y tecnologías distintos, se suele incluir la seguridad en las capas de acceso a las mismas.

- Almacenamiento de datos y *logs* seguro. Los datos y los registros de las acciones realizadas sobre el sistema se almacenan en sistemas multicapa en distintos servidores. La gestión manual de estos por parte del administrador del sistema permite un mayor control sobre exactamente qué dato se está manipulando y cuándo. Sin embargo, debido al continuo crecimiento del volumen de los mismos, es necesario el uso de herramientas que realicen estas actividades de forma automática. Estas herramientas deben estar protegidas frente accesos no autorizados.
- Validación y filtrado de entradas de datos. En muchos casos, los sistemas de *big data* utilizan conjuntos de datos provenientes de múltiples orígenes (p. ej., dispositivos *end-point*). Por tanto, es necesario el poder realizar una adecuada validación y filtrado de los datos de entrada, evitando cualquier posible incidente de seguridad.
- Monitorización de la seguridad en tiempo real. La monitorización de la seguridad en tiempo real siempre ha sido un reto debido al gran número de alertas generadas por los dispositivos y sistemas. Estas alertas, correlacionadas o no, inducen mucho a falsos positivos y son habitualmente ignoradas puesto que un operador no puede hacer frente a todas. Este problema se incrementa en el big data dado el volumen de datos y la velocidad del flujo de los mismos.
- Análisis y minería de datos que salvaguarden la privacidad. El big data puede ser visto como un amenazador elemento que potencialmente puede ser usado para invadir la privacidad, para realizar un *marketing* invasivo, disminuir las libertades civiles e incrementar el control estatal y corporativo sobre los usuarios. Es importante establecer unas guías y recomendaciones para prevenir la filtración de información privada inadvertidamente.
- Forzar el cifrado en el control de acceso y en las comunicaciones seguras. Para garantizar que los datos privados más sensibles son transmitidos de punto a punto de forma segura y que solo son accesibles por las entidades autorizadas, los datos deben estar cifrados basados en las políticas de control de acceso. Para garantizar la autenticación, el acuerdo y la equidad entre las entidades distribuidas, se tiene que implementar un marco seguro de comunicación cifrado.
- Control de acceso granular. Se debe dar acceso a las entidades solamente a aquellos datos para los que tienen las correspondientes autorizaciones.

– Auditorias granulares. Con la monitorización en tiempo real de la seguridad, se pretende alertar justo en el momento en que un ataque tiene lugar. Es necesario poder comprobar exactamente sobre qué datos se estaba intentando acceder.

– Procedencia de los datos. Debido a la propia naturaleza del *big data*, el volumen de información relativa al origen de los datos también crece rápidamente. Analizar esa ingente cantidad de información para detectar posibles dependencias o relaciones que tengan alguna implicación sobre la seguridad o confidencialidad del sistema y/o los datos que contiene es computacionalmente costoso.

«Consumerización» y BYOD

Tradicionalmente, los dispositivos que las empresas ponían a disposición de sus empleados, como ordenadores de escritorio, portátiles o teléfonos móviles, eran con frecuencia los más avanzados a los que aquellos tenían acceso. La proliferación de dispositivos de consumo como portátiles, *tablets, netbooks, smartphones,* etc., ha facilitado que los empleados dispongan en muchos casos de herramientas de productividad más avanzadas para su uso personal.

Por este motivo, a medida que la tecnología desempeña una función cada vez más importante en sus vidas personales, los empleados se acostumbran a la potencia y comodidad de los nuevos servicios (*web* 2.0, intercambio de datos con almacenamiento en la nube, correo *web*, conectividad permanente, etc.) y consultan el correo electrónico mediante *smartphones* y otros dispositivos móviles que también permiten almacenar y acceder a datos corporativos.

Desde el punto de vista del empleado, este prefiere trabajar con un portátil, *tablet* o *smartphone* elegido por él que adaptar sus necesidades y preferencias a un dispositivo seleccionado para cumplir los requisitos de una parte de la organización; lo mismo ocurre con las aplicaciones y servicios. Así, si Evernote, Google+ o Dropbox proporcionan una mejor experiencia para tomar notas, videocomunicaciones y almacenamiento en la nube que los respectivos servicios corporativos proporcionados por la empresa, los empleados terminarán haciendo uso de los primeros (86).

El neologismo *consumerización* hace referencia a la tendencia actual, en el área de TI, por la cual la tecnología y los servicios orientados al usuario común, utilizados de manera privada, (como redes sociales, almacenamiento en la nube, *webmail, smartphones*, portátiles o *tablets*), están pasando a formar parte de la tecnología empleada por las empresas y sus empleados para llevar a cabo sus obligaciones profesionales. Mediante la *consumerización*, los empleados de una empresa utilizan sus propios

dispositivos y aplicaciones particulares para realizar su trabajo. Es un término empleado para referirse al conjunto de nuevas tecnologías y servicios externos a una empresa determinada que permite a los usuarios trabajar en cualquier momento y lugar (87).

Debido a este movimiento, el modo de trabajar de empleados y empresas se está viendo transformado a gran velocidad. A pesar de no ser un término ampliamente extendido, la mayoría de los departamentos de TI se han enfrentado ya a alguno de los retos que presenta esta *consumerización.* Las implicaciones de la extensa utilización de dispositivos personales en el lugar de trabajo están forzando el cambio en las filosofías de trabajo y las prácticas de los profesionales de TI. La *consumerización* tiene un importante impacto en el modo en que los departamentos de TI de las empresas protegen sus puestos de trabajo y los datos corporativos (88).

El principal problema viene dado por el hecho de que las limitaciones hasta ahora impuestas por los departamentos de TI tienen su razón de ser: asegurar que el *software* corporativo es compatible con el *hardware* proporcionado, simplificar las tareas de soporte y, por encima de todo, garantizar la seguridad de la información.

La primera señal de que una empresa está aceptando la *consumerización* de la TI es la aplicación de programas «trae tu propio dispositivo» (ya referido anteriormente como BYOD). El BYOD se ha convertido en uno de los fenómenos que más incidencia ha tenido o tendrá en las organizaciones de TI. La tendencia BYOD permite que los empleados usen sus propios dispositivos, como ordenadores portátiles, *tablets* o *smartphones,* para acceder a los recursos de la empresa, así como aplicaciones móviles que habilitan el acceso a servicios corporativos (89).

Por tanto, el término BYOD se utiliza para referirse a una gran corriente actual que permite a los empleados conectarse a la red de su empresa y acceder a sus datos mediante la utilización de sus dispositivos personales. Requiere, por consiguiente, la introducción de algunos cambios para adaptarse al empleo de nuevos dispositivos en el entorno laboral. Los programas BYOD revelan que las empresas no solo toleran el uso de dispositivos responsabilidad y propiedad del usuario sino que también lo incentivan y lo promueven.

Según diversos informes (90), el BYOD está ya bien establecido en el mundo empresarial y su nivel de implantación continúa en claro ascenso. Se estima que el porcentaje de empresas que soportan de manera formal BYOD aumentó del 72% al 76% entre el año 2011 y el 2012. Además, un 13% asegura que planea incorporar programas BYOD en los próximos 12 meses. Solo un 5% no tiene planes de incorporar nunca BYOD de manera formal.

Principales vulnerabilidades del BYOD

Normalmente, el primer paso para la adopción de BYOD es permitir el uso de *smartphones* personales para acceder al correo corporativo. Este hecho sirve de ejemplo para ilustrar algunos de los aspectos que deben ser tenidos en cuenta por parte de las empresas al incorporar estas prácticas a su modelo de negocio.

Si el *smartphone* es propiedad del empleado, no hay garantía de que la información de la empresa (correos y ficheros adjuntos) que quede almacenada en el dispositivo pueda ser protegida de todas las aplicaciones que pueden estar ejecutándose en él. Si una aplicación maliciosa enviase dicha información a un tercero, no queda claro sobre quién recaería la responsabilidad de sus consecuencias.

En muchas ocasiones, la información de identificación y autenticación que el usuario utiliza para acceder al correo corporativo es la misma que para acceder a otros recursos de la empresa. Por tanto, aumentan gravemente las posibles consecuencias si estos datos fuesen robados y enviados a un atacante sin que el usuario legítimo fuese consciente de ello.

Mientras las empresas ven en la tendencia BYOD una estrategia para reducir costes y aumentar la productividad, los departamentos de TI y seguridad de la información suelen poner de manifiesto los numerosos riesgos que esta nueva práctica TI supone para el control de la empresa sobre su propia información, haciéndola altamente vulnerable, además de aumentar el abanico de dispositivos, plataformas y aplicaciones sobre los que proporcionar soporte.

La tabla 1 muestra algunos ejemplos de las principales vulnerabilidades y los riesgos asociados a los que se enfrentan las empresas con las nuevas tendencias de *consumerización* descritas en los párrafos anteriores (91):

Tabla 1. Principales vulnerabilidades del BYOD (fuente: ISACA, 2012).

Vulnerabilidad	Amenaza	Riesgo
La información viaja a través de redes inalámbricas que normalmente son menos seguras que aquellas cableadas.	Numerosos ataques documentados sobre redes inalámbricas.	Interceptación de información con el resultado de acceso a información sensible. Daño a la imagen de la empresa.
La movilidad proporciona la oportunidad de extender la zona de trabajo más allá de los límites físicos de las instalaciones de la empresa, por lo tanto, determinadas medidas y controles de seguridad no tienen efecto.	Los dispositivos de usuarios pueden contener *malware*, que podría ser más fácilmente introducido en las redes y sistemas de la organización.	Propagación de *malware*. Fuga de datos. La integridad, disponibilidad y confidencialidad de los datos pueden verse afectadas.

Vulnerabilidad	Amenaza	Riesgo
Muchos usuarios utilizan la tecnología *Bluetooth* para conectar dispositivos manos libres; sin embargo, no lo deshabilitan cuando no se está utilizando.	El dispositivo es visible para *hackers*, pudiendo lanzar un ataque.	Corrupción del dispositivo. Pérdida de datos. Exposición de información sensible.
El dispositivo almacena información no cifrada.	En el caso de pérdida o robo del dispositivo, la información almacenada en él estaría en claro y sería accesible a terceros.	Exposición de información sensible.
La pérdida de datos puede afectar a la productividad del empleado.	Debido a la portabilidad, los dispositivos pueden sufrir pérdidas o robos, y con ellos toda la información que almacenan.	Fuga de información.
La organización no gestiona los dispositivos.	Si no existe una estrategia de dispositivos móviles, el empleado puede conectar fácilmente sus dispositivos inseguros a la infraestructura de red de la empresa.	Fuga de información. Propagación de *malware*. Pérdida de control de la ubicación y accesos a la información.
El dispositivo permite la instalación de aplicaciones de terceras partes.	Las aplicaciones pueden contener *malware*, troyanos o virus.	Propagación de *malware*. Fuga de información. Puertas traseras en la red de la empresa.

Las vulnerabilidades mostradas en la tabla anterior evidencian la presencia de riesgos asociados al BYOD que deberán ser gestionados mediante estrategias (92) que contemplen no solo aspectos técnicos sino también organizativos.

Redes sociales

Es obvio que las denominadas redes sociales en Internet, como servicios que proporciona un medio de comunicación social que se centra en encontrar gente para relacionarse en línea, normalmente formadas por personas que comparten alguna relación, principalmente de amistad, mantienen intereses y actividades en común o están interesados en explorar los intereses y las actividades de otros, se están convirtiendo en muy populares y han comenzado a cambiar la forma en que vivimos y trabajamos.

Muchas empresas están evaluando el potencial de aprovechamiento de las oportunidades comerciales de esta tecnología. Aunque las activida-

des comerciales de redes sociales pueden ser un importante refuerzo de la productividad de las grandes empresas, algunos consideran que estas actividades pueden ser pérdidas de tiempo y trampas a su seguridad.

No obstante, el uso de las redes sociales por parte de las empresas como herramienta para interactuar y relacionarse con clientes sigue teniendo un enorme crecimiento. Entre las principales ventajas que ofrece el uso de estas herramientas por parte de las empresas, están (93):

- Difusión y compartición de información.
- Comunicación.
- Colaboración e innovación.
- Formación.
- Gestión del conocimiento.
- Gestión de actividades.

Frente a estas ventajas, diversos estudios (94) indican que casi dos tercios de las empresas encuestadas responden que las redes sociales pueden constituir un gran riesgo a su reputación de marca. Sin embargo, en esos mismos estudios, también se indica que el 60% de las empresas no forma a sus empleados acerca del uso de las redes sociales en relación con sus políticas de comunicación social, o únicamente lo hace en el momento de la contratación. Además, el 43% de las empresas indican que tienen menos de un empleado con dedicación específica para la gestión de esos riesgos.

En este mismo sentido, varios informes (95) apuntan a que, del total de las compañías incluidas en la lista «Fortune Global 100», un 65% tiene cuentas de Twitter activas, un 54% dispone de al menos una página corporativa en Facebook, un 50% emplea un canal propio en YouTube y un 33% dispone de *blogs* corporativos.

Principales vulnerabilidades de las redes sociales

Hay un aspecto que escapa al uso directo que las compañías hacen de las redes sociales y son los ataques directos a su reputación provenientes de terceros. Así, las redes sociales pueden afectar a la reputación de una empresa, más allá de las actividades que esta realice en las citadas redes. La publicación de comentarios negativos sobre una marca o la distribución de material ilegitimo de una compañía puede circular por Internet y distribuirse a tal velocidad que pueden representar altos costos para una empresa que no detecte a tiempo tales incidentes, afectando la imagen y reputación de la misma.

En este sentido, diversos estudios (96) apuntan a la necesidad de usar herramientas de monitorización de redes sociales como mecanismos

para vigilar, analizar y medir la actividad que se produce en relación con una marca o empresa en estas redes.

Por otro lado, para identificar mejor los peligros más comunes que pueden ser explotados por el uso de las redes sociales en las empresas, tal y como proponen varios informes (97), diferenciaremos a continuación entre las vulnerabilidades asociadas a la presencia corporativa en redes sociales y las asociadas al uso por parte de los empleados de las redes sociales.

Vulnerabilidades asociadas a la presencia corporativa en redes sociales

- Introducción de código malicioso o malware. Con la extensión del uso de las redes sociales, estos sistemas se prestan como elementos que pueden permitir la propagación de todo tipo de amenazas informáticas (virus, gusanos, troyanos, *spywares*, *adware*, etc.). Un ejemplo de esto fue el gusano Koobface, que se propagó masivamente durante el año 2009, continuando en la actualidad su dispersión de forma limitada, y que empleó Facebook como principal vía de ataque. Posibles consecuencias de esto serían el robo o fuga de información, infección de equipos, ataque a otros sistemas como parte de redes *bot* y caída de sistemas, así como el impacto en los recursos necesarios para volver a un nivel de actividad normal.
- Robo o secuestro de credenciales o identidad. En general, el acceso a los perfiles de las redes sociales se realiza utilizando el clásico par usuario/contraseña, por lo que utilizando técnicas como la ingeniería social, la búsqueda en Internet, fuerza bruta, etc., un atacante podría conseguir acceso al perfil corporativo y, a partir de la modificación de las credenciales, tomar control del perfil. Las consecuencias de esto pueden ir desde la extorsión a la compañía a la publicación de información falsa, con las consecuencias que esto puede tener para la imagen y reputación de la empresa, la cotización de la misma, etc. Así mismo, en función del uso que se haga de ello, las empresas pueden tener que afrontar posibles demandas por los daños provocados. Ejemplo de esto fue la falsa noticia publicada en la cuenta de Twitter de la agencia de noticias Associated Press (98) en abril de 2013, en la que anunciaban explosiones en la Casa Blanca que habían herido al presidente Obama; a raíz de la publicación y de forma inmediata, el índice de la bolsa de Nueva York bajó 120 puntos. Las credenciales de acceso a la cuenta habían sido robadas y eso permitió la publicación.
- Creación y empleo de identidades falsas. Un caso particular del anterior es la creación de una falsa identidad de la compañía en alguna red social y la publicación de informaciones falsas en la misma o la obtención, a través de ella, de contacto con los clientes reales o em-

pleados de la empresa, pudiendo emplear esto como base de otro tipo de ataques para conseguir acceso tanto a otras empresas clientes como a la propia compañía. Las posibles consecuencias, al igual que en el caso anterior, pueden ir desde la extorsión a la compañía a la publicación de información falsa, con las consecuencias que esto puede tener para la imagen y reputación de la empresa, la cotización de la misma, etc., así como las posibles demandas que la empresa pueda tener que afrontar. En los últimos años se han producido múltiples ejemplos del uso de falsos perfiles en diferentes redes sociales.

- Falta de definición sobre los derechos de autor de los contenidos publicados en redes sociales. Los términos de uso de las diferentes redes sociales incluyen cláusulas según las cuales se cede la propiedad, o al menos el posible uso, de cualquier información publicada en las mismas. Como consecuencia de esto, una empresa podría perder toda la propiedad intelectual sobre los activos publicados en redes sociales.
- Mayor nivel de demanda de los clientes. La exposición de la compañía en las redes sociales puede generar un nivel de demanda apoyada por la facilidad y universalidad de acceso a las mismas redes sociales por parte de posibles clientes, de forma que la empresa no sea capaz de responder de forma adecuada, lo que puede provocar descontento y desconfianza en los clientes e impactar en la imagen de la compañía.
- Filtración de información o publicación de información objeto de algún tipo de protección legal. Se puede producir filtración de información, bien por error, bien de forma intencionada, así como la publicación de información objeto de algún tipo de protección legal, como por ejemplo datos de carácter personal. Estas acciones pueden culminar en daños a la imagen y al valor de la compañía, sanciones legales, multas o demandas.

Vulnerabilidades asociadas al uso por parte de los empleados de las redes sociales

- Uso de cuentas personales en redes sociales para publicar información relacionada con el trabajo. Cada vez es mayor la información que los usuarios comparten en redes sociales. No solo es el nombre, la edad o el sexo, sino que además se incluyen datos de contacto, ubicación geográfica, fotografías, empleo, vídeos, etc. La exposición de la privacidad no solo es un riesgo asociado para los usuarios sino también para las empresas. Un ejemplo de ello es el de usuarios publicando situaciones laborales, problemas con compañeros o jefes, información de clientes, temáticas de reuniones, trabajos o proyectos y otros datos confidenciales de la empresa que, expuestos, pueden afectar la integridad de la misma. A través de los elementos publicados, se puede obtener gran cantidad de información sobre las activi-

dades presentes y futuras de una empresa. Posibles consecuencias de esto serían la filtración de información de la compañía, posibles ataques, por ejemplo, usando técnicas de phishing, daños a la reputación e imagen, etc.

- Uso de las redes sociales en el lugar de trabajo. El uso excesivo de las redes sociales por parte de los empleados de una compañía en su lugar de trabajo, sin tener ninguna responsabilidad asociada a este uso por parte de la empresa, puede dar lugar a problemas de congestión en las redes corporativas, pérdida de productividad de la compañía y aumento de la exposición de los empleados a posibles infecciones por *malware*, tal y como ya se ha expuesto.
- Uso de las redes sociales en dispositivos móviles corporativos. El uso de redes sociales, especialmente empleando perfiles personales, en los dispositivos móviles corporativos puede dar lugar a la infección de esos equipos y al robo de información a través de esas posibles infecciones, teniendo en cuenta que en la actualidad los controles aplicados a esos dispositivos, en general, son menores que a los aplicados a los dispositivos tradicionales.

Buenas prácticas de seguridad para las empresas en el ciberespacio

Uso de productos certificados

Una de las buenas prácticas en el ámbito empresarial puede ser el despliegue de productos TIC cuyas características de seguridad hayan sido certificadas por entidades independientes. El consumo de productos certificados supone a la empresa una mayor garantía de seguridad al incorporar productos en su organización cuyas propiedades de seguridad han sido evaluadas por terceros. El empleo de herramientas certificadas supone que estas han probado su utilidad en la mitigación del riesgo por materialización de amenazas y, además, se han demostrado libres de vulnerabilidades en el momento de su certificación.

En la actualidad, existen múltiples esquemas de certificación de la seguridad TIC. Unos son propietarios, y otros especializados en ciertas tecnologías. A lo largo de este capítulo, se analizará el esquema de certificación Common Criteria, al ser este un esquema global independiente de la tecnología TIC a certificar y ampliamente reconocido internacionalmente.

La norma «Common Criteria»

Los Criterios Comunes para la Evaluación de la Seguridad de los Productos de las Tecnologías de la Información (*Common Criteria for Information*

Technology Security Evaluation) constituyen un estándar internacional que, como su propio nombre indica, establece criterios comunes, rigurosos y objetivos para la evaluación de la seguridad de los productos TIC.

La norma *Common Criteria* (CC) está formada por una serie de documentos que tratan los diferentes aspectos de la evaluación de un objeto a evaluar (OE), es decir, el conjunto de *software*, *firmware* y/o *hardware* acompañado por las guías de uso e instalación que están dentro del alcance de la evaluación.

- En la primera parte de la CC (99), se recogen los fundamentos en los que se basa la certificación del producto, definiendo los conceptos básicos de la evaluación y certificación.
- En la segunda parte (100), se establece fundamentalmente una taxonomía que permite a los desarrolladores declarar las funcionalidades de seguridad que se evaluarán en su producto, es decir, los requisitos funcionales de seguridad. Esta taxonomía permite definir rigurosamente las características de seguridad del producto a certificar.
- La tercera parte de la norma CC (101) establece una segunda taxonomía que define los requisitos asociados a la garantía de seguridad declarada por el desarrollador, es decir, define, dependiendo del nivel de garantía, las actividades que el evaluador tiene que verificar durante la evaluación de un producto.

La norma CC no es específica para ninguna tecnología en concreto y, a priori, puede ser aplicada para evaluar la seguridad de cualquier producto o sistema TIC. Este estándar está complementado por una metodología de evaluación, *Common Methodology for IT Security Evaluation* (CEM) (102), que es aplicada por los laboratorios acreditados en los esquemas de certificación para verificar el cumplimiento de los requisitos de seguridad que han sido declarados por el desarrollador.

Cabe señalar que CC y CEM han sido reconocidos como estándares internacionales, conformando las normas ISO/IEC15408 (103) (104) (105) e ISO/IEC18045 (106), respectivamente. El mantenimiento de la norma se realiza por parte de las naciones firmantes del Acuerdo de Reconocimiento CCRA *(Common Criteria Recognition Arrangement)* (107), que se analizará más adelante. Una vez aprobadas las modificaciones, el comité de gestión de la CC pone a disposición de la comunidad ISO los criterios y la metodología, quien las incorpora a su catálogo de normas internacionales cuando lo considera oportuno.

Aspectos evaluados en un proceso de certificación «Common Criteria»

Tal y como se establece en la parte 1 de la CC, una certificación de este tipo se basa en proporcionar garantías por una entidad externa sobre las

características de seguridad declaradas por el fabricante. Estas características las debe recoger el fabricante en un documento denominado *Declaración de seguridad,* el cual constituye el elemento fundamental en el marco de una certificación CC.

La *Declaración de seguridad* es un documento público emitido por el desarrollador del objeto a evaluar (OE) en el cual este declara las propiedades de seguridad (requisitos funcionales de seguridad de la parte 2) que serán evaluadas en el proceso de certificación. En este documento, también se establece el problema de seguridad a estudiar en la evaluación y, por lo tanto, cubierto por el certificado. Es decir, se definen los objetivos de seguridad que cumple el OE, las amenazas frente a las que protege y establece las condiciones e hipótesis del entorno bajo las que se va a producir la evaluación. Estas últimas tendrán que ser aplicadas por el consumidor en el entorno final de operación del OE para que la garantía de seguridad certificada se demuestre válida.

Una vez establecida la *Declaración de seguridad,* es labor del laboratorio acreditado la evaluación del cumplimiento estricto de las propiedades de seguridad declaradas, teniendo en cuenta el entorno declarado por el desarrollador. El evaluador tiene que verificar que efectivamente el OE cumple con los objetivos de seguridad declarados y, por tanto, demuestra una protección efectiva en el entorno considerado frente a las amenazas declaradas.

Para realizar esta labor de evaluación, el laboratorio, teniendo en cuenta el nivel de garantía declarado por el desarrollador en la *Declaración de seguridad,* efectuará todas las actividades de evaluación que se correspondan con dicho nivel, recogidas en la parte 3 de CC, aplicando la metodología de evaluación definida en el CEM. Una vez que se hayan satisfecho todos los requisitos marcados por la norma tanto por parte del desarrollador, al facilitar todos los elementos documentales, procedimentales y técnicos necesarios, como por parte del evaluador, aplicando y demostrando la aplicación de la metodología de evaluación, se emitirá el certificado correspondiente, siempre que el proceso haya sido satisfactorio. Todo el proceso de evaluación es verificado y validado por parte de la entidad emisora del certificado, el Organismo de Certificación, quien vela por el estricto cumplimiento de la norma y de los procedimientos definidos por esta entidad para las certificaciones de este tipo.

Las certificaciones CC intentan cubrir el espectro completo de la seguridad del OE, a diferencia de las auditorías de seguridad, bien sean técnicas (revisión de código, pruebas de penetración, etc.) o de otras certificaciones que son meramente verificaciones funcionales de los requisitos implementados. Por lo tanto, un certificado Common Criteria se puede decir que certifica y evalúa prácticamente todos los aspectos relacionados con

la seguridad del OE, desde su diseño e implementación hasta los procedimientos de entrega empleados por el desarrollador para entregar el OE al consumidor final.

Otro de los aspectos fundamentales de una certificación CC es el nivel de garantía de seguridad declarado para la evaluación (EAL, *Evaluation Assurance Level*). Este nivel de garantía determina las actividades de evaluación que se han de desarrollar en el transcurso de la certificación. En la CC se definen hasta siete niveles de garantía, aumentando progresivamente la cantidad de actividades de evaluación a llevar a cabo y la profundidad de las mismas, lo que a su vez permite al consumidor ganar mayor confianza con cada nivel.

Estos niveles también marcan el nivel de detalle de la documentación y la cantidad de evidencias relacionadas con el OE que ha de proporcionar el desarrollador al evaluador para que este pueda realizar su trabajo. Teniendo en cuenta lo anterior, se puede decir que a mayor nivel de garantía, mayor esfuerzo tiene que ser dedicado tanto por el desarrollador como por el evaluador en el transcurso de la certificación.

A continuación, se recogen brevemente las características principales de los niveles de garantía más habituales:

- EAL 1: probado funcionalmente. El evaluador desarrolla su plan de pruebas basándose en la especificación funcional a alto nivel del desarrollador. Es decir, en este nivel de garantía el evaluador no cuenta con mucho conocimiento de cómo está desarrollado e implementado el OE. El análisis de vulnerabilidades se basa en la recopilación de vulnerabilidades de dominio público que puedan ser aplicables al OE y su posterior prueba, teniendo en cuenta que el perfil del atacante se considera básico (pocos medios, poco conocimiento, etc.).
- EAL 2: probado estructuralmente. La novedad de este nivel de garantía es que el evaluador cuenta, aparte de la especificación funcional, con un documento que describe la arquitectura de seguridad del OE y el diseño del mismo, por lo tanto, dispone de mayor información para incorporar a su plan de pruebas funcionales. Por otro lado, el propio desarrollador tiene que diseñar un plan de pruebas propio y ejecutarlo, de forma que se demuestre que cumple con las funcionalidades declaradas para las interfaces de seguridad. El evaluador verificará que los resultados de las pruebas del desarrollador son veraces y que ejercitan las funcionalidades declaradas por el desarrollador y, adicionalmente, propondrá pruebas teniendo en cuenta la especificación funcional y la arquitectura del OE. El análisis de vulnerabilidades realizado para este nivel de garantía empieza a tener en cuenta los aspectos específicos de la implementación del OE, aparte de las vulnerabilidades de dominio público que puedan estar presentes.

– EAL 3: probado y comprobado metodológicamente. La novedad de este nivel de garantía es que el desarrollador aporta una especificación funcional y de diseño con un nivel de detalle mayor. Los requisitos relacionados con el ciclo de vida del OE son mayores, por tanto, existe mayor conocimiento de los procedimientos de seguridad empleados por el desarrollador en el desarrollo del OE. Teniendo en cuenta que el evaluador cuenta con un nivel de detalle mayor sobre el desarrollo del OE, las pruebas funcionales tanto del desarrollador como del evaluador permiten verificar con mayor detalle la correcta implementación de funcionalidades de seguridad. Por defecto, el análisis de vulnerabilidades es el mismo que para el nivel anterior, pero con una diferencia fundamental: el evaluador cuenta con mayor información sobre el desarrollo del OE, lo que le permite plantear un mayor número de casos de prueba y descartar mayor número de vulnerabilidades relacionadas con el diseño y especificación del OE.
– EAL 4: diseñado, probado y revisado metodológicamente. La característica fundamental de este nivel de garantía es que el desarrollador tiene que aportar como evidencia la representación de la implementación de las funcionalidades de seguridad, por ejemplo, el código fuente en el caso de que el OE sea software. Asimismo, el nivel de detalle de la documentación de diseño y de especificación funcional son mayores, hecho que se ve reflejado en el nivel de detalle de las pruebas funcionales y en el análisis de vulnerabilidades al contar el evaluador con mayor información para probar y atacar al OE.

Existen otros tres niveles de garantía mayores (EAL 5, EAL 6 y EAL 7), pero el número de productos certificados en estos niveles es muy escaso y existen numerosas restricciones para el reconocimiento mutuo de estos niveles de garantía.

Consumo de productos certificados CC

Para el caso en el que una empresa desee aplicar las buenas prácticas que aconsejan el consumo de productos certificados, debería seguir una serie de indicaciones a la hora de valorar la idoneidad de estos productos.

La forma más adecuada para valorar la idoneidad de un producto certificado es a partir de un análisis de riesgos para la organización en el que se puedan apreciar las amenazas que se desean mitigar, para poder así elegir los productos que mejor se ajusten a las necesidades de la organización y que permitan mitigar el riesgo detectado. La norma CC, mediante la Declaración de Seguridad, permite adecuarse a un posible modelo de análisis de riesgos que se haya aplicado en el entorno empresarial.

Una posible empresa consumidora debe valorar las propiedades de seguridad de los productos certificados basándose en las declaraciones de se-

guridad e informes de certificación pertenecientes a los productos certificados que se desean adquirir y compararlos con las necesidades extraídas de sus análisis de riesgos. Para obtener esta información, el consumidor debe dirigirse al sitio web del Organismo de Certificación o la página web del CCRA, donde encontrará la relación de productos certificados CC.

Una vez el consumidor dispone de las declaraciones de seguridad de los productos certificados elegibles, este tiene que valorar el resumen de las características de seguridad del OE, que se encuentran en la introducción de la declaración, para posteriormente pasar a valorar el problema y los objetivos de seguridad.

Una vez visto el resumen, se debe analizar el problema de seguridad, que recoge explícitamente los siguientes apartados:

- Amenazas: parte en la que se encuentra el conjunto de amenazas que mitiga el OE por sí mismo, o bien el entorno operacional, o ambos en conjunto.
- Políticas organizativas de seguridad: parte en la que se encuentra el conjunto de políticas que implementa el OE por sí mismo, o bien el entorno operacional, o ambos en conjunto.
- Hipótesis: parte en la que se recoge el conjunto de hipótesis realizadas para el entorno operacional, de forma que este sea capaz de mitigar las amenazas o implementar las políticas.

Teniendo en cuenta lo anterior, el entorno operacional ha de configurarse por la empresa consumidora de una determinada forma para que las hipótesis realizadas por el fabricante sean factibles y ayuden a mitigar las amenazas. La forma de configurar el entorno se recoge en los manuales de preparación y operación del OE, en los que se indica al consumidor cómo preparar y operar el OE para cumplir con los objetivos de seguridad y mitigar las amenazas.

Por otro lado, el consumidor tiene que tener en cuenta que son el OE y su entorno operacional en conjunto los encargados de mitigar el conjunto de amenazas declaradas. Para diferenciar claramente qué amenazas mitiga el OE y qué amenazas mitiga el entorno, el consumidor tiene que analizar el apartado de la *Declaración de seguridad* en el que se definen los objetivos de seguridad. En dicho apartado, se citan explícitamente aquellos que implementa el OE y aquellos que son delegados a su entorno operacional.

- Los objetivos de seguridad del OE: son el conjunto de objetivos que son alcanzados mediante la funcionalidad propia del OE para mitigar una o varias amenazas o implementar una o varias políticas del problema de seguridad.
- Los objetivos de seguridad del entorno: son el conjunto de objetivos que son alcanzados mediante una serie de medidas técnicas o pro-

cedimentales que se aplican al entorno en el que se encuentra el OE, y que permiten mitigar una o varias amenazas o implementar una o varias políticas del problema de seguridad.

Cabe señalar que, durante la evaluación del producto certificado, los laboratorios acreditados realizan sus análisis para verificar que el OE es capaz de cumplir con sus objetivos de seguridad y verifican que las propiedades declaradas son ciertas.

Las restricciones en el certificado tienen que ver con lo declarado para el entorno y las hipótesis de uso, por tanto, el consumidor, en este caso la empresa, tiene que analizarlas para ver si puede cumplir con lo requerido por la declaración de seguridad. En el caso de la evaluación, los laboratorios configuran, preparan y operan el entorno tal y como se recoge en los manuales que forman parte del OE y que se suministran al consumidor final, pero las hipótesis realizadas se consideran ciertas por sí mismas, por lo que no se prueban en el proceso de evaluación.

Una vez analizado el problema de seguridad, se puede entrar a comparar los diferentes productos, teniendo en cuenta el nivel de garantía, con el principio de que a mayor nivel, mayor número de actividades de evaluación y profundidad de las mismas, por lo que la confianza en la seguridad del producto es mayor.

En relación a este punto, se debe insistir en que la empresa consumidora debe valorar su problema de seguridad, ya que puede darse el caso de que un producto certificado con un mayor nivel de garantía no cumpla las necesidades requeridas por la empresa y, en cambio, otro producto con un nivel de garantía menor cumpla con parte o todas la necesidades. En este caso, para el entorno empresarial, sería recomendable adquirir aquel que cumpla con el mayor número de necesidades, independientemente del nivel de garantía. En los casos en los que los objetivos y el problema de seguridad sean equivalentes es cuando se puede entrar a valorar los diferentes niveles de garantía.

Por otro lado, el consumidor puede encontrar mayor información en el informe de certificación que suele acompañar al producto, de forma que una posible empresa consumidora puede encontrar en él la lista de elementos que conforman el OE o la estrategia de pruebas seguida por el evaluador. En ciertos casos, las recomendaciones o restricciones tanto del laboratorio evaluador como del certificador pueden servir para aclarar algunas de las hipótesis de uso o reseñar la importancia de cumplir estrictamente con alguno de los objetivos del entorno. Teniendo en cuenta esto es muy recomendable verificar estos apartados del informe de certificación antes de consumir productos certificados.

Por último, se debe tener en cuenta que, independientemente del nivel de garantía y de las restricciones de uso, todos los productos certificados

han pasado por una evaluación por parte de entidades independientes ajenas a los propios desarrolladores o fabricantes. En el proceso de evaluación se han verificado las características de seguridad declaradas, por lo tanto, el certificado aporta mayor confianza en la seguridad de estos productos que aquellos que nunca han sido evaluados por terceros. Se puede concluir que los productos certificados, independientemente del problema de seguridad o nivel de garantía declarado, siempre aportan mayores garantías que aquellos que no se han enfrentado a un proceso de certificación.

La norma CC en la cadena de suministro

Tal y como se ha señalado anteriormente, la norma CC, aparte de abarcar actividades de evaluación puramente técnicas, como las relacionadas con el desarrollo del OE o las pruebas funcionales o de penetración, evalúa los aspectos procedimentales relacionados con el ciclo de vida completo del OE. La CC contempla la evaluación de aspectos como la gestión de configuración, los procedimientos de entrega del OE en todo el ciclo de vida o la evaluación de las medidas de seguridad empleadas en el lugar de desarrollo del OE.

Desde el punto de vista de la gestión de la configuración, para niveles de garantía EAL3 o superiores, la norma CC evalúa que todos los componentes que conforman el OE estén identificados unívocamente, de forma que el desarrollador ha de proporcionar al evaluador una lista de configuración que incluya todos los elementos que componen el OE (funciones, clases, objetos, librerías, circuitos integrados, máscaras, etc.). También el desarrollador tiene que disponer de un plan de control de la configuración en el que se indiquen las medidas seguidas para que solo se puedan incorporar cambios a los elementos de configuración que hayan sido autorizados previamente y, además, todos estos elementos de configuración tienen que mantenerse en un sistema (herramienta) de gestión de la configuración. Este sistema de gestión de la configuración tiene que indicar además quién es el desarrollador de cada uno de los elementos que componen el OE, por lo que, en caso de que existan procesos de subcontratación, el desarrollador debe indicar al menos el responsable del desarrollo de cada elemento.

Atendiendo a los procedimientos de entrega del OE en la CC, para niveles de garantía EAL2 o superiores el desarrollador ha de documentar los procedimientos de entrega de todas las partes que componen el OE, de forma que en el plan de entrega se indiquen todas las medidas de seguridad aplicadas que garanticen la seguridad de la entrega del OE y así se garantice la integridad del mismo en la entrega. Así mismo, el desarrollador ha de proporcionar asimismo la información suficiente al consumidor del OE certificado para verificar que la versión de producto

que recibe no ha sido modificada en el proceso de entrega, de forma que se garantice la integridad de las características de seguridad del OE si el consumidor respeta las indicaciones proporcionadas en los manuales y guías que forman parte del OE.

Finalmente, para niveles de garantía EAL3 o superiores, la CC indica la obligación de que el desarrollador proporcione al evaluador la documentación de seguridad que describa todas las políticas y procedimientos de seguridad del entorno de desarrollo; esta documentación debe describir todas las medidas de seguridad físicas y lógicas, medidas de seguridad en las personas y todas aquellas otras medidas que garanticen la confidencialidad e integridad del diseño y la implementación del OE. En este caso, se considera entorno de desarrollo todos aquellos lugares donde se han desarrollado tareas de implementación o diseño que puedan afectar a la seguridad del OE, de tal forma que en el caso de que parte de los desarrollos hayan sido subcontratados, la empresa subcontratada también tiene que proporcionar dicha documentación.

Resulta pues evidente, a la vista de los requisitos marcados por la CC para la evaluación del ciclo de vida del OE, que la CC puede ser una herramienta útil para la evaluación de la seguridad de la cadena de suministro de los productos de seguridad a ser utilizados por las empresas.

Buenas prácticas para la gestión de la seguridad de la información

ISO 27000: Sistemas de gestión de la seguridad de la información

Un sistema de gestión de la seguridad de la información (SGSI) es una herramienta que permite a la organización mantener el nivel de riesgo asociado al manejo de sistemas de información y comunicaciones por debajo del umbral establecido por sus responsables. Con objeto de proporcionar un marco de referencia común para su desarrollo y basándose en experiencias previas en este ámbito, la Organización Internacional para la Normalización (ISO, *International Organization for Standardization*) ha elaborado un conjunto de normas, agrupadas en la serie ISO 27000.

Esta serie de normas recoge la experiencia de ISO en el desarrollo de otros sistemas de gestión corporativa, como los relacionados con la gestión de la calidad (ISO 9000) o la gestión medioambiental (ISO 14000), y comparte con estos modelos la necesidad de entender la gestión como un proceso orientado a la mejora continua, cuyo elemento clave es el Ciclo de Deming o PDCA *(Plan Do Check Act)*.

El ciclo PCDA consiste en la ejecución iterativa de cuatro fases:

- Planificar: fase en la que se determinan los objetivos que se desean alcanzar, así como los recursos, métodos, actividades y procedimientos necesarios para el logro de dichos objetivos.
- Hacer: o puesta en práctica de las actividades planificadas durante la fase de planificación.
- Verificar: incluye la medición de los resultados alcanzados por las actividades implantadas.
- Actuar: fase que, tras la comparación entre los objetivos propuestos y los resultados alcanzados, permite identificar aquellas áreas que, por no haber alcanzado las metas esperadas, requieren la aplicación de alguna medida correctora. La planificación de estas medidas da inicio a una nueva iteración del ciclo completo.

Las dos normas fundamentales de la serie ISO 27000 son la ISO/IEC 27001 y la ISO/IEC 27002, ambas editadas por la Organización Internacional para la Normalización en 2005.

La norma ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements* (108), es el documento básico de la serie 27000 y en él se especifican los requisitos mínimos que la organización debe cumplir para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI, definiendo las acciones a realizar en cada una de las fases del ciclo de mejora continua.

Una organización que disponga de un SGSI implantado y en operación puede solicitar su certificación por parte de una entidad autorizada; en caso de superar satisfactoriamente este proceso de revisión, se emite el certificado correspondiente.

Por otro lado, la norma ISO/IEC 27002:2005, *Information technology - Security techniques - Code of practice for information security management* (109), complementa a la ISO 27001 y, a diferencia de esta, no es certificable. Su objetivo es proporcionar una relación de medidas de seguridad fruto de la experiencia acumulada en este ámbito y que pueden ser utilizadas como referencia a la hora de seleccionar las medidas de seguridad asociadas al establecimiento y mantenimiento de un SGSI.

La norma está estructurada en once capítulos, cada uno de los cuales está dedicado a un ámbito específico de la seguridad de la información y que suelen denominarse «dominios de seguridad». Cada uno de estos capítulos se divide en categorías principales de seguridad, también denominadas «objetivos de control» que, a su vez, se subdividen en una o más medidas de seguridad o «controles de seguridad», de acuerdo con la distribución contenida en la tabla 2 adjunta.

Tabla 2. Estructura de dominios de seguridad, objetivos de control y controles de la norma ISO 27002.

Dominios de seguridad	Objetivos de control	Controles
Política de seguridad.	1	2
Aspectos organizativos de la seguridad de la información.	2	11
Gestión de activos.	2	5
Seguridad ligada a los recursos humanos.	3	9
Seguridad física y ambiental.	2	13
Gestión de comunicaciones y operaciones.	10	32
Control de acceso.	7	25
Adquisición, desarrollo y mantenimiento de sistemas de información.	6	16
Gestión de incidentes de seguridad de la información.	2	5
Gestión de la continuidad del negocio.	1	5
Cumplimiento.	3	10
	39	133

Actualmente, ambas normas están en proceso de revisión por el organismo encargado de su elaboración, estando prevista la publicación de una nueva versión en octubre de 2013.

«20 Critical Security Controls»

Los denominados «20 Controles críticos de seguridad para una ciberdefensa efectiva» son el resultado de un consenso alcanzado por el consorcio auspiciado por el CSIS[68] (Center for Strategic and International Studies) norteamericano, en el que estaban representados, entre otros muchos, organismos tales como: NSA[69], US Cert[70], DoD JTF-GNO, Department of Energy Nuclear Laboratories, Department of State, DC3 (DoD Cyber Crime Center), etc. Actualmente, el organismo encargado de publicar la documentación referente a los *20 Controles críticos* (110) es el SANS Institute[71].

Se trata de un conjunto de medidas de seguridad cuyo objetivo es servir como elemento de apoyo a la decisión, que proporciona una guía que permita a las organizaciones priorizar sus inversiones en materia de seguridad y garantiza que las medidas que se implantan son aquellas cuya

[68] http://csis.org/.
[69] http://www.nsa.gov/.
[70] http://www.us-cert.gov/.
[71] http://www.sans.org/.

efectividad ha quedado acreditada por la experiencia real. De esta forma, se busca maximizar el retorno de la inversión realizada para la implantación de medidas de seguridad.

Esta lista de medidas de seguridad tiene su origen en los trabajos realizados por la Agencia de Seguridad Nacional (National Security Agency, NSA) de los Estados Unidos a partir del año 2000. Actualmente se encarga de su revisión y mantenimiento un consorcio internacional denominado CCA (Consortium for Cybersecurity Action), en el que se integran más de 100 departamentos y agencias gubernamentales, organismos públicos y empresas privadas de Estados Unidos, Reino Unido y Australia. Entre sus miembros cabe señalar los siguientes:

- Estados Unidos:
  - DoD (Department of Defense).
  - DHS (Department of Homeland Security).
  - NSA (National Security Agency).
  - Mandiant.
  - Symantec.
- Reino Unido:
  - CPNI (Centre for the Protection of National Infrastructure).
- Australia:
  - Department of Innovation, Industry, Climate Change, Science, Research and Tertiary Education.

La relevancia de los *20 Controles críticos de seguridad* ha ido incrementándose de manera progresiva en los últimos años. A título de ejemplo, cabe mencionar que son el marco de referencia seleccionado por el CPNI del Reino Unido para la selección de las medidas técnicas de seguridad a implantar en el ámbito de la protección de las infraestructuras críticas.

Las principales características de los *20 Controles críticos de seguridad* son las siguientes (111):

- Enfoque práctico y realista. Desde sus inicios, la selección de las medidas de seguridad se basaba en su capacidad para hacer frente a ataques conocidos.
- Selección por consenso de expertos. Los miembros del CCA son especialistas con profundos conocimientos en sus respectivas áreas.
- Actualización permanente. El contenido de los *20 Controles críticos* es revisado periódicamente en el seno del CCA, lo que garantiza que las medidas de seguridad se adaptan a la naturaleza cambiante de las amenazas.
- Priorización. Uno de los elementos diferenciadores de los *20 Controles críticos* respecto a otros marcos de referencia es que establece

una clasificación priorizada de las medidas de seguridad, basada en la relevancia de cada medida de seguridad para la mitigación de ataques. Esta información es un apoyo fundamental para el responsable de la seguridad de la información a la hora de seleccionar qué medidas de seguridad deben implantarse en la organización, convirtiendo a los *20 Controles críticos* en una excelente herramienta de apoyo en la toma de decisiones en esta materia.

- Eficacia demostrada. El Departamento de Estado del Gobierno de los Estados Unidos implantó los *20 Controles críticos* y automatizó su seguimiento y monitorización, obteniéndose una reducción de más del 90% en el nivel de riesgo existente en la organización (112).
- Compatibilidad con otros marcos de referencia. *Los 20 Controles críticos* se ajustan a la perfección al conjunto de medidas de carácter técnico asociado a la existencia de un sistema de gestión de la seguridad de la información.
- Carácter técnico. Los *20 Controles críticos* se centran exclusivamente en las medidas de seguridad de carácter técnico; esta característica constituye, probablemente, la principal objeción que puede hacerse a los *20 Controles críticos*, ya que no incluyen en su alcance las medidas de seguridad de carácter organizativo y procedimental cuyo correcto diseño, implantación y monitorización tiene una relevancia tan importante –si no mayor– como la de las medidas técnicas.

La edición más reciente, correspondiente a la versión 4.1, apareció en marzo de 2013 (111). Los *20 Controles críticos* incluidos en esta versión son, en orden de importancia decreciente, los que se relacionan a continuación:

1. Inventario de dispositivos autorizados y no autorizados.
2. Inventario de *software* autorizado y no autorizado.
3. Configuración segura de *hardware* y *software* en dispositivos portátiles, estaciones de trabajo y servidores.
4. Evaluación y tratamiento continuos de las vulnerabilidades.
5. Protección contra el código malicioso.
6. Seguridad de las aplicaciones.
7. Control de dispositivos inalámbricos.
8. Capacidad para la recuperación de datos.
9. Evaluación de las capacidades relacionadas con la seguridad y formación apropiada.
10. Configuración segura de dispositivos de red: cortafuegos, *routers* y *switches.*

11. Limitación y control en el uso de puertos de red, protocolos y servicios.
12. Uso controlado de los privilegios de administración.
13. Defensa perimetral.
14. Mantenimiento, monitorización y análisis de ficheros de auditoría (*logs*).
15. Control de accesos basado en la necesidad de conocer.
16. Control y monitorización de cuentas.
17. Prevención de pérdida de datos.
18. Gestión de la respuesta a incidentes.
19. Ingeniería de red segura.
20. Pruebas de penetración y ejercicios *Red Team*.

La concienciación de *ciberseguridad* en las empresas

Programas de formación y concienciación

Llegados a este punto, y sabiendo que el factor humano es siempre el eslabón más débil de la cadena de la seguridad, toca abordar cómo las empresas pueden difundir a lo largo de toda su organización los conceptos de *ciberseguridad* analizados en los apartados anteriores para asegurarse de que los diferentes miembros de la misma disponen del conocimiento adecuado, según su rol y responsabilidad, para asegurar una adecuada conciencia de la situación de la empresa en el ciberespacio que permita a esta garantizar su éxito en este nuevo medio.

Para ello, se debe analizar cómo se puede implantar un programa de concienciación de *ciberseguridad* como herramienta mediante la cual difundir el conocimiento sobre los riesgos para la *ciberseguridad* y las posibles contramedidas para paliarlos para así asegurar la consecución de los objetivos de concienciación citados anteriormente.

Según el NIST (113), existen diferentes niveles de aprendizaje a la hora de aplicarlos a los diferentes miembros de la empresa según los roles y responsabilidades en *ciberseguridad* que desempeñan dentro de ella, que son:

– Concienciación: es un proceso de aprendizaje destinado a todos los miembros de la empresa y se enfoca en cambiar las actitudes individuales y colectivas para comprender la importancia de la seguridad y las consecuencias adversas de su fracaso.

  Trata de responder a la pregunta ¿qué? Su objetivo es que la audiencia objetivo reconozca y retenga la información que se le proporciona.

Ejemplos de canales para proporcionar este aprendizaje son los folletos, posters, vídeos, comunicados por *email, banners,* etc. Se busca alcanzar un impacto en un corto espacio de tiempo.

– Formación: es un proceso que se centra en enseñar al personal de la empresa los conocimientos y habilidades que les permitan realizar su trabajo con mayor eficacia.

  Trata de responder a la pregunta ¿cómo? Su objetivo es que la audiencia conozca y domine las habilidades necesarias para desempeñar adecuadamente un rol determinado. Ejemplos de canales para proporcionar este aprendizaje son los cursos, las prácticas, las demostraciones, los talleres, etc. Se busca alcanzar un impacto temporal a medio plazo.

– Educación: es el proceso de formación en *ciberseguridad* más avanzado y se centra en el desarrollo de la capacidad y la visión para llevar a cabo actividades complejas y multidisciplinares, así como las habilidades necesarias para promover el desarrollo profesional en *ciberseguridad*.

  Trata de responder a la pregunta ¿por qué? Su objetivo es que la audiencia desarrolle un entendimiento profundo y sea capaz de gestionar el conocimiento en la materia. Las actividades para proporcionar este tipo de aprendizaje incluyen la investigación y desarrollo, los seminarios y grupos de trabajo, los cursos monográficos avanzados, etc. Se busca alcanzar un impacto temporal a largo plazo.

Las acciones de concienciación deben centrarse en las funciones de trabajo específicas, o roles y responsabilidades de *ciberseguridad*, que desempeñan los individuos, no en los títulos de sus puestos de trabajo. De hecho, una persona puede tener más de una función[72] en la empresa y, por tanto, necesitará capacitación en *ciberseguridad* para poder cumplir con las responsabilidades específicas de cada rol que desempeñe.

Como ya hemos visto, todo el mundo necesita una formación básica en los conceptos y procedimientos de *ciberseguridad,* pues actualmente todos somos como mínimo usuarios de los servicios del ciberespacio. Por encima de este nivel básico, en función de los roles y responsabilidades desempeñadas, se pueden establecer diferentes niveles de capacitación de *ciberseguridad*, como por ejemplo: principiantes, intermedios o avanzados.

Además, dado que los individuos pueden realizar más de una función dentro de la organización, pueden necesitar de un nivel intermedio o

[72] Por ejemplo, alguien puede ser «director de división», con ciertas responsabilidades específicas de seguridad cibernética de su área de actividad, pero, al mismo tiempo, será «usuario» de los servicios TIC de la empresa, como cualquier otro de sus empleados.

avanzado de capacitación en *ciberseguridad* en su puesto de trabajo principal, pero solo el nivel de principiante en un rol secundario o terciario.

Por tanto, cada empresa debe analizar cuidadosamente las audiencias objetivo de las acciones de concienciación de *ciberseguridad* que va a realizar para asegurarse de que se cubren todas sus necesidades. Según el NIST (114), además de la concienciación básica que precisamos todos (como usuarios genéricos del ciberespacio), como mínimo deben analizarse los siguientes grupos de roles para determinar sus necesidades específicas de formación en *ciberseguridad*:

- Dirección ejecutiva: los líderes de la empresa deben conocer plenamente la legislación y la normativa sobre *ciberseguridad* que es de obligado cumplimiento para su organización. Además, también necesitan comprender su papel de liderazgo en ciberseguridad para asegurar el pleno cumplimiento de las responsabilidades de sus subordinados dentro de sus unidades.
- Personal de seguridad: incluye a los directores de los programas de *ciberseguridad* (CISO[73]). Son personas que actúan como consultores expertos en la organización y, por lo tanto, deben tener un profundo conocimiento de la política, los procedimientos y las mejores prácticas de *ciberseguridad*.
- Responsables funcionales de los sistemas de información: deben tener un conocimiento amplio de la política de seguridad y un alto grado de comprensión de los requisitos de ciberseguridad aplicables, según el tipo de información que manejen, así como de los controles de seguridad con los que satisfacer dichos requisitos en los sistemas de información de su responsabilidad.
- Administradores de sistemas y soporte TI: es el personal responsable de realizar las operaciones de apoyo críticas para una adecuada implantación y funcionamiento de las medidas técnicas de *ciberseguridad*. Estas personas deben tener un muy alto grado de conocimiento técnico en los controles de *ciberseguridad*, así como en su implementación y configuración práctica.
- Gerentes y usuarios de los sistemas de información: son personas que deben tener un alto grado de concienciación y formación en los controles técnicos de seguridad informática y en los procedimientos de uso de los sistemas que utilizan para realizar las actividades propias del negocio de la empresa.

Tal y como se ha visto, las empresas precisan desarrollar los correspondientes programas de formación y concienciación en seguridad cibernética que satisfagan las necesidades de los diferentes colectivos que las

[73] *Chief Information Security Officer.*

componen. Según ENISA[74], estos programas deben desarrollarse en tres fases (115):

– Fase 1: planificar, estimar y diseñar. Los programas de formación y concienciación deben ser diseñados teniendo siempre en cuenta la misión, visión y objetivos de cada empresa. Es muy importante que apoyen las necesidades de negocio y que influyan en la cultura de la empresa y, también, en las arquitecturas que soportan sus servicios TI. Los programas más exitosos son aquellos en los que los usuarios consideran que son relevantes para los problemas que se tratan de resolver. En esta etapa se identifican las necesidades de formación y concienciación, se diseña un plan eficaz que cubra dichas necesidades, se busca y se asegura la disponibilidad de los servicios de formación necesarios y se establecen las prioridades para llevarlas a cabo.

  En esta fase se deben llevar a cabo las siguientes actividades:

  - Establecer el equipo inicial del programa de concienciación.
  - Adoptar un enfoque de gestión del cambio que incluya una adecuada estrategia de comunicación.
  - Definir metas y objetivos.
  - Definir los grupos y audiencias objetivo.
  - Identificar al material de formación y el personal necesario para impartir el programa.
  - Evaluar las posibles soluciones, analizando la posibilidad de externalización o la impartición con medios propios.
  - Seleccionar la solución y el procedimiento de impartición, identificando los beneficios del programa.
  - Obtener el apoyo de la alta dirección y la financiación adecuada, por medio de una adecuada identificación de los costes que permita hacer un plan de negocio formal para validar y justificar la necesidad de las inversiones requeridas.
  - Elaborar el plan de trabajo, que debe incluir la lista de actividades, los hitos y el calendario, así como la distribución de los recursos y el presupuesto por cada actividad.
  - Desarrollar el programa y las listas de comprobación de las tareas.
  - Definir el concepto de comunicación, incluyendo el plan de comunicación y los canales para llevarlo a cabo.
  - Definir los indicadores para medir el éxito del programa, identificando los grupos de audiencia a los que se les va a aplicar los indicadores y definiendo las métricas a utilizar.
  - Establecer la línea base para la evaluación.
  - Documentar las lecciones aprendidas.

[74] European Network and Information Security Agency, o, en español, Agencia Europea de Seguridad de las Redes y de la Información. http://www.enisa.europa.eu/.

– Fase 2: desarrollar y gestionar. En esta fase se incluye cualquier actividad necesaria para implementar el programa de formación y concienciación sobre *ciberseguridad*. Las acciones del programa, que ejecuta la estrategia establecida para cubrir las necesidades de formación identificadas, solo se podrán gestionar y llevar a cabo una vez haya sido desarrollado el correspondiente material formativo.

  En esta fase se deben llevar a cabo las siguientes actividades:

  - Confirmar el equipo de trabajo del programa.
  - Revisar el plan de trabajo.
  - Iniciar la ejecución del programa.
  - Entregar las comunicaciones.
  - Documentar las lecciones aprendidas.

– Fase 3: evaluar y ajustar. Los mecanismos de evaluación y de retroalimentación son componentes críticos para cualquier programa de concienciación sobre la *ciberseguridad*. La mejora continua solo se puede alcanzar si podemos conocer cómo está funcionando el programa actual. Además, hay que tener en cuenta que los mecanismos de evaluación se deben diseñar para cubrir objetivos establecidos inicialmente para el programa. Una vez que se han alcanzado los requisitos iniciales básicos de concienciación, se puede diseñar y empezar a aplicar una estrategia de mejora continua.

  En esta fase se deben llevar a cabo las siguientes actividades:

  - Realizar evaluaciones que permitan medir el éxito del programa.
  - Recopilar los datos, de forma automática y/o manual que permita analizarlos y obtener una retroalimentación.
  - Incorporar la retroalimentación para futuros programas.
  - Revisar los objetivos del programa.
  - Poner en práctica las lecciones aprendidas.
  - Ajustar el programa según sea necesario.
  - Volver a iniciar el programa de concienciación.

Bibliografía

1. Organisation for Economic Cooperation and Development, «Shaping Policies for the Future of the Internet Economy». *OECD Ministerial Meeting on the Future of the Internet Economy,* Seúl, Corea: OECD, marzo de 2008.
2. *Estrategia de Seguridad Nacional: un proyecto compartido*. Presidencia del Gobierno, Gobierno de España, 2013.
3. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. The White House, 2011.

4. *Canada's Cyber Security Strategy. For a stronger and more prosperous Canada*. Government of Canada, 2010.
5. *Information Security Strategy for Protecting the Nation*. Information Security Policy Council of Japan, 2010.
6. *Cyber Security Strategy of the United Kingdom Safety, Security and Resilience in Cyber Space*. UK Office of Cyber Security, 2009.
7. *Cyber Security Strategy for Germany*. Federal Ministry of Interior, 2011.
8. *Information systems defence and security: France's strategy*. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 2011.
9. *The National Cyber Security Strategy (NCSS)*. Ministry of Security and Justice, 2011.
10. *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*. Cabinet Office, 2011.
11. *The Cost of Cyber Cryme.* United Kingdom: Detica y Office of Cyber Security and Information Assurance in the UK Cabinet Office, 2011.
12. QUEVEDO PUENTE, E. DE, FUENTE SABATÉ, J. M. DE LA y GARCÍA, J. B. D. «Reputación corporativa y creación de valor. Marco teórico de una relación circular». *Investigaciones europeas de dirección y economía de la empresa*, vol. 11, n.º 2, pp. 81-97, 2005.
13. CARROLL, A. B. y BUCHHOLTZ, A. K. *Business & Society: Ethics and Stakeholder Management*. Thomson/South-Western, 2003.
14. KENDRICK, J. W. «Total capital and economic growth», *Atlantic Economic Journal*, vol. 22, n.º 1, pp. 1-18, marzo de 1994.
15. KAPLAN, R. S. *Strategy maps: Converting Intangible Assets into Tangible Outcomes.* Harvard Business Press, 2004.
16. TORO, J. A. O. y PAVÍA, C. F. *Los índices de reputación corporativa y su aplicación en las empresas de comunicación,* presentado en III Congreso Asociación Española de Investigación de la Comunicación. Tarragona: 2012.
17. NEVADO PEÑA, D. *El capital intelectual: valoración y medición: modelos, informes, desarrollos y aplicaciones*. Madrid: Pearson Educación, 2002.
18. ARGENTI, P. y DRUCKENMILLER, B. «Reputation and the Corporate Brand», *SSRN Scholarly Paper ID 387860.* Rochester, NY: Social Science Research Network, marzo de 2003.
19. STEWART, T. A. *Intellectual Capital: The new wealth of organization*, 1.ª ed. Crown Business, 1998.
20. VILLAFAÑE, Justo. *La comunicación empresarial y la gestión de los intangibles en España y Latinoamérica: Informe anual 2005*. Ediciones Pirámide, 2005.

21. *Libro Verde: fomentar un marco europeo para la responsabilidad social de las empresas*. Comisión de las Comunidades Europeas, 2001.
22. E. El País, «243 muertos en el siniestro en una fábrica textil de Bangladesh», *El País*. E. El País, 25 de abril de 2013.
23. Agencia EFE. «Inditex y H&M respaldan acuerdo de seguridad en industria textil Bangladesh», *elEconomista.es*, 14 de mayo de 2013.
24. CAÑIBANO CALVO, Leandro y GISBERT CLEMENTE, Ana. *Los intangibles en las normas internacionales de información financiera.* 2005.
25. MELJEM ENRÍQUEZ DE RIVERA, Sylvia e IZTCHEL ALCALÁ CANTO, María. *Herramientas para la administración y valuación del capital intelectual.* Instituto Tecnológico Autónomo de México, Departamento Académico de Contabilidad, mayo de 2003.
26. SALINAS FABBRI, G. *Valoración de marcas: revisión de enfoques, metodologías y proveedores*. Barcelona: Ediciones Deusto, Instituto de Análisis de Intangibles, 2007.
27. COM (2006) 786 final: *Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas*. Comisión Europea, 2006.
28. *Directiva 2008/114/CE*. Consejo de la Unión Europea, 2008.
29. Ley 8/2011, de 28 de abril, *por la que se establecen medidas para la protección de las infraestructuras críticas*. Jefatura del Estado, 2011.
30. Real Decreto 704/2011, de 20 de mayo, *por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas*. Ministerio del Interior, 2011.
31. CARABÍAS, J. I. «Protección de las infraestructuras críticas», *Revista UNE de AENOR*, 06 de noviembre de 2010.
32. *El ministro del Interior, Jorge Fernández Díaz, ha inaugurado las I Jornadas Técnicas de Protección de Sistemas de Control en Infraestructuras Críticas.* Ministerio del Interior, 11 de abril de 2012.
33. RINALDI, S. M., PEERENBOOM, J. P. y KELLY, T. K. «Identifying, understanding and analyzing critical infrastructure interdependencies», *IEEE Control Systems*, vol. 21, n.º 6, pp. 11-25, 2001.
34. Instituto Nacional de Tecnologías de la Comunicación (INTECO), *Guía para empresas: seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA).* Observatorio de la Seguridad de la Información, marzo de 2012.
35. CORNISH, Paul; LIVINGSTONE, David; CLEMENTE, Dave, y YORKE, Claire. *Cyber Security and the UK's Critical National Infrastructure.* London: Chatham House, The Royal Institute of International Affairs, septiembre de 2011.

36. KOPYLEC, J., D'AMICO, A. y GOODALL, J. «Visualizing Cascading Failures in Critical Cyber Infrastructures», *International Federation for Information Processing Digital Library*, vol. 253, n.º 1, agosto de 2010.
37. Instituto Nacional de tecnologías de la Comunicación (INTECO). *Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA).* Observatorio de la Seguridad de la Información, marzo de 2012.
38. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). *Alert (ICS-ALERT-11-343-01) Control System Internet Accessibility.* Department of Homeland Security (DHS), diciembre de 2011.
39. MACÍAS, Esther. «Los ciberataques a las empresas son imposibles de evitar», *TICbeat*. 14 de marzo de 2013.
40. CSIC. *Importancia de la propiedad industrial para la empresa*. Cámara de Comercio de Madrid, 2009.
41. Comisión de las Comunidades Europeas, *Propiedad intelectual: guía de buenas prácticas. 10 recomendaciones eficaces para integrar mejor la propiedad intelectual en su empresa.* Comisión de las Comunidades Europeas, 2003.
42. Morgan Franklin Consulting, BURNS, Jim y HELD, Bruce. «Intellectual Property Theft Briefing», presentado en ISACA's NACACS. *North America computer audit, control and security conference.* Orlando, Florida: 2012.
43. SAMUEL, A. W. *Hacktivism and the future of political participation,* Harvard University Cambridge, Massachusetts, 2004.
44. BENEDICTO SOLSONA, Miguel A. «EE. UU. ante el reto de los ciberataques», *Documento de opinión.* IEEE (Instituto Español de Estudios Estratégicos), abril de 2013.
45. *APT1: Exposing One of China's Cyber Espionage Units,* The Mandiant® Intelligence Center™, febrero de 2013.
46. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012.* Office of the Secretary of Defense, DoD, mayo de 2012.
47. Verizon RISK Team. *Data Breach Investigations Report (DBIR). Snapshot: Intellectual Property Theft.* Verizon, 2012.
48. Joint Task Force Transformation Initiative. *Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology.* NIST SP 800-53r4, abril de 2013.
49. ¿Qué es *la operación Aurora?* Latinoamérica: Laboratorio ESET, enero de 2010.
50. «Important information about Night Dragon», *McAfee Knowledge Base*. McAfee, marzo de 2013.

51. VILLAFAÑA, Miguel. «Atacan a RSA Security», *Hacking Mexico*, marzo de 2011.
52. CHABROW, Eric. «DHS Responds to RSA SecurID Breach», *Govinfo Security*. 18 de marzo de 2011.
53. CHABROW, Eric. «RSA Breach Costs Parent EMC $66.3 million», *Govinfo Security*. 1 de agosto de 2011.
54. PEPITONE, Julianne. «RSA offers to replace all SecurID tokens after hack attack», *CNN Money*. 8 de junio de 2011.
55. *Anatomy of an Attack,* RSA Fraud Action Research Labs, abril de 2011.
56. RICHMOND, S. «Millions of Internet users hit by massive Sony PlayStation data theft», *The Telegraph*, 26 de abril de 2011.
57. CONTRERAS, Manuel. «GeoHot hackea el sistema de PlayStation 3», *Gizmología*, 3 de enero de 2011.
58. «Anonymous publica toda la discografía de Sony», *La Vanguardia*. L. V. Ediciones, 23 de enero de 2012.
59. SEYBOLD, Patrick. «Press Release: Some PlayStation Network and Qriocity Services to be Available this Week», *PlayStation.Blog*, 30 de abril de 2011.
60. TAKAHASHI, Dean. «Chronology of the attack on Sony's PlayStation Network», *VentureBeat*, 4 de mayo de 2011.
61. LYTLE, Chris. «Possible PlayStation Network Attack Vectors», *Veracode Blog,* mayo de 2011.
62. WILLIAMS, Martyn. «PlayStation Network hack will cost Sony $170M», *Network World*. 23 de mayo de 2011.
63. JIMÉNEZ CANO, Rosa. «Una disputa entre empresas ralentiza Internet». *El País*, 28 de marzo de 2013.
64. RUBENKING, Neil J. «Understanding the SpamHaus DDoS Attack», *PC Magazine*, 29 de marzo de 2013.
65. «DNS Amplification Attacks», *Alert TA13-088A.* Department of Homeland Security's, United States Computer Emergency Readiness Team (US-CERT), marzo de 2013.
66. «Ataque informático lleva a DigiNotar a la quiebra», *Blog del Laboratorio ESET*. ESET Labs, 7 de octubre de 2011.
67. *Global risks 2012.* Colonia, Suiza: World Economic Forum, 2012.
68. «La crisis entre Estonia y Rusia llega a Internet», *El País*, 17 de mayo de 2007.
69. MCDONALD, Geoff; MURCHU, Liam O.; DOHERTY, Stephen, y CHIEN, Eric. *Stuxnet 0.5: The missing link,* Symantec, febrero de 2013.
70. SANGER, D. E. «Obama Ordered Wave of Cyber Attacks Against Iran», *The New York Times*, 1 de junio de 2012.

71. *NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology, junio de 2011.
72. REALS, Tucker. «Stuxnet Worm a U. S. Cyber-Attack on Iran Nukes?», *CBS News*, 24 de septiembre de 2010.
73. *Predicciones de amenazas para 2012,* McAfee Labs, diciembre de 2011.
74. *Informe de actualidad STIC CCN-CERT IS 05/13.* Centro Criptológico Nacional, CCN-CERT, abril de 2013.
75. VAQUERO, L. M.; RODERO-MERINO, L.; CÁCERES, J., y LINDNER, M. «A break in the clouds: towards a cloud definition», *ACM SIGCOMM Computer Communication Review*, vol. 39, n.º 1, pp. 50–55, diciembre de 2008.
76. DIKAIAKOS, M. D.; KATSAROS, D.; MEHRA, P.; PALLIS, G., y VAKALI, A. «Cloud Computing: Distributed Internet Computing for IT and Scientific Research», *IEEE Internet Computing*, vol. 13, n.º 5, pp. 10-13, 2009.
77. MELL, Peter y GRANCE, Timothy. *NIST SP 800-145, The NIST Definition of Cloud Computing*. SP800-145.pdf. National Institute of Standards and Technology, septiembre de 2011.
78. *Cloud computing: La tecnología como servicio.* Observatorio Regional de Sociedad de la Información en Castilla y León (ORSI), Junta de Castilla y León, diciembre de 2010.
79. SCHULLER, Sinclair. «Demystifying the Cloud: Where do SaaS, PaaS and Other Acronyms Fit In?», *SaaS Blogs*, 1 de diciembre de 2008.
80. MCFEDRIES, Paul. «The Cloud is the Computer», *IEEE Spectrum*, agosto de 2008.
81. *Top Threats to Cloud Computing V1.0.* Cloud Security Alliance, marzo de 2010.
82. *Big data: Impactos y beneficios*. Information Systems Audit and Control Association (ISACA), marzo de 2013.
83. KATSOV, Ilya. «NoSQL Data Modeling Techniques», *Highly Scalable Blog*, 1 de marzo de 2012.
84. JACS. «Las ventajas de NoSql», *Php México*, abril de 2012.
85. *Top Ten Big Data Security and Privacy Challenges.* Cloud Security Alliance, noviembre de 2012.
86. *Consumerization of IT: Top Risks and Opportunities.* European Network and Information Security Agency (ENISA), septiembre de 2012.
87. «The Executive's Guide to BYOD and the Consumerization of IT». *ZDNet* y *TechRepublic,* febrero de 2013.
88. *Consumerization of IT: Risk Mitigation Strategies.* European Network and Information Security Agency (ENISA), diciembre de 2012.

89. JOHNSON, Kevin. *SANS Mobility/BYOD Security Survey.* SANS Institute, marzo de 2012.
90. *Good Technology's 2nd Annual State of BYOD Report,* Good Technology, enero de 2013.
91. *Securing Mobile Devices Using COBIT 5 for Information Security*. Information Systems Audit and Control Association (ISACA), 2012.
92. ORANS, Lawrence. *Securing BYOD With Network Access Control, a Case Study.* SANS Institute, agosto 2012.
93. TURBAN, E., BOLLOJU, N. y LIANG, T. P. «Enterprise Social Networking: Opportunities, Adoption, and Risk Mitigation», *Journal of Organizational Computing and Electronic Commerce*, vol. 21, n.º 3, pp. 202-220, julio de 2011.
94. WEBBER, Alan, LI, Charlene y SZYMANSKI, Jaimy. *Guarding the Social Gates: The Imperative for Social Media Risk Management*. Altimeter Group, 2012.
95. BURSON-MARSTELLER. «The Global Social Media Check-up Insights from the Burson-Barsteller Evidence Based Communications Group», Burson-Marsteller, 2010.
96. STAVRAKANTONAKIS, Ioannis; GAGIU, Andreea-Elena; KASPER, Harriet; TOMA, Ioan, y THALHAMMER, Andreas. «An approach for evaluation of social media monitoring tools», en *1st International Workshop on Common Value Management CVM2012*, Heraklion, Greece, 2012.
97. ISACA, *Social media: Business Benefits and Security, Governance and Assurance Perspectives.* Information Systems Audit and Control Association, 2010.
98. REUTERS. «Un falso tweet sobre un ataque a la Casa Blanca provoca caídas momentáneas en la bolsa estadounidense», *RTVE.es*, 24 de abril de 2013.
99. *Common criteria for Information Technology Security Evaluation. Part 1: Introduction and general model.* Common Criteria Management Board, septiembre de 2012.
100. *Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components.* Common Criteria Management Board, septiembre de 2012.
101. *Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components.* Common Criteria Management Board, septiembre de 2012.
102. *Common Criteria for Information Technology Security Evaluation. Evaluation methodology.* Common Criteria Management Board, septiembre de 2012.

103. *ISO/IEC 15408-1:2009 - Information technology - Security techniques - Evaluation criteria for IT security. Part 1: Introduction and general model.* International Organization for Standardization (ISO/IEC), 2009.
104. *ISO/IEC 15408-2:2008 - Information technology - Security techniques - Evaluation criteria for IT security. Part 2: Security functional components.* International Organization for Standardization (ISO/IEC), 2008.
105. *ISO/IEC 15408-3:2008 - Information technology - Security techniques - Evaluation criteria for IT security. Part 3: Security assurance components.* International Organization for Standardization (ISO/IEC), 2008.
106. *ISO/IEC 18045:2008 - Information technology - Security techniques - Methodology for IT security evaluation.* International Organization for Standardization (ISO/IEC), 2008.
107. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*. CCRA Common Criteria Management Comitee, 2000.
108. *ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements.* International Organization for Standardization (ISO/IEC), 2005.
109. *ISO/IEC 27002:2005. Information Technology - Security Techniques - Code of practice for information security management.* International Organization for Standardization (ISO/IEC), 2005.
110. SANS, «*A Brief History of the 20 Critical Security Controls*», SANS Institute, 2013.
111. Consortium for Cybersecurity Action. *CSIS: 20 Critical Security Controls. Version 4.1.* SANS Institute, marzo de 2013.
112. HARDY, G. Mark. *Reducing Federal Systems Risk with the SANS 20 Critical Controls*. SANS Institute, abril de 2012.
113. WILSON, M.; DE ZAFRA, D. E.; PITCHER, S. I.; TRESSLER, J. D., e IPPOLITO, J. B. *NIST SP 800-16 - Information Technology Security Training Requirements: A Role and Performance Based Model.* National Institute of Standards and Technology, 1998.
114. WILSON, Mark y HASH, Joan. *NIST SP 800-50, Building an Information Technology Security Awareness and Training Program*. National Institute of Standards and Technology, octubre de 2003.
115. «The new users' guide: How to raise information security awareness», *Report/Study.* ENISA, noviembre de 2010.

Cooperación internacional en temas de *ciberseguridad*

Por Emilio Sánchez de Rojas Díaz

Capítulo quinto

Introducción

> *EE. UU. también debe hacerle frente a la amenaza real y creciente de los ciberataques. Sabemos que los piratas informáticos roban las identidades de personas y se infiltran en correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos y que nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones financieras y nuestros sistemas de control del tráfico aéreo. (Obama)*

«No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía. Es por eso que hoy, más temprano, firmé un nuevo decreto ejecutivo que fortalecerá nuestras defensas cibernéticas aumentando el intercambio de información y desarrollando normas que protejan nuestra seguridad nacional, nuestros empleos y nuestra privacidad. Ahora bien, el Congreso también debe actuar aprobando las leyes que otorguen a nuestro Gobierno una mayor capacidad para proteger nuestras redes y disuadir los ataques» (1).

Australia (2009), Austria (2012), Canadá (2010), República Checa (2011), Estonia (2008), la Unión Europea (2013), Finlandia (2013), Francia (2011), Alemania, (2011), India (2011), Japón (2010), Lituania (2011), Luxembur-

go (2011), Nueva Zelanda (2011), Noruega, Polonia (2008 y 2011), Rumanía (2011), la Federación Rusa (2000, 2011), Eslovaquia (2008), Sudáfrica (2012), Suiza (2012), Países Bajos (2012), Uganda (2011), Reino Unido (2011), EE. UU. (2011)..., todos ellos forman parte del número creciente de países que están promulgando sus estrategias nacionales de seguridad. España lo acaba de hacer (31 de mayo de 2013). Muchas de ellas recogen en mayor o menor medida la necesidad de cooperación internacional; por ejemplo, la Estrategia Nacional de *Ciberseguridad* de los Países Bajos (2012) recoge entre sus «principios básicos» la «cooperación internacional activa»:

> *El carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación internacional. Debemos aspirar a un campo de juego de nivel internacional. Muchas medidas solo pueden ser eficaces si se toman o son coordinadas a nivel internacional. Los Países Bajos apoyan y contribuyen activamente a los esfuerzos con la Agenda Digital de la UE para Europa y la Estrategia de Seguridad Interior; el desarrollo de la política de ciberdefensa de la OTAN como parte de su nueva visión estratégica; el Foro de Gobernanza de Internet, y otras asociaciones. Países Bajos defiende la amplia ratificación y aplicación del Convenio del Consejo de Europa sobre la ciberdelincuencia.*

Comienza la amenaza transfronteriza

Podría decirse que el primer *ciberataque* ocurrió en la Unión Soviética cuando en 1982 explotó un oleoducto transiberiano[1]. La explosión, registrada por satélites de EE. UU, fue calificada como «la explosión no nuclear e incendio más monumental jamás vistos desde el espacio» (2). Al parecer, la explosión fue causada por un *malware* informático implantado por la Agencia Central de Inteligencia en el *software* canadiense, previendo que el *software* sería obtenido ilegalmente por agentes soviéticos. La explosión ocurrió en la remota Siberia y no dio lugar a víctimas. El KGB, que pensaban que habían robado a los EE. UU. la tecnología de *software* más reciente, estaba avergonzado. Los hechos fueron ocultados y la URSS nunca acusó públicamente a EE. UU. de provocar el incidente (3).

Los ataques informáticos «blandos» contra los sistemas de EE. UU., como Internet, han crecido de manera exponencial en los últimos 25 años. Muchos de ellos intentaban obtener información confidencial o eran ataques de denegación de servicio, relativamente simples pero potencialmente devastadores. Entre los más dañinos se incluyen Moonlight Maze (1998-2001), que puso a prueba los sistemas informáticos gubernamentales y académicos de los EE. UU.; Code Red (2001), que introdujo un gusano

[1] Este hecho fue recogido por *The New York Times* en 2004 en el artículo «*The Farewell Dossier*» (Safire, 2004).

destinado a realizar un ataque de denegación de servicio contra los ordenadores de la Casa Blanca, y Mountain View (2001), una serie de intrusiones en los sistemas informáticos municipales de EE. UU. para recoger información sobre los servicios públicos, oficinas de gobierno y sistemas de emergencia. Aunque se especuló acerca de los orígenes, ninguno de estos incidentes pudo ser atribuido de forma incontestable a un actor estatal (3).

Hace unas semanas, el secretario de Estado de EE. UU. John Kerry criticaba los procedimientos de las elecciones presidenciales iraníes, de las que dijo no mostraban «ningún respeto por la voluntad popular». Describió las medidas del Gobierno iraní para frenar o cortar el acceso a Internet antes de la votación como «indicador de problemas» que privan a los iraníes de su capacidad de compartir información e intercambiar ideas.

Mientras Kerry estaba reprendiendo al régimen de Teherán, un agente de la CIA, Edward Snowden, estaba filtrando documentos al diario *The Guardian* que revelaban cómo la Agencia de Seguridad Nacional de EE. UU. (NSA) había estado espiando a la comunidad mundial de Internet desde 2007. Al participar en un programa secreto denominado PRISM, empresas estadounidenses como Google, Yahoo, Skype, Apple y Facebook, entre otras, dieron acceso directo a la NSA a sus sistemas, lo que permite la vigilancia de las comunicaciones en vivo y la información almacenada como historiales de búsqueda (4).

Dominios conectados globalmente

Los dominios conectados globalmente como el ciberespacio están siendo desafiados de forma creciente por actores tanto estatales como no estatales. Los actores no estatales como grupos terroristas, traficantes o la delincuencia internacional organizada están interesados en explotar estos dominios, mientras que ciertos países desarrollan actividades encaminadas a reducir la libertad de movimiento internacional.

La *ciberamenaza* se extiende y acrecienta por una falta de normativas internacionales, la dificultad a la hora de atribuir ataques, barreras de acceso débiles y una facilidad relativa para desarrollar capacidades de ataque potentes. Nuestra capacidad de operar en el ciberespacio dependerá de la colaboración entre agencias estatales, no gubernamentales, industria y actores internacionales en el desarrollo de nuevas capacidades, organizaciones y normas, de manera que seamos capaces de proporcionar un amplio abanico de posibilidades para asegurar nuestro propio acceso y uso del dominio del ciberespacio así como permitir la persecución de los actores maliciosos. Es necesario mejorar las capacidades de detección, disuasión, bloqueo de acceso y defensa en varias capas (5).

«Hay factores legales y tecnológicos que incrementan las posibilidades de que las *ciberamenazas* se materialicen», como recoge la Estrategia Española de Seguridad (2011):

> *Entre los primeros, la ausencia de una legislación común o de seguridad global que permita una lucha más efectiva contra ellas. Tecnológicamente, Internet fue creado para ser útil y sencillo, no para ser seguro. La creciente interconexión de la Red, incluyendo necesariamente las infraestructuras, suministros y servicios críticos, incrementa los niveles de riesgos sobre estos. El anonimato y la dificultad para rastrear los «ciberataques» son factores añadidos que entorpecen su neutralización (...). Los «ciberataques» más comunes tienen fines comerciales, pero también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, incluso de estados.*

«La evolución del ciberespacio es demasiado rápida para hacer predicciones, pero es poco probable que las cuestiones de *ciberseguridad* disminuyan con el creciente consumo de las tecnologías de la información y las comunicaciones (TIC) en todo el mundo»; esto es lo que afirma la OCDE en su informe sobre *Futuros shocks globales* (2011):

> *A menos que el ritmo de los avances en la ciencia forense cibernética alcance la creciente facilidad de despliegue y la sofisticación de los ciberataques deliberados, seguirá siendo extremadamente difícil para las víctimas conocer la identidad de un atacante –lo que se conoce como problema de la atribución–. Esto quiere decir que una doctrina de defensa basada en la disuasión es menos probable que tenga éxito, y que ciertas partes malignas que actualmente carecen de la capacidad para poner en marcha un ataque a gran escala con éxito en el futuro puedan hacerlo.*

Otro informe también publicado por la OCDE, *Reducción del riesgo sistémico en ciberseguridad,* afirma que la cooperación internacional es una de las claves para reducir los riesgos de *ciberseguridad*. Los ataques contra los sistemas conectados a la Internet pública pueden originarse en cualquier parte de esa red. Los fallos en las infraestructuras de información esenciales en una nación pueden transmitirse en cascada en los sistemas dependientes en cualquier parte, pero aunque muchos organismos internacionales han emitido declaraciones de principios de apoyo mutuo y protección, no existe un mecanismo sustantivo o gobernanza internacional para resolver crisis relacionadas con ataques informáticos distintas de la estructura FIRST/CERT dominada por ingenieros (6).

Las principales mejoras que se podrían hacer serían aumentar el número de estados que forman parte del Convenio sobre la Delincuencia Cibernética, y así fortalecer los mecanismos de cooperación

internacional y desarrollo de capacidades. Sería particularmente útil que países con un gran número de usuarios de Internet, como Rusia y China, ratifiquen la convención sobre *cibercrimen*. Pero esto puede requerir flexibilidad por parte de los estados que forman parte actualmente para responder a las preocupaciones sobre soberanía de Rusia y otros (6).

Recientemente, hemos tenido un ejemplo de ataque con transmisión en cascada. Internet es un conjunto de redes independientes conectadas entre sí. CloudFlare dirige una red, Google dirige una red y los proveedores de ancho de banda como Level3, AT&T, y Cogent operan redes. Estas redes se interconectan posteriormente a través de lo que se conoce como relaciones de interconexión. Desde allí, nos conectamos con los puntos de intercambio de Internet (IXP o IX), una infraestructura física a través de la cual los proveedores de servicios de Internet intercambian tráfico entre sus redes (sistemas autónomos).

La mayoría de las ciudades importantes tienen un IX, que son diferentes en cada parte del mundo. En Europa funcionan algunos de los más robustos, y CloudFlare se conecta a varios de ellos. Un altercado entre un grupo *antispam,* Spamhaus, y una empresa holandesa que hospeda sitios *web*, CyberBunker, comenzó cuando Spamhaus situó a la compañía holandesa una lista negra de *spammers*.

El ataque fue escalando en intensidad y nivel, pasando a atacar a CloudFlare, la proveedora de nivel 3 de Spamhaus, y posteriormente a los proveedores de ancho de banda de CloudFlare, proveedores de ancho de banda nivel 2, que a su vez compran ancho de banda de los proveedores nivel 1 (aproximadamente una docena en el mundo). Además de atacar a líneas directamente dependientes de CloudFlare, los atacantes también lo hicieron sobre las infraestructuras IX de London Internet Exchange (LINX), Amsterdam Internet Exchange (AMS-IX), Frankfurt Internet Exchange (DE-CIX) y Hong Kong Internet Exchange (HKIX), alcanzando sus mayores efectos sobre LINX (ver gráfico).

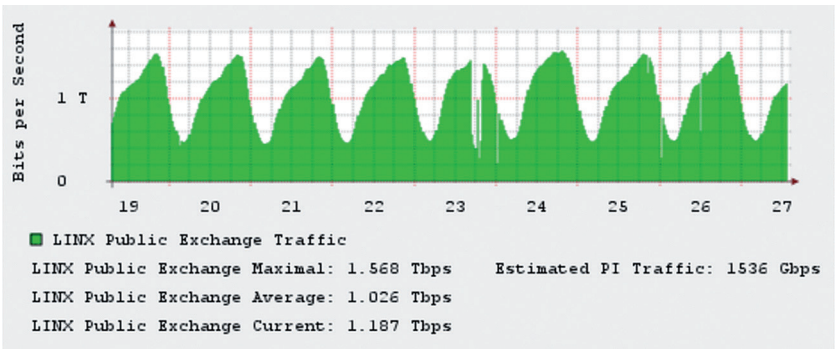


Figura 5.1. Impacto en el tráfico general (7).

Figura 5.2. Zona de concentración de ataques (7).

Para Matthew Prince, de CloudFlare, estos grandes ataques de nivel 3 son difíciles de detener. En pocas palabras: «Si tienes un *router* con un puerto de 10 Gbps y alguien te envía 11 Gbps de tráfico, no importa que dispongas de *software* inteligente para detener el ataque, porque tu enlace a la red está completamente saturado» (7).

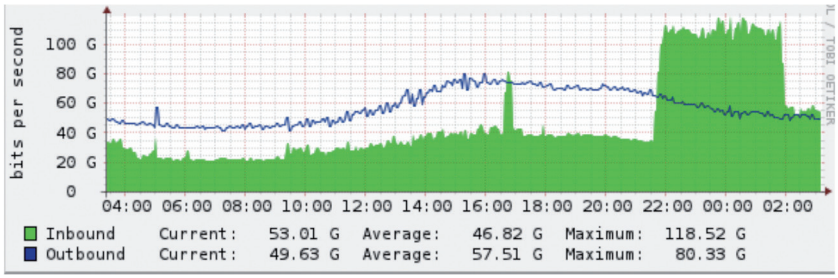


Figura 5.3. Impacto sobre el tráfico 2 (7).

Estos ataques han expuesto algunas vulnerabilidades en la arquitectura de algunos IX. Pero no dejará de impresionarnos cómo una riña entre empresas puede desencadenar el *ciberincidente* conocido de mayor intensidad, especialmente cuando este se ha atribuido a *hackers*.

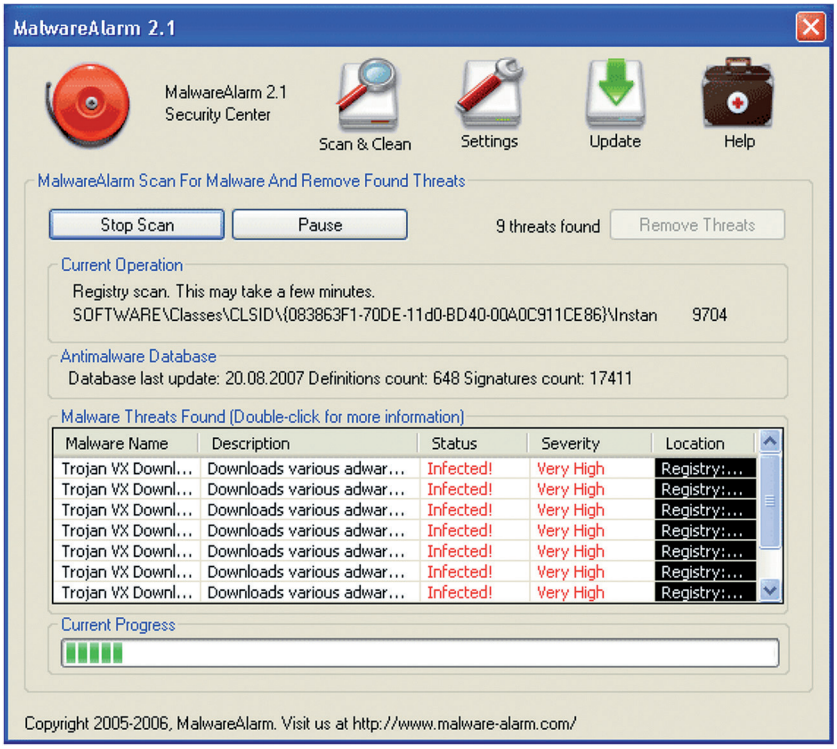


Figura 5.4. Pantalla que muestra los ataques (7).

Spamhaus

Fue un tipo de ataque *smurf* –«pitufos» en inglés– conocido como amplificación DNS. En los ataques *smurf*, enviando una pequeña cantidad de tráfico se consigue que llegue a la víctima mucho más tráfico. ¿Cómo protegerse de este ataque? Difícilmente, ya que el fallo está en equipos ajenos (y en el diseño inicial de Internet y el DNS, basados en gran parte en la buena fe) repartidos por todo el mundo que permiten ser usados como equipos *zombis* para un ataque. Además, los equipos *zombis* que se están usando no son una modesta *botnet* construida con equipos domésticos infectados y con una conexión ADSL: son miles de servidores con conexiones de alta capacidad (8).

El tratamiento de la «ciberdefensa» en las políticas de defensa

Uno de los elementos clave de la *ciberseguridad* es la defensa. El tratamiento de la *ciberdefensa* en las políticas de defensa puede variar de acuerdo con el «color político» de los Gobiernos. La dimensión *cíber* en las políticas de defensa puede depender de múltiples factores, como nos recuerda Daniel Ventre (9):

– El contexto internacional:

  • Los ataques contra Estonia se traducen en una fuerte conciencia de los desafíos para los estados que ha ido acompañada de la creación de instituciones dedicadas a la ciberdefensa (CCDCOE Tallinn).
  • La pertenencia a organizaciones internacionales (como la OTAN) impone directrices y medidas a los estados miembros.

– El contexto nacional e internacional:

  • Japón, país de alta tecnología, hiperconectado, cuya sociedad es probablemente una de las más «dependientes» del ciberespacio, tuvo que esperar hasta 2010 para desarrollar las políticas de *ciberdefensa*[2]. Es uno de los elementos que contribuyen a la reformulación de la política de defensa de Japón y supone una ruptura en cuestiones clave como un nuevo concepto de defensa dinámica para adaptar las fuerzas japonesas en el entorno geopolítico (aumento de las capacidades militares de China, la amenaza de Corea del Norte...).

– Los factores internos:

  • La crisis financiera en los países puede ser una razón para cuestionar los presupuestos destinados a la defensa. Bajo la presión de la opinión pública, se pueden reducir los presupuestos de defensa. Las *ciberamenazas* se pueden considerar como no prioritarias frente a otras contingencias inmediatas.
  • La imagen de la institución militar en la opinión pública puede influir también; una imagen positiva permitiría una mayor receptividad a la hora de obtener financiación.

Los principales actores nacionales

Aunque de hecho tengamos casi tantas aproximaciones como países a la *ciberseguridad*, podríamos definir tres cosmovisiones básicas; la *ciberliberal* defensiva, representada por la UE y compartida por casi todos los países europeos; la *ciberliberal* ofensiva, representada por los EE. UU., y la *cibernacionalista*-aislacionista, representada por China y Rusia. A ellas hay que añadir las que, como Irán o Corea del Norte, sin disponer de la sofisticación de las grandes potencias disponen de unas capacidades ofensivas que están dispuestas a emplear directa o indirectamente.

Rusia y China hicieron un gran esfuerzo para «capturar» el control de Internet en una reunión de la Unión Internacional de Telecomunicacio-

[2] Después de un cambio de Gobierno, cuando el Partido Democrático de Japón llegó al poder en 2009.

nes en diciembre de 2012 y con el objetivo de restringir el acceso a la información. Recibieron un sorprendente grado de apoyo. Muchos países están desencantados con el modelo ortodoxo de múltiples partes de la gobernanza de Internet, al que encuentran incapaz de satisfacer sus necesidades gubernamentales y de desarrollo, y se mueven en silencio hacia un modelo «no occidental» de la gobernanza de Internet. Los regímenes autoritarios se han percatado de esta insatisfacción y la intentan aprovechar para sus propios fines políticos. No ha habido casi ningún nuevo pensamiento en Occidente sobre la manera de ir más allá de la antigua ortodoxia de Internet; todo está diseñado para un momento en que el mundo todavía giraba en torno al Océano Atlántico (10).

El Gobierno de la India, junto con las organizaciones privadas, está poniendo en marcha varias iniciativas para combatir los *ciberataques*. Sin embargo, el mayor desafío que enfrenta actualmente el país es la falta de profesionales de la *ciberseguridad*. Según los últimos datos, la India tiene actualmente alrededor de 22.000 profesionales de la *ciberseguridad* certificados, número que es minúsculo en comparación con China, que tiene casi 25 millones de expertos en cibernética o comandos. Los expertos señalan que el país necesitaría 500.000 expertos de *ciberseguridad* en 2015 para proteger su infraestructura de TI. Como resultado, ellos creen que el país debe prepararse para crear un fuerte grupo de expertos de seguridad informática para fortalecer su espacio de *ciberseguridad* (11).

El Gobierno indio ha aprobado la propuesta de Política Nacional de Ciberseguridad, que está dirigida a la creación de un «entorno informático seguro y la confianza en las transacciones electrónicas adecuadas» (12). Entre las prioridades, figuran: «Acciones de mitigación proactivas, preventivas y reactivas para alcanzar y neutralizar las fuentes de problemas y el apoyo a la creación de un ecosistema global de seguridad, incluidos los acuerdos de colaboración público-privada; el intercambio de información; acuerdos bilaterales y multilaterales con los CERT en el extranjero, los organismos de seguridad y de los proveedores de seguridad...».

En el Reino Unido, no todos los *building blocks* para mover la arquitectura informática del Gobierno a una nube segura están todavía en su lugar. Durante la elaboración de la Estrategia Nacional de Seguridad, un desafío clave fue hacer que departamentos y empresas entendieran que la *ciberseguridad* debe ser entendida como vital para la prosperidad económica del Reino Unido y por ello requiere necesariamente la inversión de una amplia gama de actores. La orientación actual del Gobierno se basa en la seguridad perimétrica.

La seguridad perimetral tiene un defecto importante. Un informe del Centro para la Protección de la Infraestructura Nacional (CPNI) prevé que las mejoras en las medidas de seguridad perimetral solo serán graduales y

se verán emparejadas –si no superadas– por la evolución de los medios de ataque. Este es el riesgo común para la UE y gran parte de sus países, una estrategia de defensa perimetral –similar a la que se empleaba militarmente en el Medievo– pero que no solo es enormemente cara, sino que será –más pronto que tarde– penetrada por ataques en alguno de sus puntos vulnerables.

Posición respecto a la cooperación internacional

Alemania

Werner Hoyer, secretario de Estado del Ministerio Federal de Relaciones Exteriores de Alemania, en una conferencia internacional de alto nivel sobre *Desafíos en ciberseguridad, riesgos, estrategias y fomento de la confianza* que se celebró en Berlín en diciembre 2011, hizo hincapié en la importancia de garantizar la accesibilidad, la transparencia y la integridad de Internet a través de la cooperación internacional. Subrayó que el ciberespacio ha sido desde el principio una red global y abierta (13).

La atención se debería centrar –en opinión de Hoyer– en las áreas donde el consenso para cooperación internacional es más fuerte y pueda dar lugar a normas de conducta políticamente vinculantes. Transparencia y medidas de fomento de la confianza (como las de control de armas convencionales) pueden proporcionar una plataforma para el desarrollo de medidas específicas para el ciberespacio como un «código de conducta cibernética». Alemania está a favor de la creación de una obligación de los países para garantizar la seguridad en el ámbito cibernético, y que esta deba estar anclada en el derecho internacional humanitario (DIH).

Cornelia Rogall-Grothe, secretaria de Estado del Ministerio Federal del Interior de Alemania, opina que los estados tienen un interés vital en asegurar su capacidad de recuperación, la seguridad y la estabilidad por razones económicas, y de seguridad pública, por lo que tiene que proteger el ciberespacio en su propio territorio, pero además deben cooperar a nivel internacional para eliminar las vulnerabilidades en el ciberespacio. El primer paso sería acordar los principios y normas existentes e internacionalmente reconocidos que también podrían aplicarse al ámbito cibernético. Una vez acordados los principios generales, como la utilización con fines pacíficos y la obligación de asegurar la infraestructura crítica, se podría aplicar la cooperación entre estados en la atribución de *ciberataques*. Sin embargo, opina Rogall-Grothe, los estados deben ser responsables de la prevención de *ciberataques* procedentes de su territorio, de lo contrario deben esperar una respuesta razonable, como por ejemplo las sanciones (13). Este último aspecto es significativo puesto que introduce el concepto –disuasorio– de «respuesta razonable».

EE. UU.

Los Estados Unidos dan importancia a la construcción de un consenso internacional sobre normas de conducta en el ciberespacio. De acuerdo con la Estrategia Internacional para el Ciberespacio, elaborada por los Estados Unidos, los acuerdos y normas comunes deberían centrarse en los mundos físicos y cibernéticos por igual. Estos deben incluir las libertades fundamentales en línea y fuera de línea, los derechos de propiedad, la privacidad pública, la protección contra el delito cibernético, el derecho a la legítima defensa, la estabilidad técnica, el acceso fiable y la resistencia nacional (13). Aquí, los EE. UU. van más allá de Alemania e introducen el concepto de «legítima defensa», lo que le supondría el derecho a responder a un ataque digital con cualquier medio.

El Grupo de los Ocho (G8), la OSCE y la Organización para la Cooperación y el Desarrollo Económico (OCDE) son –en opinión de EE. UU.– los foros apropiados para articular estas normas. Según la visión de EE. UU., las medidas de fomento de la confianza de carácter militar deben basarse en los principios de proporcionalidad y distinción, mientras que otras medidas de fomento de la confianza deben tratar de prevenir la escalada. Se destacó la necesidad de un diálogo más global, que se inició en la conferencia de Londres en noviembre de 2011. Es destacable la falta de referencias a la ONU como foro por parte de los EE. UU. La posición de los EE. UU. será desarrollada posteriormente en profundidad.

Rusia

Al igual que otros grandes países, Rusia ha desarrollado capacidades para la guerra de información (IW) y las operaciones de información (IO). Dentro de la Administración rusa, varias organizaciones son responsables del empleo de las capacidades de guerra de información, incluyendo las operaciones de la red de ordenadores, guerra electrónica, operaciones psicológicas y campañas de desinformación (*maskirovka*). El Servicio Federal de Seguridad (FSB) es, probablemente, la autoridad responsable de la seguridad de la información de la Federación de Rusia.

El enfoque de Rusia sobre IW e IO difiere en cierta medida del de los países occidentales, así como desde el punto de vista chino. Desde el punto de vista ruso, la información en sí misma es un activo valioso que se tiene que proteger tanto en tiempos de paz como de guerra. En la doctrina de seguridad de la información de 2000, la protección de la información tiene un valor estratégico y es visto como un factor clave no solo para la estabilidad del Estado, sino también para el régimen y para los actores influyentes e importantes. En la doctrina militar publicada en la primavera de 2010, Rusia toma nota de la importancia de la guerra de la información durante la fase inicial de un conflicto para debilitar el mando

y control de la capacidad del oponente y en la forma de una campaña de información durante la batalla real para crear una visión positiva dentro de la comunidad internacional (14).

Rusia ha sido denunciada públicamente varias veces por no actuar con suficiente fuerza contra las actividades maliciosas en el ciberespacio originarias de ese país. Las acusaciones incluyen una amplia gama de comportamientos, como la criminalidad en Internet, *ciberespionaje* y *hacking* políticamente motivado (llamado *hacktivismo*). Los críticos señalan que los cuerpos de seguridad rusos han sido reacios a hacer frente a los infractores de la ley. Dos casos en particular han llegado a debate en los últimos años con respecto a las operaciones cibernéticas que podrían haber emanado de Rusia: los ataques cibernéticos contra Estonia en 2007 y contra Georgia en el año siguiente. Estos incidentes han supuesto una llamada de atención para poner de relieve los riesgos, amenazas y vulnerabilidades ante una guerra de información (14).

Rusia presentó en 2011 un proyecto de convención de las Naciones Unidas sobre información y seguridad internacionales, con propuestas de que cada Estado sea responsable de su propio espacio de información, incluyendo la seguridad de los datos; que pueda gestionar el ciberespacio en su territorio de acuerdo con las leyes nacionales y haga aplicar las libertades y derechos fundamentales de las personas y ciudadanos, así como que goce de igualdad soberana en el ámbito de la información, y que la seguridad de cada estado sea inseparable de la seguridad de la comunidad global. En junio de 2012, San Petersburgo acogió la tercera reunión internacional de representantes de alto nivel en asuntos de seguridad. Uno de los puntos principales debería haber sido una discusión del proyecto de convención de las Naciones Unidas ya que esta reunión habría sido la última antes de la presentación de la versión final de este documento para su examen por las Naciones Unidas (15).

La esencia del documento, vinculante en el plano internacional, incluye una serie de conceptos como la guerra de información, seguridad de la información, las armas de la información, el terrorismo en el ciberespacio, y otros, que han sido tratados únicamente en trabajos científicos y periodísticos, no en términos de derecho internacional. El proyecto ruso apoya claramente la preservación de la soberanía del Estado sobre su espacio de información, así como las disposiciones relativas a la «acción en el ciberespacio a fin de socavar el sistema político, económico y social de otro Estado, el tratamiento psicológico de la población, la desestabilización de la sociedad» (Fedorenko, 2012). Parece obvio que este último aspecto se refiere al empleo que los EE. UU. hicieron de estas herramientas en Serbia, Ucrania o Kirguistán y que posteriormente fueron imitados en las revueltas árabes de 2011.

En muchos aspectos, el proyecto de convención de la ONU de Rusia «para garantizar la seguridad internacional de la información» es un contrapeso a la Convención de Budapest, que Washington está tratando de imponer como la naturaleza «global» en materia de *ciberseguridad.* A Rusia no le gusta el artículo 32 de la Convención de Budapest, «El acceso transfronterizo», que permite a las agencias de inteligencia de algunos países penetrar en las redes informáticas de otros países para llevar a cabo operaciones allí sin el conocimiento de las autoridades nacionales. Durante mucho tiempo, la parte rusa trató de persuadir a los europeos en eliminar o editar la disposición que viola la soberanía del Estado, pero los países firmantes, con el apoyo de los EE. UU., se negaron rotundamente a realizar cambios en el documento (15). Rusia se niega a firmar el Convenio de Budapest.

Moscú considera que habría que hablar de la totalidad de las acciones relacionadas con posibles actos ilícitos (hostiles) relacionados con la utilización de tecnologías de la información y las comunicaciones (TIC), mientras que Washington insiste en que las negociaciones deben limitarse a las cuestiones de las *ciberamenazas*, lo que excluye las operaciones psicológicas de información, que en los últimos años han proliferado, en particular, a través de las redes sociales. Para los EE. UU., cualquier intento de abordar estos temas como cuestiones de *ciberseguridad* (o seguridad de la información) se considerará como un deseo de presionar a la «sociedad civil» y pone en peligro la «libertad de expresión» y «fortalece tendencias autoritarias» (15).

La interpretación estadounidense del problema está en desacuerdo no solo con Rusia, sino también con el aliado más fiable de Rusia en esta materia, la República Popular de China. Muchos apoyan el enfoque de acercamiento de Rusia, como los países de la CEI, Asia, África y América Latina. Y no todos los estados europeos están de acuerdo con las ideas contenidas en la Convención de Budapest: no es casualidad que solo dos tercios de los países miembros del Consejo de Europa hayan firmado o ratificado la Convención (15).

Francia

La política de seguridad francesa en el ciberespacio señala que las amenazas informáticas en Francia, desde hace muchos años, proceden tanto de actores estatales como no estatales y se ha progresado mucho al ser la seguridad un área prioritaria para el Gobierno francés. Con la aparición de la *ciberdiplomacia*, se ha convertido en global: han comenzado a surgir algunos elementos de consenso para la acción común, las alianzas internacionales y las relaciones bilaterales que están empeñadas en garantizar la seguridad y ayudar a combatir la Delincuencia informática. Destacan para Francia los esfuerzos concertados de la Unión Europea para luchar contra

la delincuencia informática, promover la solidaridad y la *ciberresiliencia* y establecer la política de cooperación con la OTAN (13).

La OSCE se centra en la confianza, en opinión de Francia, mientras que el Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG) 2012 se ha comprometido a la construcción de un consenso internacional. Es necesario un código de conducta para garantizar la libertad de expresión y la fiabilidad de Internet. La Declaración del G8 (Deauville, diciembre de 2011) acordó una serie de principios sobre cómo garantizar la actual fortaleza de Internet como un recurso para la sociedad global: la libertad, la gobernanza de múltiples partes interesadas, el respeto a la privacidad y la propiedad intelectual, la *ciberseguridad* y la protección contra los delitos informáticos.

China

La perspectiva del Gobierno chino sobre seguridad de la información es que a pesar de que la *ciberseguridad* está «de moda», muchos países no están preparados para defenderse contra *ciberataques*. Internet es una red de redes, y podría decirse que a nadie le interesa usar el ciberespacio como un campo de batalla, sino más bien mantenerlo como un espacio pacífico, seguro, equitativo y abierto a la información. Para lograr esto, los conceptos de seguridad común y el «orden favorable» en el ciberespacio y el espacio de la información tienen que desarrollarse en un clima de confianza y entendimiento mutuo (13).

El papel principal de los Gobiernos estatales sería el establecimiento de una cooperación «ganador-ganador» entre la comunidad internacional de estados, por lo que cada uno de ellos podría dotarse de información y de prosperidad cibernética. China no se ve a sí mismo como un «ciberpoder», sino más bien como uno de los mayores usuarios de las TIC que se enfrenta a graves desafíos en el ciberespacio. China –en sus propias palabras– está comprometida con el fortalecimiento de la información y la cibernética desde nuevos ángulos, adoptando un papel activo en la cooperación con el objetivo de alcanzar un consenso internacional así como el desarrollo de normas y reglas internacionales para el dominio cibernético (13).

En septiembre de 2011, se presentó en la Asamblea General de las Naciones Unidas (AGNU) una carta con el esbozo de una propuesta de código internacional de conducta para la seguridad de la información. Dicha carta tenía la intención de proporcionar una base para el proceso de búsqueda de respuestas internacionales a los problemas de seguridad en el ciberespacio y, por tanto, es una invitación para el debate internacional.

La guerra de la información en China, como en otras partes, es un tema amplio, que abarca muchas dimensiones de la actividad. Un debate fun-

damental es si la guerra de información china se aplica sobre todo en tiempos de paz, de guerra o en ambos casos. Para el profesor de West Point Edward Sobiesk, China está actualmente involucrada en una guerra de información en tiempos de paz de largo plazo que «no son combates» per se. Pero este argumento, al parecer, estaría en clara oposición con el énfasis en la acción anticipada y defensa activa que aparece en los textos oficiales chinos sobre defensa (16).

Todas las actividades cibernéticas no son iguales. Dependen del contexto y la cultura de la parte que las realiza. Para algunos, China estaría usando «paquetes de electrones» como estratagemas para llevar a cabo *ciberreconocimientos* o *ciberataques*, una estratagema diseñada para engañar a los procesos de percepción enemigos, su pensamiento, emociones y voluntad. En este caso, los paquetes de electrones podrían ser utilizados como en estratagemas clásicas chinas como «susurro de la hierba para asustar a la serpiente» (tirar miles de *pings* a un sitio determinado hasta que el *IGCC Workshop* informe sobre China, y entonces la *ciberseguridad* se evidenciará al ser estos detectados por los cortafuegos) (16).

China está probablemente influenciada por la táctica conocida como «coctel de guerras», un concepto desarrollado en el libro *Unrestricted warfare* de 1999. Uno de los autores del libro, Qiao Liang (coronel en ese momento), escribió que los nuevos conceptos de armas implican la posibilidad de combinar diferentes elementos para producir tipos de armamento nunca antes imaginados. Por ejemplo, Qiao puede estar refiriéndose a las combinaciones como «precepción cibernética + reconocimiento red + decepción de alta tecnología + desorganización del mercado financiero + disuasión de red» para obtener una nueva arma de efectos globales.

Para *Li Yuxiao*, director del Centro de Investigación de China sobre la Gobernanza de Internet, de la Universidad, Correos y Telecomunicaciones de Pekín, la seguridad del ciberespacio es un problema internacional común que tenemos resolver juntos; pero cada país tiene sus propios problemas de seguridad en Internet, y es injusto que un país mida a los demás de acuerdo a sus propias políticas. Debido a que el tema de la seguridad en el ciberespacio es muy sensible, la discusión no es lo suficientemente completa. Los Gobiernos no pueden llegar a un consenso en algunas cuestiones. A través de la cooperación académica, se podrían definir los principios y las normas básicas y establecer un mecanismo de funcionamiento. La cooperación podría incluir la seguridad informática, la privacidad y protección de datos de negocios (17).

Ubicado en la pintoresca comunidad Xianghongxi en las montañas occidentales del distrito de Haidian de Pekín, el Tercer Departamento del Estado Mayor General (GSD por sus siglas en inglés) del Ejército Popular de Liberación gestiona al parecer una amplia infraestructura de interceptación de comunicaciones orientada a las comunicaciones diplomáticas

extranjeras, actividades militares, entidades económicas o instituciones educativas públicas y particulares de interés. El Tercer Departamento del GSD puede servir como autoridad ejecutiva nacional para la explotación de la red informática (por ejemplo, los *ciberreconocimientos*). Esta hipótesis se basa en tres supuestos:

- La gradual integración técnica y de organización de la inteligencia de señales, seguridad de la información, y *ciberreconocimiento*.
- La competencia básica del Tercer Departamento sobre computación avanzada. La informática y la criptografía son fundamentales para las operaciones de la red de ordenadores (CON).
- El Tercer Departamento sirve como el mayor contratista de lingüistas bien entrenados para la traducción de información. El Tercer Departamento del GSD podrá estar apoyado por empresas comerciales y universidades.

La Estrategia Civil Nacional de Ciberseguridad de China, lanzada en 2003 e inicialmente clasificada pero luego promulgada más ampliamente, es conocida como *Documento 27. Opiniones de fortalecimiento de la información al servicio de garantía de seguridad.* La Constitución consagra el principio de «defensa activa» y establece los cimientos para las políticas para protección de infraestructuras críticas, la criptografía, control dinámico, desarrollo indígena, innovación, el talento, el liderazgo y la financiación. Las iniciativas políticas conjuntas emprendidas por el *Documento 27* han dado lugar a un sistema antagónico de espacios políticos vigorosamente defendidos por las diversas autoridades burocráticas. Cualquier incursión de otras agencias o de recién llegados ha provocado conflictos.

Unión Europea

Desde 2009, y en relación con los esfuerzos de la Unión Europea (UE), ha existido una plataforma de intercambio de información para los estados miembros. Ejercicios de *ciberseguridad* paneuropeos y Equipos de Respuesta a Emergencias Informáticas funcionales (CERT) se establecieron en todos los estados miembros de la UE en 2012 para proteger a Europa de ataques informáticos a gran escala. Se insistió en que la *ciberseguridad* «es una parte integral de la Política Exterior y de Seguridad Común de la Unión Europea (PESC de la UE) ya que tiene una dimensión política», así como la necesidad de defensa. Los próximos pasos del Servicio Europeo de Acción Exterior (SEAE) se centrarán en el desarrollo de normas y estándares para el ciberespacio, la promoción de la Convención de Budapest sobre la Ciberdelincuencia, la creación de capacidades en terceros países, el desarrollo de una estrategia europea para el ciberespacio y la organización de talleres conjuntos con la India, China y la OTAN (13).

Es obvio el cariz de escudo defensivo adoptado por la UE que pretende que otros (OTAN, o sus propios socios) realicen funciones que por su propio carácter global debían ineludiblemente ser realizados por la Unión.

El papel de las organizaciones internacionales

Dado el número de organizaciones internacionales, nos hemos centrado en las que de forma más directa afectan a Europa:

ONU

Antecedentes

A partir del año 2000 se han aprobado una serie de resoluciones de la Asamblea General de la ONU sobre la lucha contra el uso indebido e ilícito de las tecnologías de información. Por ejemplo, en el año 2000, una resolución puso de relieve la necesidad de contar con leyes nacionales modernas y eficaces para enjuiciar adecuadamente los delitos cibernéticos y facilitar la oportuna colaboración de investigación transnacional. En esa resolución, se destacó el valor de una variedad de medidas, que incluían (19):

- Que los estados deben garantizar con sus leyes y prácticas eliminar los «santuarios» para los que usan el ciberespacio con fines delictivos.
- Fomentar la cooperación policial en la investigación y el enjuiciamiento de los casos internacionales de utilización con fines delictivos.
- Que los estados deben intercambiar la información con respecto a los problemas que enfrentan en la lucha contra el uso indebido e ilícito de tecnologías de la información.
- Que los estados deben informar al público en general sobre la necesidad de prevenir y combatir el uso indebido e ilícito.
- Que, en la medida de lo posible, las tecnologías de la comunicación y la información deben estar diseñadas para ayudar a prevenir y detectar el uso indebido e ilícito, para rastrear criminales y reunir pruebas.
- Que la lucha contra el uso delictivo del ciberespacio requiere el desarrollo de soluciones que tengan en cuenta tanto la protección de las libertades individuales como la preservación de la capacidad de los estados para luchar contra el mal uso criminal.

En 2001, una resolución de la Asamblea General sobre la lucha contra los delitos de alta tecnología señaló específicamente la labor de las organizaciones internacionales y regionales. Esta resolución incluye una

referencia a la labor del Consejo de Europa en la elaboración de la Convención sobre el Delito Cibernético, así como la actividad de esas organizaciones en la promoción del diálogo entre el Gobierno y el sector privado en la seguridad y la confianza en el ciberespacio.

En 2003, los Estados reafirmaron la necesidad de crear una cultura de *ciberseguridad* y reconocieron su responsabilidad para llevar, a todos los elementos de la sociedad, a conocer sus funciones y responsabilidades en materia de *ciberseguridad*. Una resolución puso de relieve nueve elementos complementarios que todos los participantes deben abordar (19):

- Aumentar la conciencia de la necesidad de seguridad.
- Medidas que podrían tomar los estados para mejorar la *ciberseguridad*.
- Responsabilidad de la seguridad de las tecnologías de la información y comunicación.
- Capacidad de respuesta para actuar de manera oportuna para prevenir, detectar y responder a incidentes de seguridad.
- Ética en el reconocimiento de que nuestras acciones u omisiones en el ciberespacio pueden dañar a otros.
- Democracia, en el sentido de que la seguridad debe aplicarse de manera coherente con las sociedades democráticas.
- Una gran variedad de medidas de evaluaciones de riesgos, diseño e implementación de seguridad.
- Gestión de la seguridad.
- Recalificación del significando y de los enfoques actuales de las políticas de seguridad basado en el cambio de las amenazas y las vulnerabilidades de este medio de cambio rápido de las comunicaciones.

En 2004 aparece la cuestión de la protección de infraestructuras críticas en una resolución de la Asamblea General de Naciones Unidas (AGNU) que se centró sobre todo en los comportamientos y las acciones que los estados miembros deben tener en cuenta en sus esfuerzos para crear una cultura de *ciberseguridad* y protección de infraestructuras críticas de información. Estos también pueden considerarse un conjunto de acuerdos comunes a los que los Gobiernos se deben adscribir, proporcionando una base esencial para facilitar la comprensión internacional y la colaboración internacional en materia de gestión de riesgos. Entre otras cosas, esta resolución abordó (19):

- La necesidad de redes de alerta de emergencia para las *cibervulnerabilidades*.

- Sensibilización para facilitar la comprensión de las partes interesadas de la naturaleza y la extensión de las infraestructuras de información esenciales.
- El examen de las infraestructuras e identificar la interdependencia entre ellas.
- Promover las asociaciones, tanto públicas como privadas, para compartir y analizar las vulnerabilidades críticas de infraestructura de información y responder a los daños o ataques.
- Creación y mantenimiento de las redes de comunicación de crisis.
- Asegurar que las políticas de disponibilidad de datos tienen en cuenta la necesidad de proteger las infraestructuras críticas de información.
- Y una serie de compromisos en materia de cooperación internacional para asegurar esas infraestructuras, incluida la facilitación del seguimiento de ataques, formación y ejercicios de conducción. Además, tendrán que disponer de leyes procesales sustantivas y adecuadas y personal capacitado para investigar los ataques y procesar a los atacantes.

Otros acuerdos internacionales comunes afectan a cómo los Estados persiguen los objetivos de *ciberseguridad*. El derecho a la libre circulación de la información, por ejemplo, está bien establecido a nivel internacional y está consagrado en la Declaración de la ONU de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. Algunos de estos principios se han reafirmado en numerosos foros internacionales, incluyendo la Asamblea General de la ONU, la Unión Internacional de Telecomunicaciones y la Cumbre Mundial sobre la Sociedad de la Información, entre otros.

La Convención Internacional para la Represión de la Financiación del Terrorismo, de la que son parte 169 Estados, ya criminalizó la obtención o provisión de fondos para apoyar actos terroristas. Algunas resoluciones, como la Resolución 1822 (2008), hacen un llamamiento a la cooperación y al intercambio de información relacionada con fines delictivos terroristas, en particular a través de Internet.

La seguridad de la información en la ONU

La cuestión de la seguridad de la información ha estado en la agenda de la ONU desde que la Federación de Rusia en 1998 introdujo por primera vez un proyecto de resolución en la Primera Comisión de la Asamblea General de la ONU. Esta resolución fue aprobada sin votación (A/RES/53/70) y continuó hasta una proposición más detallada, aunque los contenidos eran conflictivos y probablemente inaplicables.

Estos proyectos de resolución se convirtieron en un ejercicio anual de frustración: la iniciativa rusa fue durante muchos años rechazada por algunos países occidentales, pero todavía tiene el mérito indudable de mantener vivo el argumento de que era necesario un esfuerzo normativo importante.

La resolución 66/24, en su apartado 3, invita a todos los Estados miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, sigan comunicando al secretario general sus opiniones y observaciones sobre:

- La evaluación general de los problemas de la seguridad de la información.
- Las medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera.
- El contenido de los conceptos mencionados en el párrafo 2 de la resolución.
- Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

El secretario general, en virtud del párrafo 4 de la resolución 60/45, creó un Grupo de Expertos Gubernamentales sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional. El grupo remitió, en julio de 2010 (A/65/201), las siguientes recomendaciones a la asamblea general:

> *18. Teniendo en cuenta las amenazas existentes y potenciales, riesgos y vulnerabilidades en materia de seguridad de la información, el Grupo de Expertos Gubernamentales considera oportuno recomendar nuevas medidas para el desarrollo de la confianza y otras medidas para reducir el riesgo de error de percepción resultante de las interrupciones TIC:*
>
> *(i) un mayor diálogo entre los estados para discutir las normas relativas al estado de uso de las TIC, para reducir el riesgo colectivo y proteger la infraestructura crítica nacional e internacional;*
>
> *(ii) medidas de fomento de la confianza, la estabilidad y la reducción del riesgo para hacer frente a las implicaciones del uso de las TIC del Estado, incluidos los intercambios de puntos de vista nacionales sobre el uso de las TIC en los conflictos;*
>
> *(iii) el intercambio de información sobre legislación y estrategias nacionales sobre tecnologías de la información y comunicaciones y tecnologías de seguridad, políticas y mejores prácticas;*

(iv) la identificación de medidas de apoyo a la creación de capacidad en los países menos desarrollados;

(v) búsqueda de posibilidades para la elaboración de terminología y definiciones comunes relacionados con la resolución 64/25.

Debido a la naturaleza global del ciberespacio y la utilización más activa de las tecnologías de la información y las comunicaciones (TIC), este problema es de carácter universal y transnacional y afecta a los países, la sociedad y los individuos. El problema de la seguridad de la información no se resolverá por los esfuerzos de un solo estado o grupo de estados o sobre una base regional. La solución de este problema requiere un esfuerzo conjunto de la comunidad internacional en su conjunto.

1. Debido a su carácter universal, las Naciones Unidas deben desempeñar el papel principal en las actividades intergubernamentales para el funcionamiento y la protección del ciberespacio para que no se abuse o sea explotado por los delincuentes, terroristas y estados con fines agresivos. En particular, deberá:

   a. responder a una necesidad esencial y urgente de una ley de consenso amplio del ciberespacio,
   b. avanzar en la armonización de las leyes nacionales contra el *cibercrimen*, y
   c. establecer procedimientos para la cooperación internacional y la asistencia mutua.

2. Hay que trabajar con este fin. La ONU debería reconocer la labor ya realizada por las partes negociadoras en el Consejo de Europa sobre la Ciberdelincuencia (CoE Convención). El Convenio del Consejo de Europa señala a una mayor fuerza si todas las partes que participaron en el proceso de negociación firmasen el Convenio, si aún no lo han hecho, para acelerar los procesos de ratificación y la transformación. Inmediatamente después de la entrada en vigor del Convenio, los firmantes deben adoptar medidas para designar y notificar a su autoridad para el manejo de la asistencia mutua y para participar en la red 24/7, y tomar otras medidas para promover la cooperación internacional en la derrota de delitos informáticos, como el Convenio del Consejo de Europa prevé.

Hamadoun Touré, director de Comunicaciones de la Agencia de la Tecnología de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT), dijo que el mundo necesita un tratado para evitar convertir los *ciberataques* en una guerra sin cuartel. Touré hizo esta declaración en enero de 2010, en el Foro Económico Mundial en Suiza, donde los expertos afirmaron que las naciones ahora debían tener en cuenta cuándo un *ciberataque* pasaba a ser una declaración de guerra. Touré ha añadido así una voz autorizada de la ONU en la búsqueda de un marco normativo.

Pero por muy atractiva que sea la idea de una convención amplia sobre ciberespacio –comparable a la Convención de las Naciones Unidas sobre el Derecho del Mar de 1982–, los obstáculos a dicho instrumento y su creación fueron reconocidos cada vez más como abrumadores. El ciberespacio puede ser aún más complejo que el mundo oceánico, pues las tecnologías digitales y sus usos están aún evolucionando a un ritmo rápido (20).

A pesar del sorprendente apoyo que recibieron China y Rusia en la reunión de la Unión Internacional de Telecomunicaciones en diciembre de 2012 con el modelo «no occidental» de la gobernanza de Internet (10), la negociación del tratado sería un proceso largo, y los procedimientos nacionales de ratificación no procederían en una escala de tiempo, aunque se esté mínimamente de acuerdo con la urgencia de llenar el vacío legal y exista la percepción creciente y compartida entre los Gobiernos de que la amenaza de *ciberconflictos y ciberdaños* se está haciendo inmanejable y puede acabar fuera de control. Los compromisos vinculantes para evitar ataques o actos de hostilidad y las sanciones correspondientes serían entonces inviables. Importantes problemas de definición serían probablemente irresolubles en el texto del tratado. Así, mientras que un tratado universal o ley sobre el ciberespacio sigue siendo un objetivo preferente, un concepto objetivo, razones prácticas requieren un enfoque alternativo (20).

OTAN

> *La OTAN seguirá siendo alianza multilateral preeminente para nuestra nación y seguirá impulsando nuestras relaciones de defensa con Europa. La Fuerza Conjunta seguirá cooperando para combatir el extremismo violento, centrándose en nuestra misión en Afganistán y apoyar a Pakistán. También vamos a apoyar el nuevo concepto estratégico como el espacio y la seguridad del ciberespacio…*
>
> Estrategia Nacional Militar de los EE. UU. de América de 2011

En abril y mayo de 2007, el traslado de un memorial de la guerra de la era soviética desató una serie de grandes y sostenidos ataques distribuidos de denegación de servicio (DDoS) que inundaron redes o sitios *web* con un tráfico de ataques que las hicieron inaccesibles. Los ataques –muchos de los cuales procedían de Rusia o eran escritos en ruso o coordinados en sitios *web* rusos– deshabilitaron los sitios *web* del presidente de Estonia, el Parlamento y los ministerios junto con los sitios *web* de los partidos políticos, los bancos y agencias de noticias. En fases de intensidad variable, los ataques se prolongaron durante más de tres semanas (21).

No se encontraron evidencias que vincularan directamente estos ataques con el gobierno ruso, pero los mismos fueron al menos ignorados y pro-

bablemente alentados por Moscú. Estos ataques supusieron un punto de inflexión en la política de la OTAN sobre *ciberseguridad*.

El crecimiento explosivo de «la banda» durante la década de 1990 coincide con la primera intervención militar importante de la OTAN. Así como la guerra de Vietnam fue la primera televisada del mundo, Kosovo fue la primera guerra de Internet en amplia escala. Cuando los aviones de la OTAN comenzaron a bombardear Serbia, numerosos grupos de *hackers* proserbios (o antioccidentales) como la Mano Negra –tomando prestado su nombre de la sociedad secreta paneslava que ayudó a comenzar la Primera Guerra Mundial– comenzaron a atacar la infraestructura de Internet de la OTAN. Se desconoce si alguno de los *hackers* trabajó directamente para el Ejército yugoslavo; en cualquier caso, su objetivo declarado era interrumpir las operaciones militares de la OTAN (22).

Los ordenadores de la OTAN, EE. UU. y Reino Unido fueron atacados durante toda la guerra por medio de «ataques de denegación de servicio» e infectados con virus por correo electrónico (fueron detectadas 25 diferentes cepas de virus). El ataque a la sede de la OTAN en Bélgica fue una victoria de relaciones públicas y propaganda para los piratas informáticos (22).

En 2002, la cumbre de Praga decide afrontar la defensa de la organización contra ataques informáticos, estableciendo la NATO Computer Incident Response Capability (NCIRC). Pero es en 2006, en la de Riga, cuando el mensaje se hace más evidente; en la declaración final, apartado 24, se lee: «La adaptación de nuestras fuerzas debe continuar. Hemos aprobado una serie de iniciativas para aumentar la capacidad de nuestras fuerzas para hacer frente a las amenazas y desafíos contemporáneos».

> *Trabajar para desarrollar una NATO Network Enabled Capability para compartir información, datos e inteligencia de forma fiable, segura y sin demora en las operaciones de la Alianza, al tiempo que mejora la protección de nuestros sistemas de información clave contra ciberataques.*

La cumbre de 2008 en Bucarest da un paso más en el párrafo 47 de la declaración:

> *47. La OTAN mantiene su compromiso de fortalecer los sistemas clave de información de la Alianza contra ciberataques. Recientemente hemos adoptado una Política de Defensa Informática, y se están desarrollando las estructuras y autoridades para llevarlo a cabo. Nuestra Política de Ciberdefensa hace hincapié en la necesidad de que la OTAN y las naciones, para proteger los sistemas de información clave de acuerdo con sus respectivas responsabilidades, compartan sus mejores prácticas y pongan a disposición sus capacidades, previa solicitud, para ayudar a las naciones aliadas a contrarrestar un ataque informático.*

En la cumbre de Lisboa, en noviembre de 2010, se acordó en el párrafo 2: «... de conformidad con las disposiciones de aplicación de la presente Declaración, hemos también (...) acordado mejorar nuestras capacidades de *ciberdefensa».* Y en el apartado 40:

> *Con el fin de garantizar el acceso permanente y sin restricciones de la OTAN al ciberespacio y la integridad de sus sistemas críticos, (...) se tendrá en cuenta en la doctrina de la OTAN la dimensión cibernética de los conflictos modernos y mejorará sus capacidades para detectar, evaluar, prevenir, defender y recuperar en caso de un ciberataque contra los sistemas de importancia crítica para la Alianza. Nos esforzaremos en particular para acelerar el NATO Computer Incident Response Capability, hasta alcanzar la capacidad operativa plena (FOC) en 2012 y la disposición bajo la protección cibercentralizada de todos los organismos de la OTAN.*

Además, indica que:

> *Vamos a utilizar los procesos de planificación de la defensa de la OTAN con el fin de promover el desarrollo de cibercapacidades de defensa, para ayudar a los aliados tras su solicitud y para optimizar el intercambio de información, la colaboración y la interoperabilidad.*

Por último:

> *Para hacer frente a los riesgos de seguridad que emanan desde el ciberespacio, trabajaremos en estrecha colaboración con otros actores, tales como la ONU y la UE, según lo acordado. Hemos encomendado al Consejo que elabore, basándose sobre todo en las estructuras internacionales y sobre la base de nuestra política actual, una revisión en profundidad de la política de la OTAN en ciberdefensa para junio de 2011 y que prepare un plan de acción para su implementación.*

Un primer borrador del concepto de *ciberdefensa* de la OTAN fue elaborado por los ministros de Defensa en marzo de 2011, lo que constituyó la base conceptual de la versión revisada de la Política sobre Defensa Cibernética de la OTAN. La citada política fue desarrollada y aprobada por los ministros de Defensa el 8 de junio. El documento va acompañado de un plan de acción, lo que representa un documento detallado con las tareas y actividades específicas para las estructuras propias de la OTAN y las fuerzas aliadas de defensa. Los principales elementos del nuevo enfoque son (21):

- Asunción de que la *ciberdefensa* es necesaria para realizar las tareas básicas de la OTAN de defensa colectiva y la gestión de crisis.
- La prevención, la resistencia y la defensa de los activos críticos para la *ciberseguridad* de la OTAN y sus aliados constituyentes.
- La aplicación de capacidades de *ciberdefensa* sólidas y la protección centralizada de redes propias de la OTAN.

- Definición de los requisitos mínimos para la *ciberdefensa* de las redes nacionales críticas para las tareas centrales de la OTAN.
- Asistencia a los aliados para alcanzar un nivel mínimo de *ciberdefensa* que reduzca la vulnerabilidad de la infraestructura crítica nacional.
- Compromiso con los socios, otras organizaciones internacionales, el sector privado y el académico.

Para poner en práctica estas nuevas políticas y capacidades, el principal órgano de gobierno de la OTAN para *ciberdefensa*, el Consejo de Dirección para Ciberdefensa (CDMB), ha firmado memorandos de entendimiento con la autoridad correspondiente de cada país miembro.

La declaración de la cumbre de 2012 en Chicago reafirma –en su artículo 49– los compromisos de *ciberdefensa* de la Cumbre de Lisboa, y, después de Lisboa, el año pasado (2011) se adoptó un concepto, una política y un plan de acción en *ciberdefensa* que ya se están aplicando.

Para hacer frente a las amenazas a la *ciberseguridad* y mejorar nuestra seguridad común,

> *...nos comprometemos a colaborar con los países socios pertinentes sobre una base de caso por caso y con las organizaciones internacionales, en particular la Unión Europea, según lo acordado, el Consejo de Europa, las Naciones Unidas y la OSCE, con el fin de aumentar la cooperación concreta.*

El futuro cibernético de la OTAN pasa por la *ciberdisuasión* de la Alianza. A pesar de que la *ciberdisuasión* es un tema muy discutido, es previsible que la OTAN siga el liderazgo del Departamento de Defensa de los EE. UU. y se centre en la disuasión por denegación. La defensa antes de un ataque, y las respuestas tras él, deben ser lo suficientemente eficaces para que los potenciales adversarios sepan que no pueden alcanzar los efectos deseados. Una fuerte defensa y las medidas de respuesta de la actual política de *ciberdefensa* de la OTAN pueden, en caso de aplicarse, ser un fuerte elemento de disuasión al denegar el beneficio de atacar en el primer lugar, para disuadir a los potenciales adversarios. La Alianza también puede lograr la disuasión castigando de varias maneras (21):

1. Cualquier nación que decida realizar un ataque importante incluso contra un aliado pequeño, como Estonia, ahora sabe que los líderes políticos de la OTAN tienen una forma bien definida para poder escalar la situación, como invocar el artículo 4 o el artículo 5 para una defensa colectiva.
2. Tanto la Casa Blanca como el Pentágono han sido sumamente claros en que los compromisos de la Alianza se extienden a los ataques informáticos importantes.

3. Aunque la OTAN no tiene una capacidad *ciberofensiva*, varias naciones aliadas disponen de las mismas, que podrían utilizarse en respuesta a un ataque importante.

Ni la disuasión ni el castigo garantizan que no habrá ataques futuros, pero las herramientas de las que disponen actualmente los Gobiernos aliados son muy diferentes de las que disponía Estonia cuando fue atacada en 2007. Al menos en la OTAN. Es interesante recordar las organizaciones con las que la OTAN se compromete a colaborar: Unión Europea, el Consejo de Europa, las Naciones Unidas y la OSCE, por este orden; igualmente, es importante recordar que es la OTAN la única organización internacional en la que confía plenamente EE. UU., la principal superpotencia en el ciberespacio.

Consejo de Europa

El Consejo de Europa (CoE) ha estudiado la *ciberseguridad* sobre todo desde el ángulo de la *ciberdelincuencia*. En 2001, el Consejo de Europa presentó la Convención sobre la Ciberdelincuencia –instrumento destinado a apoyar una política penal común encaminada a la protección de la sociedad contra la *ciberdelincuencia*–.

El Departamento de Justicia de EE. UU. ha sido un jugador clave en el desarrollo del acuerdo final.

Según Froomkin (2004), es creencia general que fue impulsada por EE.UU –que la habría redactado– a través del Consejo para obtener acceso a las comunicaciones extranjeras y sobre todo para dar la impresión al Congreso de que *Carnivore* –un *software* para monitorizar correo electrónico y de comunicaciones electrónicas empleado por el FBI– debe ser visto como ordinario, y algo exigido por sus aliados.

Estas afirmaciones son en alguna medida confirmadas por el Informe para el Congreso de Kristin Archick (23):

> *Tanto la Administración Clinton como la de Bush trabajaron en estrecha colaboración con el Consejo de Europa sobre la Convención. Funcionarios estadounidenses creen que «elimina o minimiza los numerosos obstáculos procesales y jurisdiccionales que pueden retrasar o poner en peligro las investigaciones internacionales y el enjuiciamiento de los delitos informáticos» (...). Políticos de EE. UU. afirman que la Convención no exigirá legislación para su aplicación, EE. UU. cumplirá con el Convenio, basado en la existente ley federal de los EE. UU. Los analistas legales dicen que los negociadores estadounidenses habían logrado separar las disposiciones más comprometidas, como por ejemplo el artículo de la incitación al odio, garantizando así que el Convenio se ajusta a las actuales leyes estadounidenses.*

La Convención contra la *Ciberdelincuencia* es referida a menudo como clave para la solución de los asuntos de *ciberseguridad.* Sus artículos 2-13 abordan el sustancial derecho penal que obliga a los estados a que tipifiquen los delitos informáticos. La Convención enumera los delitos contra la confidencialidad, integridad y disponibilidad de ordenadores, datos y sistemas, la falsificación y el fraude informático y delitos relacionados con el contenido así como la propiedad intelectual y la violación de la intimidad. Los artículos 14-22 abordan la ley procesal, incluyendo la evidencia electrónica, los poderes y los procedimientos apropiados para las investigaciones. Comprende, entre otros, el sistema de búsqueda y captura, la recogida de datos del tráfico en tiempo real, la interceptación de los contenidos de los datos y la preservación y rápida divulgación de los datos informáticos almacenados relacionados con el tráfico. Los artículos 23-35 están dedicados a la cooperación internacional (24).

Lo cierto es que la aplicación de la Convención no es uniforme y a menudo no se corresponde con las amenazas emergentes contra la seguridad nacional. Por otro lado, como afirman Schjølberg y Ghernaouti-Hélie (25), «la Convención se basa en las conductas delictivas de finales de 1990 y que no cubren técnicas como el *phishing*, *botnets*, *spam*, o *ciberterrorismo* y la terminología de la Convención es la terminología de los 90, no necesariamente adecuada para la década de 2010».

OSCE

La mayor organización de seguridad del mundo ha estado activa en la *ciberseguridad*, principalmente desde la perspectiva del *ciberterrorismo.* La Unidad de Acción contra el Terrorismo coordinó y facilitó desde 2002 los programas pertinentes de la OSCE para la lucha contra el terrorismo. En 2010, en un taller de la OSCE sobre un enfoque global para mejorar la *ciberseguridad,* los delegados coincidieron en que la función de la OSCE en la *ciberseguridad* mundial necesita ser redefinida:

> *Preocupados por la complejidad de las actividades maliciosas en línea, la OSCE ha decidido intensificar la acción mediante la mejora de la cooperación internacional en la lucha contra el uso de Internet con fines terroristas, para considerar la adopción de todas las medidas apropiadas para proteger las infraestructuras críticas y redes de información vitales contra la amenaza de ciberataques, al considerar ser parte e implementar sus obligaciones en virtud de los instrumentos internacionales y regionales existentes, y para explorar la posibilidad de una participación más activa de las instituciones de la sociedad civil y el sector privado en la prevención y lucha contra el uso de Internet con fines terroristas (26).*

Así es recogido en el informe del secretario general de la OSCE:

> *Desde 2009, la OSCE ha promovido un enfoque más amplio de la ciberseguridad. Este enfoque se basa en el entendimiento de que el uso generalizado de Internet por los terroristas, traficantes y delincuentes hace cada vez más difícil el desarrollo de respuestas eficaces a las amenazas transnacionales sin promover un ciberespacio más seguro. Un enfoque integral de la ciberseguridad debe: (a) fortalecer la seguridad nacional; (b) hacer frente a los ciberdelitos; (c) inhibir la utilización de Internet por terroristas; (d) responder a una amplia variedad de riesgos y amenazas, incluyendo peligros político-militares; (e) permitir a las autoridades competentes la protección de una amplia gama de objetivos que van desde el usuario particular de Internet a las infraestructuras críticas, y (f) salvaguardar Internet como un espacio de libre expresión y de reunión*[3].

El citado informe recoge que:

> *Muchos estados participantes han expresado su apoyo a un enfoque más amplio de la ciberseguridad, tal como se refleja en la FSC. DEC/10/08, en la que los estados participantes decidieron organizar un taller OSCE sobre un enfoque integral de la OSCE para mejorar la ciberseguridad (17 a 18 marzo, 2009, Viena) con la participación de las organizaciones internacionales pertinentes.*

La decisión del Foro de Cooperación en Materia de Seguridad incluye el objetivo del taller:

- Aumento de la conciencia de los estados participantes de la OSCE sobre las medidas concretas que se pueden tomar para fortalecer la *ciberseguridad*.
- Intercambio de información sobre las prácticas nacionales en materia de ciberseguridad entre los estados participantes de la OSCE y las organizaciones y actores internacionales pertinentes.
- Exposición de medidas defensivas potenciales, lecciones aprendidas y mejores prácticas pertinentes.
- Focalización en el posible papel de la OSCE en un enfoque integral para mejorar la *ciberseguridad*, y la identificación de medidas concretas para posibles acciones de seguimiento por todos los organismos pertinentes de la OSCE.

El taller de la OSCE de marzo de 2009 no solo proporcionó una mayor conciencia de las posibles medidas para fortalecer integralmente la *ciberseguridad*; también dio lugar a recomendaciones y sugerencias sobre el futuro papel de la OSCE en este ámbito temático (FSC.DEL/92/09) que siguen siendo objeto de examen por los países participantes.

[3] Report by the OSCE Secretary General on the Implementation of MC.DEC/2/09.

Un cable de la embajada de los EE.UU ante la OSCE indica que:

> *…una de las actividades recomendadas de seguimiento al taller de marzo observó que un «primer paso» esencial para el desarrollo de la ciberresiliencia era un autoestudio que identifique las políticas, las prácticas, las carencias y las capacidades dentro de las infraestructuras nacionales de información. Esta recomendación fue hecha por un experto panelista de EE. UU. y recibió un amplio apoyo. Como resultado, los expertos en ciberseguridad interagencias de Washington han desarrollado un autoestudio y evaluación para los estados participantes de la OSCE. Este documento se basa en una encuesta preparada para –pero nunca utilizado por– la Unión Internacional de Telecomunicaciones (UIT) de Naciones Unidas (27).*
>
> *Cada país debe determinar sus necesidades de ciberseguridad y tomar medidas para proteger sus infraestructuras críticas de información. Este autoestudio está destinado a ayudar a esta introspección para los miembros de la OSCE.*

Entre las preguntas, se tratarían temas como el desarrollo de una Estrategia Nacional de Ciberseguridad, la implementación de la citada estrategia nacional, colaboración Gobierno-industria o la promoción de una cultura nacional de seguridad informática. En una segunda parte, se incluirían descripciones y explicaciones sobre las preguntas de la primera parte, pero también recomendaciones para el desarrollo y la implementación de un programa de *ciberseguridad* nacional para la capa de política y de gestión, y se ocuparía de las políticas, el marco institucional y las relaciones de la *ciberseguridad*. Esta herramienta supondría un modelo marco con el que una nación podría comparar sus propios esfuerzos.

El ámbito geográfico de los 56 estados miembros de la OSCE cuenta con niveles extremadamente altos de penetración de Internet y, aún más importante, muy altos niveles de dependencia del Gobierno en infraestructura cibernética y de los sistemas SCADA (es decir, la energía, el agua y otras infraestructuras críticas que están vinculados a las tecnologías de la información y la comunicación que estamos debatiendo hoy), lo que significa –en opinión de EE. UU.– que la OSCE podría tener un interés particularmente fuerte en la discusión de medidas para aumentar la estabilidad a lo largo de estas líneas. Este foro ofrece un concepto integral de la seguridad y un espacio para el debate maduro en el que plantear estas cuestiones, creemos.

Finalmente, los EE. UU. presentaron un documento de reflexión e invitaron a la panelista Dra. Deborah Schneider a que interviniera ante una sesión conjunta del Consejo Permanente (CP) y del Foro de Cooperación en Materia de Seguridad (FCS). El documento de reflexión presentado en marzo de 2010 muestra el pensamiento de EE. UU. en cuestiones tales como:

– ¿Cómo podemos extender el entendimiento común entre los estados al ámbito cibernético para ayudar a garantizar la paz y la estabilidad internacionales?

– ¿Qué principios existentes del derecho internacional se aplican en el ciberespacio?

– ¿Cómo podemos aumentar la previsibilidad del comportamiento del Estado en el ciberespacio?

En relación con el segundo punto, indico que las delegaciones en el Grupo de Expertos Gubernamentales han estudiado la idea de mejorar la previsibilidad y la regularización de las nociones de comportamiento del Estado. Ese grupo, incluyendo los EE. UU., ha llegado a la conclusión de que los principios del *ius ad bellum* y *el ius in bello* aplican en el ciberespacio. El ciberespacio no está exento de ninguna manera; creemos que los principios básicos se aplican y proporcionan una base sólida para las discusiones sobre las expectativas acerca de la conducta de los estados en el ciberespacio. En concreto, EE.UU opina (Schneider, 2010):

– Con respecto al ius ad bellum, que algunos incidentes cibernéticos pueden elevarse al nivel de un uso de la fuerza.

– Con respecto a la ius in bello, que el derecho de los conflictos armados se aplica generalmente en el ciberespacio.

No obstante, EE. UU. continúa el estudio de los atributos únicos de la información y las comunicaciones, lo que presenta desafíos en la manera de aplicar estos principios. Creemos que esta es una vía útil y fructífera de exploración para el diálogo en el marco de la OSCE.

Este comienzo prometedor en la Organización para la Seguridad y la Cooperación en Europa (OSCE) para lograr un acuerdo sobre las medidas de fomento de la confianza cibernética fracasó cuando Rusia –como era de esperar– se apartó de los anteriores acuerdos. Esto puede haber sido una reacción a la aprobación del Congreso de EE. UU. de una resolución sobre derechos humanos en Rusia, pero también hay una división entre los países sobre cómo abordar el tema de Internet y la *ciberseguridad* basada en las actitudes hacia la democracia, los derechos humanos y el desarrollo económico. Es probable que haya pocos avances en la cooperación internacional en materia de *ciberseguridad* si la oposición rusa permanece firme, lo que puede obligar a EE. UU. a adoptar un nuevo enfoque que se dirija primero hacia un acuerdo con naciones «afines» (10).

Caso de análisis: la Unión Europea

La UE añadió a finales de los 90 el *cibercrimen* a los temas de interés. En abril de 1998, la Comisión presentó al Consejo los resultados de un

estudio sobre los delitos informáticos (estudio de la denominada *Comcrime*). En octubre de 1999, la Cumbre del Consejo Europeo de Tampere llegó a la conclusión de que el examen de delincuencia de alta tecnología debía ser incluido en los esfuerzos para acordar definiciones comunes y sanciones (24).

La decisión marco del Consejo de 2005 relativa a los ataques contra la información *Systems158* es un hito de la actividad de la UE en la lucha contra la *ciberdelincuencia*. Trata de mejorar la cooperación entre el poder judicial y otras autoridades competentes. El documento subraya la importancia de la aproximación de los sistemas de derecho penal y el aumento de la cooperación entre las autoridades judiciales en relación con el acceso ilegal a sistemas de información, la injerencia ilegal en el sistema y la interferencia ilegal en los datos(28). En 2010, se presentó una propuesta de directiva relativa a los ataques contra los sistemas de información, que derogaría la Decisión Marco 2005/222/JAI del Consejo. Por el momento, cuenta con la oposición del Reino Unido.

En opinión de la UE, para que el ciberespacio se mantenga abierto y libre, las mismas normas, principios y valores que defiende la Unión Europea fuera de línea también deberían aplicarse en línea. Los derechos fundamentales, la democracia y el Estado de derecho deben ser protegidos en el ciberespacio. Nuestra libertad y prosperidad dependen cada vez más de una Internet robusta e innovadora, que seguirá floreciendo si la innovación del sector privado y la sociedad civil impulsan su crecimiento.

En febrero de 2013 la Unión Europea (UE) ha aprobado el documento *Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, seguro y protegido.* Como puede apreciarse, deja bien sentada su prioridad: ciberespacio *abierto y libre;* pero cualquiera que esté familiarizado con las negociaciones en el marco de la UE sabe que la sustancia viene después del *but…:*

> *Pero la libertad en línea requiere también protección y seguridad. El ciberespacio debe ser protegido de los incidentes, las actividades maliciosas y mal uso; y los Gobiernos tienen un papel importante para garantizar un ciberespacio libre y seguro.*

Y reserva las tareas más importantes para los Gobiernos:

> *Los Gobiernos tienen varias tareas: para salvaguardar el acceso y apertura, de respeto y protección de los derechos fundamentales en línea y para mantener la fiabilidad y la interoperabilidad de Internet. Sin embargo, el sector privado posee y opera una parte significativa del ciberespacio, por lo que cualquier iniciativa que pretenda tener éxito en este área tiene que reconocer su papel de liderazgo (29).*

Es importante la lectura de este documento porque nuestro país comparte con sus socios de la UE una misma *cosmovisión*, que algunos califican

de posmodernista y que nos diferencia de otras potencias globales, incluso de los EE. UU.

Como nos recordaba Robert Kagan (30), es hora de dejar de pensar en que europeos y americanos comparten una misma visión del mundo:

> *En todos los asuntos importantes relacionados con el poder –la eficacia del poder, la moralidad del poder, la atracción del poder– las perspectivas europeas y americanas divergen. Europa se está moviendo más allá del poder a un mundo autocontenido de las leyes y las normas y la negociación transaccional y la cooperación. Está entrando en un paraíso posthistórico de paz y prosperidad relativa, la realización de la «paz perpetua» de Emmanuel Kant.*

Mientras tanto, los EE. UU. permanecen sumidos en la historia, ejerciendo su poder en un anárquico mundo *hobbesiano*:

> *Donde las leyes y regulaciones internacionales no son fiables y donde la auténtica seguridad y defensa y la promoción de un orden liberal aún depende de la posesión y empleo del poder militar.*

Es por ello que, en las principales cuestiones internacionales de hoy en día, los estadounidenses vienen de Marte y los europeos de Venus: están de acuerdo en poco y se entienden entre ellos cada vez menos, afirma Kagan.

Hay que reconocer que el prestigioso escritor publicó estos párrafos en 2003, y que la aproximación del actual presidente Barak Obama es «cosméticamente» diferente a la de su antecesor George W. Bush y, aun con diferentes cosmovisiones, actualmente es más lo que compartimos que lo que nos separa. Pero, como nos recuerda Noam Chomsky en una entrevista con Eric Bailey:

> *Las políticas de Obama han sido aproximadamente las mismas de Bush, aunque ha habido algunas pequeñas diferencias, pero eso no es una gran sorpresa. Los demócratas apoyaron las políticas de Bush. Hubo algunas objeciones, en su mayoría por razones partidistas, pero en su mayor parte, apoyaron sus políticas y no es sorprendente que no hayan dejado de hacerlo. En algunos aspectos, Obama ha ido más allá que Bush…*

En cuanto a los asesinatos, a pesar de que la campaña fue iniciada por Bush, Obama ha aumentado considerablemente la citada campaña global de asesinatos y se han incluido en la lista a ciudadanos estadounidenses. ¿Se aplica el *proceso legal establecido*? Eric Holder, fiscal general del Departamento de Justicia con Obama, explicó que «sí se había aplicado el proceso legal establecido ya que se discutió previamente en el Ejecutivo». El Gobierno norteamericano ha dejado muy claro que los asesinatos cuentan con la aprobación de Obama (31). En definitiva, EE. UU. y la UE son como Marte y Venus.

La UE se reserva el papel de salvaguarda de los derechos y libertades, mientras deja para los estados miembros los temas de seguridad:

> *La UE debe salvaguardar un entorno en línea que ofrece la mayor libertad posible y la seguridad para el beneficio de todos. Si bien reconoce que es predominantemente la tarea de los estados miembros para hacer frente a los desafíos de seguridad en el ciberespacio, esta estrategia propone acciones específicas que pueden mejorar el rendimiento global de la UE (29 pág. 4).*

Esto nos debería dejar perplejos, dado que si el espacio es parte de los *global commons*, parece que la UE debería llevar la voz cantante y no solo en los asuntos de derechos y libertades, sino también en estos asuntos de seguridad global. La UE propone en esta estrategia una visión articulada en cinco prioridades estratégicas:

- Lograr *ciberresiliencia*.
- Reducir drásticamente la *ciberdelincuencia*.
- El desarrollo de la política de *ciberseguridad* y las capacidades relacionadas con la Política Común de Seguridad y Defensa (PCSD).
- Desarrollar los recursos industriales y tecnológicos para la *ciberseguridad*.
- Establecer una política internacional coherente para la Unión Europea en el ciberespacio y promover valores esenciales de la UE.

Es destacable la *ambigüedad constructiva* del tercer apartado –es el más largo, pero no dice nada– y la omisión expresa de la palabra «intereses» en el último apartado: la UE promueve valores, pero deja la defensa de los intereses a los países. Una aproximación muy lejana de la visión posthistórica; Europa sigue siendo básicamente *westfaliana* por dejación.

Las actividades de la alta representante en relación con el apartado 3 se centrarán, entre otras labores «insustanciales», en promover el diálogo y la coordinación entre los actores civiles y militares de la UE y asegurar el diálogo con los socios internacionales, incluida la OTAN, otras organizaciones internacionales y los centros multinacionales de excelencia, para garantizar las capacidades efectivas de defensa, identificar áreas para la cooperación y evitar la duplicación de esfuerzos. Es decir, promover, coordinar y dialogar (en resumen, nada de utilidad).

Sin embargo, es en el punto 5 donde la UE puede ser más proactiva y eficaz: «Preservar el ciberespacio abierto, libre y seguro es un desafío global que la UE debe abordar junto con los interlocutores pertinentes y organizaciones internacionales, el sector privado y la sociedad civil». La Comisión, la alta representante y los estados miembros deberían articular una política internacional coherente de la UE en el ciberespacio, que se dirigirá a una mayor participación y fortalecimiento de las relaciones con los principales socios internacionales y las organizaciones, así como con la sociedad civil y el sector privado (29 pág. 15).

Las consultas de la UE con los socios internacionales sobre cuestiones cibernéticas deben ser diseñadas, coordinadas e implementadas para obtener valor añadido a los actuales diálogos bilaterales entre los estados miembros de la UE y terceros países:

> *La UE pondrá un énfasis renovado en el diálogo con terceros países, con especial atención a socios afines que comparten los valores de la UE. Se promoverá lograr un alto nivel de protección de datos, incluyendo la transferencia de datos personales a terceros países. Para hacer frente a los desafíos mundiales en el ciberespacio, la UE promoverá una cooperación más estrecha con organizaciones que trabajan en este campo, tales como el Consejo de Europa, la OCDE, la ONU, la OSCE, la OTAN, la Unión Africana, la ASEAN y la OEA.*

Particulariza la cooperación con los EE. UU. –socio afín que comparten los valores de la UE– a nivel bilateral, que se seguirá desarrollando, especialmente en el contexto del Grupo de Trabajo UE-EE. UU. sobre *ciberseguridad* y *ciberdelincuencia* (29).

Considera que «la responsabilidad de un ciberespacio más seguro depende de todos los actores de la sociedad mundial de la información desde los ciudadanos a los Gobiernos».

De acuerdo con el texto, uno de los elementos más importantes de la política internacional de la UE en este campo será la promoción de la libertad y los derechos fundamentales el ciberespacio, y recuerda que las obligaciones legales consagradas en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta Europea de Derechos Fundamentales deben ser respetados también en línea.

La Unión Europea no exige la creación de nuevos instrumentos legales internacionales para asuntos cibernéticos, y considera que:

- Para hacer frente a los delitos informáticos, la Convención de Budapest es un instrumento abierto a la aprobación de terceros países.
- Si los conflictos armados se extienden al ciberespacio, el derecho internacional humanitario y el derecho internacional de los derechos humanos, según proceda, se aplicarán al caso que nos ocupe.

La Comisión y la alta representante, en cooperación con los estados miembros, deberán, entre otras tareas, apoyar el desarrollo de normas de conducta y medidas de fomento de la confianza en la *ciberseguridad*, facilitar el diálogo sobre la manera de aplicar el derecho internacional existente en el ciberespacio y la promoción de la Convención de Budapest para hacer frente a los *ciberdelitos*.

Esto nos da paso al estudio de las relaciones bilaterales, particularmente desde la perspectiva de EE. UU., la cooperación internacional en *ciberdefensa* a través de la OTAN y el desarrollo de normas de conducta y

medidas de fomento de la confianza en la seguridad informática, particularmente en la OSCE, organización con capacidad demostrada en este ámbito, y la ONU.

Caso de análisis: los EE. UU.

Los orígenes de la política de *ciberseguridad* de EE. UU. se basan en los esfuerzos de protección de infraestructuras críticas que comenzaron durante la Administración Clinton. La Orden Ejecutiva 13010, Protección de las Infraestructuras Críticas, de 1996, creó la Comisión Presidencial sobre Protección de Infraestructuras Críticas y destacó la amenaza a la seguridad económica y nacional que los *ciberataques* suponían para la nación. Las recomendaciones de la comisión dieron lugar a la Decisión Directiva Presidencial 63, de mayo 1998 (32).

La Estrategia Nacional para Asegurar el Ciberespacio del presidente George W. Bush fue publicada en 2003, pero fue criticada por representar más una lista de recomendaciones que un documento de estrategia global que recoja los fines, las formas y los medios. Además, la Administración Bush publicó en 2006 el Plan Nacional de Protección de Infraestructuras, que designa 17 (ahora 18) sectores clave de infraestructuras que requieren planes de protección individual. También publicó la *Iniciativa nacional integral de ciberseguridad* en 2008, pero su enfoque en el dominio de Internet del Gobierno era demasiado limitado.

La Administración Obama inició sus esfuerzos en *ciberseguridad* con *Los 60 días de examen de las políticas sobre el ciberespacio.* Publicado en mayo de 2009, presenta una revisión sólida de dónde estaba el Gobierno en relación con la *ciberseguridad,* pero ofrecía poco de su visión de la forma de llegar a su destino. La principal recomendación fue que el presidente debería nombrar a un solo coordinador central de los esfuerzos nacionales y del Gobierno para las políticas de *ciberseguridad* (32).

Para Daniel Ventre (33), la política exterior de EE. UU. desde 1948 es «uno de los principales campos de batalla de los dos grandes partidos». El paso de una Administración demócrata a una republicana se traduce en nuevas formulaciones de las cuestiones estratégicas; así, la llegada de la administración republicana (Gobierno de G. W. Bush) está marcada por un cambio semántico en materia de defensa de misiles (pasando de la defensa nacional de misiles de la noción de defensa de misiles), indicativo de un cambio estratégico y de postura («de un Gobierno demócrata poco convencido [...] una Administración republicana decidida»)[4].

[4] GRAND, Camille. «La défense anti-missile: un nouveau paradigme stratégique? », *Revue Politique Etrangère,* 2001, vol. 66, n.° 4, pp. 811-826. http://www.persee.fr/articleAsPDF/polit_0032- 342x_2001_num_66_4_5125/article_polit_0032-342x_2001_num_66_4_5125.pdf.

Los programas de los partidos Republicano y Demócrata (Plataforma Republicana y Plataforma Nacional Demócrata) dedican un espacio relativamente pequeño al problema (33).

La Plataforma Republicana:

- El Partido Republicano es abiertamente hostil a una mayor regulación.
- Los ataques informáticos han seguido creciendo y el fenómeno crecerá. La estrategia de Obama se basa en las prácticas defensivas, aceptando el riesgo de un Pearl Harbor cibernético.
- La política de *ciberseguridad* Republicana se centraría en la desarrollo de capacidades ofensivas.
- Identifican amenazas: China, Rusia, el terrorismo, el ciberespacio…
- El gobierno debe mejorar la seguridad de sus propios sistemas.
- Los republicanos critican la reducción de los gastos de defensa durante el gobierno de Obama (señal de debilidad).
- Proponen el fomento de la cooperación público-privada. El Gobierno debe compartir la información que obtiene sobre la amenaza cibernética con el sector privado, y viceversa, sin poner en peligro la seguridad nacional.
- El Partido Republicano está a favor de la desregulación.

La Plataforma Demócrata:

- La amenaza cibernética está calificada como uno de las más grandes amenazas emergentes contra la seguridad nacional.
- Herramientas que EE. UU. solía emplear son ahora utilizadas por los delincuentes y terroristas, y por otros países para tratar de interrumpir o destruir infraestructuras vitales críticas para la economía, el comercio, la seguridad o el Ejército.
- Las soluciones que propone son el desarrollo de redes seguras y resilientes, la creación del primer *cibermando* dedicado a la *ciberseguridad*, la disuasión, la prevención, la detección y la defensa del país contra las intrusiones digitales.
- Lo anterior requiere inversiones en I+D, el desarrollo de una cultura de ciberseguridad y el fortalecimiento de la colaboración con los actores privados e internacionales.
- La regulación dirigida al fortalecimiento de la capacidad de *ciberseguridad* y basada en el respeto de los derechos de los ciudadanos.
- Neutralidad de la red, abierta a un Internet libre, que favorezca la innovación, la creación, el consumo y la libertad de expresión, libre de toda forma de censura y de violaciones de los derechos privados.

– La Administración Obama da más poder al Department of Homeland Security (DHS) en su misión de protección de los organismos civiles.

Similitudes y diferencias

– Ambos convergen en el reconocimiento de una importante amenaza de naturaleza cibernética contra la seguridad nacional, la necesidad de la cooperación público-privada y el intercambio de información.
– Las diferencias surgen sobre el papel del Gobierno federal en el establecimiento de normas de seguridad. Los republicanos son más reacios a imponer nuevas regulaciones sobre el sector privado (prefieren que la cooperación público-privada sea voluntaria) mientras que los demócratas son más sensibles con los derechos de privacidad del ciudadano.
– También se aprecian diferencias en la posición a adoptar: más defensiva para los demócratas y ofensiva para los republicanos.

De acuerdo con la conocida experta Melisa Hatada (con la que me reuní en Washington en 2012), responsable de la revisión de la política cibernética del presidente Obama y que también tuvo un puesto de gran responsabilidad en la seguridad informática en la Administración Bush, con el Sr. Romane la política de seguridad informática se enfocaría a la gestión: un análisis coste-beneficio por objetivos. Enfoque que no caracteriza la aproximación de Obama.

Debido a su dependencia del ciberespacio, los EE. UU. conscientemente deberían idear una estrategia para influir en el desarrollo del derecho consuetudinario internacional sobre cibernética en lugar de simplemente observar su desarrollo. La mejor manera de hacerlo es a través de una práctica estatal, reconoció. Debido al secreto en el que se envuelven muchas actividades del ciberespacio, en realidad se influye poco en el desarrollo de las normas. Un examen prudente de las acciones de EE. UU. –y la divulgación pública de algunas– ayudaría a establecer una línea de base para el comportamiento aceptable.

Después de que EE. UU. determine las acciones que cree que está autorizado a tomar en el ciberespacio, debe compartir abiertamente al menos ejemplos de las acciones que ha tomado. Además, sin duda debe mirar a la posibilidad de divulgar las acciones emprendidas en su contra. Al proponer algunas de sus propias acciones como aceptables y reconocer las tomadas en su contra como aceptables o inaceptables, EE. UU. podría liderar un diálogo sobre las normas cibernéticas, conduciendo a conclusiones que serían beneficiosas para su seguridad nacional (3).

Estas afirmaciones del coronel Gary Brown y la comandante Kira Poellet, de la Fuerza Aérea norteamericana, introducen el tema central: qué estrategia sigue y sobre todo qué estrategia debería seguir EE. UU. Por

lo que hemos visto hasta el momento, los EE. UU. practican una política activa en multitud de foros (Consejo de Europa, OSCE, ONU...) internacionales tratando de adaptar las normativas a sus propias necesidades o intereses. Examinemos sus estrategias.

La Estrategia de Ciberseguridad de los EE. UU., tiene dos líneas de acción principales:

- Mejorar su capacidad de adaptación a los incidentes cibernéticos.
- Reducir la amenaza cibernética.

El presidente Obama ha declarado que la «amenaza cibernética es uno de los más graves desafíos de la seguridad económica y nacional al que nos enfrentamos como nación» y que «la prosperidad económica de EE. UU. en el siglo XXI dependerá de la *ciberseguridad*». El presidente ordenó una revisión en profundidad de los esfuerzos del Gobierno para defender su infraestructura de información y comunicaciones que se tradujo en un informe titulado *Examen de las políticas del ciberespacio*. Para poner en práctica los resultados de este examen, el presidente ha nombrado un coordinador de *Ciberseguridad* de EE. UU. y creó la Oficina de *Ciberseguridad* en el Estado Mayor de la Seguridad Nacional.

El vicepresidente Biden (34) identificó en su discurso en la Conferencia sobre el CIberespacio de Londres dónde se encuentra EE. UU. en relación con los retos del futuro del ciberespacio:

> *En primer lugar, ¿qué actitud tomar para asegurarse de que la propia Internet siga siendo segura, abierta a la innovación y al mundo a través de la interoperabilidad, lo suficientemente segura como para ganarse la confianza de nuestro pueblo, y lo suficientemente fiable para apoyar su trabajo? Y, en segundo lugar, ¿cómo podemos lograr la seguridad de las naciones, las empresas y las personas en línea sin comprometer la apertura, que es el mayor atributo de Internet?*
>
> *Parece que la respuesta a estas preguntas es una prioridad fundamental, no solo para nuestra Administración sino para todos los que se reunieron en la sala, y para articular nuestra posición, hemos presentado la Estrategia Internacional para el Ciberespacio. Sabemos que necesitamos muchos años y el compromiso paciente y persistente con personas de todo el mundo para construir un consenso en el ciberespacio, pero no hay atajos, porque lo que los ciudadanos hacen en línea no debe, como algunos han sugerido, ser decretado únicamente por grupos de Gobiernos que toman decisiones desde arriba y en su favor. Hay algunos que tienen un punto de vista diferente. Buscan un instrumento jurídico internacional que conduzca al control gubernamental exclusivo sobre los recursos de Internet, las instituciones y los contenidos y las barreras nacionales a la libre circulación de información en línea. Pero esto daría lugar a un Internet fragmentado que no conecta*

a la gente, sino que los divide, un ciberespacio estancado, no innovador, y, finalmente, un ciberespacio menos seguro con menos confianza entre las naciones.

EE. UU. está detrás del actual enfoque que aprovecha lo mejor de los Gobiernos, del sector privado y la sociedad civil para gestionar la evolución técnica de Internet en tiempo real. Esta colaboración público-privada ha mantenido Internet en funcionamiento en todo el mundo.

Tenemos una expresión en nuestro país: si no está roto, no lo arregles. Sería un error, a nuestro juicio, romper con el sistema que ha funcionado tan bien durante tanto tiempo. Sin embargo, hay maneras de mejorar lo que estamos haciendo, por ejemplo, lograr una mayor transparencia y rendición de cuentas al Gobierno e instituciones de Internet, mediante la inclusión de más voces procedentes de los países en desarrollo y el apoyo a las iniciativas de éxito como el Foro de Gobernanza de Internet.

Estamos trabajando con otros países para combatir la delincuencia transnacional, incluido el de ayudar a otras naciones a construir sus capacidades de aplicación de la ley. Hemos ratificado y promovemos enérgicamente la Convención sobre «Cibercrimen» de Budapest, que establece los pasos que deben adoptar los países para reducir la delincuencia al tiempo que protege los derechos humanos. Y, como era de esperar, seguimos comprometidos con la lucha contra el terrorismo internacional y en frustrar los ataques terroristas que se han planeado y puesto en marcha en Internet. Podemos y debemos hacer todo esto sin tener que recurrir a una falsa solución que racionaliza la apropiación del gobierno de Internet. No hay duda en nuestra opinión de que cada nación debe proteger a sus ciudadanos contra la delincuencia y los ataques en línea, y fuera de línea. Pero hay que hacerlo de una manera que sea consistente con nuestros valores compartidos.

Y esto me lleva al concepto que es absolutamente fundamental, en nuestra opinión, llevar a cualquier negociación sobre el futuro del ciberespacio: los principios existentes del derecho internacional se aplicarán en línea tal como se hace fuera de línea. Internet representa y presenta nuevos desafíos, pero para resolverlos no es necesario empezar de cero. Los principios de derecho internacional no se suspenden en el ciberespacio. Se aplican allí con la misma fuerza y la misma urgencia (34).

Los EE. UU. trabajarán a nivel internacional para promover una información abierta, interoperable, segura y fiable y la infraestructura de comunicaciones que apoya el comercio internacional y el comercio, fortalece la seguridad internacional y promueve la libertad de expresión y la innovación para alcanzar esa meta; vamos a construir y mantener un entorno en el que las normas de conducta de una actuación

responsable guían, sostienen las asociaciones, y apoyan el estado de derecho en el ciberespacio (35).

Entre los objetivos de la estrategia se incluye un objetivo de defensa. Junto con otras naciones, fomentará un comportamiento responsable y se opondrá a aquellos que tratan de interrumpir las redes y sistemas, disuadirá y desalentará a los agentes maliciosos, y se reservará el derecho de defensa de estos recursos nacionales vitales cuando sea necesario y apropiado. Con dos formas de acción:

- *Disuasión. Proteger las redes de alto valor requiere de sólidas capacidades de defensa. EE. UU. continuará fortaleciendo su defensa de la red y su capacidad para resistir y recuperarse de las interrupciones y otros ataques. Contra esos ataques más sofisticados que producen daños, vamos a actuar con planes de respuesta bien desarrollados para aislar y mitigar la interrupción de nuestras máquinas, los efectos limitantes en nuestras redes y sus posibles efectos en cascada más allá de ellos.*
- *Intimidación. Los EE. UU. se asegurarán de que los riesgos asociados con atacar o explotar nuestras redes sean mucho mayores que los beneficios potenciales. Cuando sea necesario, los EE. UU. responderán a actos hostiles en el ciberespacio como lo haríamos con cualquier otra amenaza a nuestro país. Todos los estados poseen un derecho inherente a la legítima defensa, y ciertos actos hostiles realizados a través del ciberespacio podrían obligar a acciones en el marco de los compromisos que tenemos con nuestros socios de tratados militares; nos reservamos el derecho de utilizar todos los medios necesarios –diplomáticos, informativos, militares y económicos– que procedan y sean compatibles con el derecho internacional aplicable, a fin de defender a nuestra nación, nuestros aliados, nuestros socios y nuestros intereses. Al hacer esto, vamos a agotar todas las opciones antes de la fuerza militar siempre que podamos, cuidadosamente sopesar los costos y riesgos de la acción contra los costos de la inacción, y actuaremos de una manera que refleje nuestros valores y se refuerce nuestra legitimidad, en busca de amplio apoyo internacional siempre que sea posible.*

Es más, entre las políticas prioritarias, se incluye la militar:

- *Reconocer y adaptarse a la creciente necesidad de redes militares fiables y seguras. Reconocemos que nuestras Fuerzas Armadas dependen cada vez más de las redes que las apoyan, y vamos a trabajar para que nuestras Fuerzas Armadas sigan estando totalmente equipadas para operar incluso en un ambiente donde otros podrían tratar de interrumpir sus sistemas u otras infraestructuras vitales para la defensa nacional. Como todas las naciones, EE. UU. tiene un interés apremiante en la defensa de sus recursos naciona-*

les vitales, así como nuestros principios y valores fundamentales, y estamos comprometidos en la defensa contra aquellos que tratan de impedir nuestra capacidad para hacerlo.

– *Desarrollar y mejorar las alianzas militares existentes para hacer frente a las posibles amenazas en el ciberespacio. Ninguna nación sola puede lograr la «ciberseguridad», y son necesarios mayores niveles de cooperación internacional para hacer frente a esos actores que tratan de perturbar o explotar nuestras redes. Este esfuerzo comienza por reconocer que la naturaleza interconectada de los sistemas en red de nuestros aliados más cercanos, tales como las de la OTAN y sus estados miembros, crea oportunidades y nuevos riesgos en el futuro. Los EE. UU. seguirán trabajando con los militares y sus contrapartes civiles de nuestros aliados y socios para ampliar el conocimiento de la situación y los sistemas compartidos de alerta, aumentar nuestra capacidad de trabajar juntos en tiempos de paz y crisis y desarrollar los medios y el método de la legítima defensa colectiva en el ciberespacio.*

– *Ampliar la cooperación en el ciberespacio con aliados y socios para aumentar la seguridad colectiva. Mediante el desarrollo de un entendimiento común de los procedimientos normalizados de trabajo, nuestras Fuerzas Armadas pueden mejorar la seguridad a través de la coordinación y un mayor intercambio de información, estos compromisos se reducirá percepciones erróneas sobre las actividades militares y la posibilidad de distensión y diálogos comportamiento intercambios de mejores prácticas para mejorar las capacidades asociadas, como la digital, forense, desarrollo de fuerza de trabajo, y la penetración de la red y las pruebas de resistencia serán importantes para este esfuerzo de EE. UU., que trabajará en estrecha colaboración con los estados de ideas afines para aprovechar las capacidades, reducir el riesgo colectivo y promover iniciativas de participación múltiple para impedir las actividades maliciosas en ciberespacio.*

«Las normas internacionales son fundamentales para el establecimiento de una infraestructura digital segura y próspera», afirma el *Cyberspace Policy Review* (2011). «EE. UU. tiene que desarrollar una estrategia diseñada para conformar un entorno internacional y trabajar junto a naciones afines en una serie de cuestiones, entre ellas unas normas aceptables de jurisdicción territorial, la responsabilidad soberana y el uso de la fuerza». Abordar estos temas requiere de los EE. UU. trabajar con todos los países –incluidos los en vías de desarrollo, organismos internacionales, aliados militares y socios de inteligencia–.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, el foro Coope-

ración Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– abordan cuestiones relativas a la infraestructura, información y comunicaciones. Los acuerdos, normas o prácticas promulgadas en estas organizaciones tienen efectos globales y no pueden ser ignorados. El gran número, variedad y diferentes enfoques de estas organizaciones pone a prueba la capacidad de muchos Gobiernos, entre ellos el de EE. UU., para participar adecuadamente (36).

Cuando el 12 de marzo, como todos los años por estas fechas, el director de Inteligencia Nacional de los EE. UU., James R. Clapper, presento la evaluación de la amenaza mundial de la comunidad de inteligencia de los EE. UU., dentro de las amenazas globales, la cibernética ocupaba el primer lugar, por delante de terrorismo y delincuencia transnacional organizada, proliferación de ADM, contraespionaje, medidas contraespaciales o recursos naturales: la inseguridad y la competencia, entre los argumentos.

Inicialmente, define qué entienden por *ciberamenazas*:

> *En los EE. UU., definimos ciberamenazas en términos de «ciberataques» y «ciberespionaje» (37): un «ciberataque» es una operación ofensiva no cinética con la intención de crear efectos físicos o manipular, alterar o suprimir datos. Puede ir desde una operación de denegación de servicio que impide temporalmente el acceso a un sitio «web» a un ataque contra una turbina de generación de energía que causó un daño físico y un apagón que duró varios días. El «ciberespionaje» se refiere a intrusiones en las redes de acceso a información sensible diplomática, militar o económica.*

Luego, se centra en los riesgos crecientes de la infraestructura crítica. Descartando por el momento ataques devastadores por parte de *ciberactores* avanzados como Rusia o China (37):

> *Juzgamos que hay una remota posibilidad de un «ciberataque» importante en contra de los sistemas de infraestructura crítica de EE. UU. durante los próximos dos años, que daría lugar a una interrupción de los servicios de largo plazo y a gran escala como un corte de energía regional. El nivel de conocimientos técnicos y sofisticación operativa necesarios para este tipo de ataque, incluyendo la posibilidad de crear un daño físico o superar los factores de mitigación como el manual, estará fuera del alcance de la mayoría de los actores durante este marco de tiempo. Es poco probable que actores avanzados en el ciberespacio –como Rusia y China– lancen un ataque devastador contra los EE. UU. fuera de un conflicto militar o una crisis que ellos crean que amenaza a sus intereses vitales.*

Actores aislados estatales o no estatales pueden realizar ataques menos sofisticados como una forma de represalia o provocación. Estos actores

muy motivados podrían acceder a redes mal protegidas que controlan las funciones básicas, como la generación de energía, durante los próximos dos años, aunque su capacidad de causar un gran impacto y perturbaciones sistémicas probablemente será limitado. Al mismo tiempo, existe el riesgo de que los ataques sofisticados tuvieran resultados significativos debido a inesperadas configuraciones de sistema, o que la mayor vulnerabilidad de un nodo podría extenderse y contaminar otras partes de un sistema en red (37).

La estrategia del Departamento de Defensa para operar en el ciberespacio de julio 2011 contempla cinco iniciativas estratégicas. La iniciativa estratégica n.º 4 propone «construir relaciones sólidas con nuestros socios y aliados internacionales para fortalecer la *ciberseguridad* colectiva».

Con su compromiso internacional, el Departamento de Defensa apoyará la estrategia internacional de EE. UU. para el ciberespacio y el compromiso del presidente con las libertades fundamentales, la privacidad y el libre flujo de información. El Departamento de Defensa colaborará en los esfuerzos para avanzar en el desarrollo y promoción de unas normas internacionales para el ciberespacio y de los principios que promuevan la apertura, interoperabilidad, seguridad y fiabilidad.

Mientras continúa desarrollándose la cooperación internacional en materia de ciberespacio, el Departamento de Defensa promoverá la cooperación en el ciberespacio con sus aliados más cercanos para defender los intereses en el ciberespacio. El Departamento de Defensa trabajará con sus aliados y socios internacionales para desarrollar capacidades comunes de alerta, participar en la creación de capacidades y llevar a cabo actividades conjuntas de capacitación. Esto creará oportunidades para iniciar diálogos para intercambiar las mejores prácticas en áreas como la forense, el desarrollo de las capacidades, participación en ejercicios y alianzas público-privadas. Además, el desarrollo de los acuerdos para el reparto de carga puede jugar a favor al fortalecer las capacidades centrales de cada país, y lo que reforzará áreas donde los socios son menos competentes aumentará su capacidad y fortalecerá la *ciberseguridad* colectiva.

En su declaración ante la Comisión del Senado de Servicios Armados el 12 marzo 2013, el general Keith B. Alexander (38), comandante del Cibermando de EE. UU., indicó:

> *El Cibermando de los EE. UU. opera en un entorno dinámico y controvertido que cambia literalmente sus características cada vez que alguien enciende la alimentación en un dispositivo de red. Los límites geográficos son quizás menos evidentes en el ciberespacio, pero cada servidor, línea de fibra óptica, antena de telefonía móvil, memoria USB, «router» y ordenador portátil es propiedad de alguien y reside en alguna localidad física. De esta manera, el ciberespacio se asemeja al dominio terrestre –todo tiene un poseedor, y puede ser reformado–.*

> *En este ambiente, que es a la vez ordenado y caótico, beneficioso y peligroso, nosotros en USCYBERCOM tenemos que centrarnos en los actores que poseen la capacidad –y, posiblemente, la intención– de perjudicar los intereses de nuestra nación en el ciberespacio o el uso de medios informáticos para causarnos daño de otras formas. Por desgracia, la lista de los actores de interés para nosotros es cada vez mayor y cada vez también mayor en cuanto a la variedad y complejidad de las formas en que pueden afectar a nuestras operaciones y seguridad. Los agentes estatales siguen encabezando la lista de preocupaciones.*
>
> *Estamos seguros de que los líderes extranjeros creen que un ataque devastador sobre la infraestructura crítica y la población de Estados Unidos por medios cibernéticos sería correctamente remontado hasta su origen y provocaría una respuesta rápida y proporcionada. No obstante, es posible que algún futuro régimen o actor cibernético pudieran malinterpretar el impacto y la certeza de nuestra determinación.*

De acuerdo con la estrategia del Departamento de Defensa para operar en el ciberespacio, el Cibermando de los EE. UU. y la NSA están juntos apoyando al departamento en construir:

- una arquitectura defendible;
- conocimiento de la situación global y una imagen operativa común;
- un concepto para el funcionamiento en el ciberespacio;
- las fuerzas cibernéticas capacitadas y listas, y
- capacidad para actuar cuando sea autorizado.

Y es en este punto donde resalta la importancia de la cooperación con socios y aliados:

> *También nos beneficiamos al compartir con los servicios y organismos asociados y aliados clave.*
>
> *Además, las nuevas reglas de enfrentamiento para el ciberespacio actualmente en desarrollo cumplirán con y apoyarán a las directrices de política recientemente emitidas en «ciberoperaciones» estadounidenses.*

El general de Ejército Keith B. Alexander afirmó que el Mando está desarrollando equipos que protegerían los intereses de la nación en el ciberespacio, junto con las tácticas, técnicas y procedimientos y la doctrina que describe cómo los equipos trabajarán en ese ambiente (39).

> *Estos equipos para defender la nación no son equipos defensivos, son equipos ofensivos que el Departamento de Defensa podría utilizar para defender a la nación si fueran atacados en el ciberespacio (...). Trece de los equipos que estamos creando son solo para ese conjunto de misio-*

> *nes. También estamos creando 27 equipos que apoyarían comandos combatientes y a su proceso de planificación de capacidades cibernéticas ofensivas.*

El CYBERCOM también tiene una serie de equipos que van a defender las redes del Departamento de Defensa en el ciberespacio. La intención es poner en pie cerca de un tercio de los equipos antes de septiembre, otra tercera parte en septiembre de 2014, y la tercera final para septiembre de 2015.

> *Estos tres grupos de equipos son el núcleo, la construcción por el que estamos trabajando con los servicios para desarrollar nuestros cuadros cibernéticos.*

Por su parte, el general C. R. Kehler, comandante del Mando Estratégico de EE. UU., indicó que mejorar la capacidad del Departamento de Defensa para operar de manera efectiva en el ciberespacio requería una inversión en cinco grandes áreas: arquitectura defendible (ambiente de información conjunta), fuerzas entrenadas y listas, mando y control efectivo, conocimiento de la situación global y reglas de enfrentamiento para entablar combate para defender a la nación en el ciberespacio. De todas ellas, la inversión más urgente es aumentar el número, la formación y la preparación de las *ciberfuerzas* (40).

La expansión aumentará el CYBERCOM del Departamento de Defensa a más de 4.000 personas, frente a los actuales 900 –de acuerdo con un funcionario estadounidense–. Un reto formidable para el crecimiento del Mando sería encontrar, formar y retener a un número tan grande de personas cualificadas.

En octubre, el señor Panetta advirtió seriamente de que EE. UU. se enfrenta a la posibilidad de un «Pearl Harbor cibernético» y cada vez eran más vulnerables a piratas informáticos extranjeros que podrían desmantelar la red nacional de energía eléctrica, el sistema de transporte, la red financiera o la del Gobierno. Dijo que «una nación agresora» o grupo extremista podría causar una catástrofe nacional, y que él estaba reaccionando a la creciente asertividad y los avances tecnológicos por los adversarios de la nación, identificados por los funcionarios como China, Rusia, Irán y los grupos militantes (41).

Funcionarios de Defensa dijeron que el señor Panetta estaba especialmente preocupado por un ataque informático en agosto pasado contra la petrolera estatal saudí Aramco, que infectó e inutilizó a más de 30.000 ordenadores. En octubre, los funcionarios de inteligencia estadounidenses dijeron que estaban cada vez más convencidos de que los ataques saudíes se habían originado en Irán. Describieron una guerra en las sombras emergente de ataques y contraataques en curso entre EE. UU. e Irán en el ciberespacio. Entre los funcionarios estadounidenses, la sospecha

se ha centrado en los Cybercorps, creado en 2011 por el Ejército de Irán, en parte en respuesta a los ataques informáticos estadounidenses e israelíes sobre la planta de enriquecimiento de uranio iraní en Natanz. No hay pruebas contundentes, sin embargo, los ataques fueron sancionados por el Gobierno iraní (41).

Un resumen de EE. UU. en el ciberespacio para 2013 sería: ninguna ley y un entorno de negociación internacional duro, pero se aprecian progresos por parte del poder ejecutivo en el esclarecimiento de las actividades militares digitales, vinculándolas a la *ciberdefensa,* y en el establecimiento de normas para el desarrollo de una infraestructura crítica más segura. De ser ampliamente adoptadas las nuevas normas, que se centran en las vulnerabilidades más frecuentes, se acelerará esta tendencia. La *ciberseguridad* en EE. UU. ha mejorado a pesar del *impasse* en el Congreso, pero ulteriores progresos requerirán del acuerdo internacional para limitar la actividad maliciosa en el ciberespacio, lo que parece ser una posibilidad remota. Los EE. UU. son más seguros de lo que eran hace cinco años, pero todavía no son seguros (10).

Conclusiones

Parece existir una práctica unanimidad a la hora de indicar la necesidad de negociar acuerdos internacionales que regulen el ciberespacio. Pero parecen existir diferencias insalvables en cuanto a qué deberían incluir esos acuerdos, el carácter de los mismos y las organizaciones de referencia.

Podríamos definir tres cosmovisiones básicas: la *ciberliberal* defensiva representada por la UE, y compartida por casi todos los países europeos; la *ciberliberal* ofensiva representada por los EE. UU., y la *cibernacionalista*-aislacionista representada por China y Rusia. A ellas hay que añadir las que, como Irán o Corea del Norte, sin disponer de la sofisticación de las grandes potencias, disponen de unas capacidades ofensivas a tener en cuenta.

El paso de una Administración demócrata a una republicana en EE. UU. se traduce en un cambio estratégico y de postura «de un Gobierno demócrata poco convencido (...) a una Administración republicana decidida». De acuerdo con Melissa Hathaway, con el Sr. Romney la política de seguridad informática se enfocaría a la gestión: un análisis coste-beneficio por objetivos; enfoque que no caracteriza la aproximación de Obama.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, OSCE, el foro Cooperación Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– están involucradas en seguridad ciber-

nética. EE. UU. y Rusia tienen sus propias organizaciones de referencia, Consejo de Europa y OSCE en el caso norteamericano y Naciones Unidas en el ruso. Ambos se bloquean respectivamente en sus propuestas.

Rusia y China recibieron un sorprendente grado de apoyo en su propuesta ante la ONU. Muchos países están desencantados con el modelo ortodoxo y se mueven en silencio en hacia un modelo «no occidental» de la gobernanza de Internet. Los regímenes autoritarios se han aprovechado de esta insatisfacción y la intentan utilizar para sus propios fines políticos.

El establecimiento de normas para el empleo del ciberespacio por parte de los estados no debería requerir una modificación de las leyes internacionales consuetudinarias ni considerar obsoletas las leyes actuales; lo que sería necesario es aclarar cómo esas normas existentes se aplican y que nuevos elementos serían necesarios para que fueran útiles.

En cualquier caso, se tienen que mantener unos valores esenciales como son: respeto a los derechos fundamentales de libertad de expresión y asociación, incluso *online,* respeto a la propiedad intelectual (patentes, *copyright*), y evitar interferencias estatales injustificadas, pero permitiendo la lucha contra los *ciberdelincuentes*, asegurando el Estado de derecho y evitando la creación de santuarios para estos delincuentes.

Todo país tiene derecho a la autodefensa contra actos de agresión en el ciberespacio, autodefensa enfocada en el mantenimiento del funcionamiento de la red global y en la mejora de *ciberseguridad*.

Otros elementos a tener en cuenta a la hora de redactar normas son: interoperabilidad global, estabilidad de la red y libre flujo de información, acceso fiable a todo individuo y presencia de grupos distintos del Gobierno en la gobernanza de Internet, abierta a actores no gubernamentales

En cualquier caso, no debemos perder la esperanza de que las grandes *ciberpotencias* lleguen a un acuerdo que permita fomentar la confianza y aumentar la transparencia reduciendo los crecientes riesgos asociados con los cada vez más numerosos y cada vez más complejos ataques cibernéticos. En unos años podría alcanzarse un acuerdo…

¡O no!

Bibliografía

1. OBAMA, Barak. *Discurso sobre el estado de la Unión de Barack Obama.* Washington: The White House, 2013.
2. STEPHENS, Bret. «The Limits of Stuxnet». *The Wall Street Journal.* [En línea] 18 de enero de 2011 [citado el 2 de enero de 2013]. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.

3. BROWN, Gary y POELLET, Keira. «The Customary International Law of Cyberspace», IV, 2012. *Strategic Studies Quarterly,* otoño de 2012, vol. 6, págs. 126-145.
4. HOWEIDY, Amira. «Big Brother or war criminal?» *Al Ahram weekly.* [En línea] 11 de junio de 2013 [citado el 2013 de junio de 15]. http://weekly.ahram.org.eg/News/2947/19/Big-Brother-or-war-criminal-.aspx.
5. *Estrategia Nacional Militar de los Estados Unidos de América.* Washington, EE. UU.: Joint Chief of Staff, 2011.
6. SOMMER, Peter y BROWN, Ian. *Reducing Systemic Cybersecurity Risk.* Informe OCDE, 2011.
7. PRINCE, Matthew. «The DDoS That Almost Broke the Internet». [En línea] 27 de marzo de 2013 [citado el 28 de marzo de 2013]. *Cloud Flare.* http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet.
8. PÉREZ, Jesús. «Cómo Cyberbunker atacó a Spamhaus y casi se llevó a medio Internet por delante». *Security by Default.* [En línea] 28 de marzo de 2013 [citado el 12 de mayo de 2013]. http://www.securitybydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.
9. VENTRE, Daniel. «Japon: stratégies de cyberdéfense, Multi-System and Internet-Security-Cookbook». *MISC,* 2012, n° 64, págs. 65-73.
10. LEWIS, James Andrew. *Critical Questions for 2013: Global Challenges. What's Next in Cybersecurity?* [En línea] 25 de enero de 2013 [citado el: 30 de marzo de 2013]. Center for Strategic and International Studies. http://csis.org/publication/critical-questions-2013-global-challenges.
11. BAGCHI, Sohini. «India needs more warriors in the cyber space». *Cxotoday.com.* [En línea] 3 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.cxotoday.com/story/india-needs-more-warriors-in-the-cyber-space/.
12. ZORZ, Zeljka. «India has a new National Cyber Security Policy». *Help net security organization.* [En línea] 10 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.net-security.org/secworld.php?id=14891.
13. PERTERMANN, Kerstin. *Conference report: Challenges in Cybersecurity, Risks, Strategies, and Confidence-Building International Conference.* Hamburgo: Institute for Peace Research and Security Policy at the University of Hamburg, 2011.
14. HEICKERÖ, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Estocolmo: Swedish Defence Research Agency Division of Defence Analysis, 2010.
15. FEDORENKO, Andrei. «The Fight Over the Draft. UN Convention on International Information Security». *Regulatory cyber security: The*

FISMA focus IPD. [En línea] 15 de julio de 2012 [citado el 12 de mayo de 2013]. http://www.thecre.com/fisma/?p=2173.

16. DEAL, Jacqueline N. *IGCC Workshop Report on China and Cybersecurity. Information Warfare Doctrine. Chinese Information War: Historical Analogies and Conceptual Debates.* San Diego: Universidad de California, 2012.
17. YUXIAO, Li. *National Cybersecurity Policy Cyberspace Security and International Cooperation in China.* San Diego: Universidad de California, 2012.
18. STOKES, Mark. *People's Liberation Army Infrastructure for Cyber Reconnaissance.* San Diego: Universidad de California, 2012.
19. SCHNEIDER, Deborah. *United States Mission to the OSCE Cyber Security Keynote Address by Dr. Deborah Schneider, U. S. Department of State as Delivered to the Joint FSC/PC.* Viena: OSCE, 2010.
20. WEGENER, Henning. *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence Building Measures.* [En línea] 23 de agosto de 2012 [citado el 29 de marzo de 2013]. http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Wegener publication.docx.
21. HEALEY, Jason y VAN BOCHOVEN, Leendert. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington: The Atlantic Council of the United States, 2011.
22. GEERS, Kenneth. *Cyberspace and the changing nature of warfare.* [En línea] 27 de agosto de 2008 [citado el: 31 de marzo de 2013]. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.
23. ARCHICK, Kristin. *CRS Report for Congress. Cybercrime: The Council of Europe Convention.* Washington: Congressional Research Service, 2004.
24. TIKK, Eneken. *Comprehensive legal approach to cyber security 2011.* Tarfu, Estonia: Faculty of Law, University of Tartu, 2011.
25. SCHJØLBERG, Stein y GHERNAOUTI-HÉLIE, Solange. *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace,* segunda edición. Oslo: AiTOslo, 2011.
26. OSCE_MC.DEC/7/06. *DECISION No. 7/06 Countering the Use of the Internet for Terrorist Purposes.* Bruselas: OSCE, 2006.
27. [En línea] 16 de octubre de 2009 [citado el 31 de marzo de 2013]. EE. UU.: OSCE, 2013. https://dazzlepod.com/cable/09STATE107552/.
28. Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* [En línea] 16 de marzo de 2005 [citado el 31 de marzo de 2013]. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

29. UE. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruselas: European Commission & High Representative of the European Union for Foreign Affairs And Security Policy, 2013.
30. KAGAN, Robert. *Paradise and Power: America and Europe in the New World Order.* Londres: Atlantic Books, 2004.
31. BAILEY, Eric. *«Nothing Can Justify Torture»: An Interview with Noam Chomsky on Obama's Human Rights Record.* [En línea] 12 de diciembre de 2012 [citado el 30 de marzo de 2013]. http://chomsky.info/interviews/20121212.htm.
32. NEWMEYER, Kevin P. *Who should lead U.S. cyber security efforts? PRISM*, 2012, vol. 3, n.º 2, págs. 115-126.
33. VENTRE, Daniel. *La politique de cyberdéfense peut-elle être a-politique?* Paris: Ministère de la défense Délégation aux Affaires Stratégiques, 2013.
34. BIDEN, Joseph R. *VP's Remarks to London Cyberspace Conference.* Londres: The White House, 2011.
35. *International Strategy for Cyberspace.* Washington: The White House, 2011.
36. *Cyberspace Policy Review.* Washington: The White House, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
37. CLAPPER, James R. *Worldwide Threat Assessment of the US Intelligence Community 2013.* Washington D. C.: Office of the Director of National Intelligence, 12 de marzo de 2013.
38. ALEXANDER, Keith B. *Statement of general Keith B. Alexander Commander United States Cyber Command before the Senate Committee on Armed Services.* Washington: United States Cyber Command, 2013.
39. PELLERIN, Cheryl. American Forces Press Service. Cybercom Builds Teams for Offense, Defense in Cyberspace. [En línea] 12 de marzo de 2013 [citado el 30 de marzo de 2013]. http://www.defense.gov/news/newsarticle.aspx?id=119506.
40. KEHLER, C. R. *Statement of general C. R. Kehler Commander United States Strategic Command before the Senate Committee on Armed Services.* Washington: United States Strategic Command, 12 de marzo de 2013.
41. BUMILLER, Elisabeth. «Pentagon to Beef Up Cybersecurity Force to Counter Attacks», *The New York Times*. [En línea] 29 de marzo de 2013 [citado el 31 de marzo de 2013]. www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html.
42. OCDE. *Future Global Shocks. Improving Risk Governance.* París: OCDE, 2011.

43. FROOMKIN, Michael. «Cybercrime Treaty Goes Live». *Discourse.net.* [En línea] 19 de marzo de 2004 [citado el 31 de marzo de 2013]. http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html.
44. SAFIRE, William. «The Farewell Dossier». *The New York Times.* [En línea] 2 de Febrero de 2004 [citado el 2 de enero de 2013]. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsaire.
45. *Estrategia Española de Seguridad.* Madrid: Gobierno de España, 2011.

Conclusiones de una conciencia de *ciberseguridad* y *ciberdefensa*

La esperanza tiene dos preciosos hijos: sus nombres son enfado y valor; enfado al ver cómo son las cosas y valor para no permitir que continúen así

San Agustín

La elaboración de las conclusiones de esta monografía es desarrollada a título estrictamente personal después de una reflexión detallada de los cinco documentos que la componen.

Vivimos momentos especialmente interesantes para una reflexión como la que se ha llevado a cabo en este trabajo. La noticas sobre *ciberseguridad* inundan los espacios informativos y se considera, en las estrategias de seguridad de todos los países, incluido el nuestro, que la *ciberseguridad* es un elemento clave a tener en cuenta para el desarrollo de una sociedad civil adecuadamente formada, de unas empresas con formación y tecnologías suficientes de prevención ante los incidentes derivados de la misma y de una Administración Pública dotada de tecnologías y formación para prestar al ciudadano los servicios públicos que se necesitan con garantías suficientes y que permita que la ciudadanía se relacione con la Administración de forma segura y confiable, avanzando, como en el caso de España, en el desarrollo de la agenda digital. Parte fundamental de esta agenda digital es la *ciberseguridad*.

Es el momento adecuado para progresar en el desarrollo de una estrategia de *ciberseguridad* donde, además de detallar los riesgos, las amenazas y las vulnerabilidades, se trate a aquella como un elemento tractor de la industria especializada de la información. También es forzoso abordar los papeles que tienen que desarrollar los distintos actores de la Administración, incluido el tema fundamental, el de la gobernanza. Para que esta estrategia se consolide, necesita abordar como elemento vertebrador la relación público-privada, siendo esta última el elemento que permite actuar sobre las amenazas y los riesgos de una forma rápida y en continuo movimiento. Si algo caracteriza a este sector es el cambio continuo y, para prevenir y actuar contra los ataques, es necesaria una flexibilidad que aporta el sector privado. La necesidad de abordar una política de I+D nacional en este área es fundamental para desarrollar tecnologías que permitan una vida ordenada en este espacio de posibilidades que es el ciberespacio.

Intentar describir la inquietud ante la necesidad de vertebrar elementos público-privados en el desarrollo de las capacidades de *ciberseguridad*, inteligencia y seguridad económica de nuestro país para el fortalecimiento de nuestra posición en el mercado internacional, el desarrollo de la competitividad del tejido industrial, la seguridad de la economía y de las empresas y el refuerzo de la influencia de nuestro país no es algo nuevo.

En el caso de los intervinientes en este trabajo, los evangelizadores, ha sido una labor de comunicación continuada durante muchos años intentando hacer comprender el escenario que se nos avecinaba, avanzando en todas nuestras intervenciones, la necesidad de concienciar a la Administración, a las empresas y a los particulares sobre las amenazas, los riesgos y las oportunidades que este nuevo modelo de interrelación social iba a generar.

Acaba de ser publicada la Estrategia Nacional de Seguridad para España y estamos a la espera de que vea la luz la Estrategia Nacional de Ciberseguridad. Un mundo que no deja de avanzar de una forma cada vez más acelerada donde el análisis de los acontecimientos nos hace modificar nuestras percepciones y los modelos con los que tradicionalmente habíamos entendido la realidad. Es por ello que dichas estrategias son elementos vertebradores fundamentales para el posicionamiento de nuestro país en la esfera internacional y permiten desarrollar las bases y los objetivos y esbozar el recorrido para alcanzar ese fin.

La crisis económica, los conflictos sociales, los nuevos escenarios de guerra económica, las situaciones de nuevos espacios de confrontación son parte sustancial de nuestra vida diaria. Pero, del mismo modo, aparecen nuevas oportunidades que permiten comprender por qué las grandes crisis proporcionan nuevas vías de expresión del ser humano, elabo-

rando nuevas construcciones de entendimiento de nuestro presente y de nuestro futuro.

Hablar de *ciberseguridad*, en estos últimos trece años, ha sido la prédica de la anticipación de una revolución tecnológica que iba aparejada a un nuevo modelo de cambio social. La tecnología de Internet ha proporcionado un nuevo paradigma de la comunicación social, rompiendo las dimensiones clásicas del espacio y el tiempo. La tecnología que posibilita este cambio también permite que se desarrollen capacidades que generan amenazas para las que ni países ni empresas ni individuos estábamos preparados. Por ello, esa labor de comprensión del nuevo entorno necesita nuevas herramientas de estudio, de formación y de colaboración entre todos los agentes sociales tanto públicos como privados.

La colaboración público-privada es reconocida por todos como la única vía de abordar esta situación. La gestión de los riesgos, las amenazas, la prevención de estos elementos y el desarrollo de la capacidad de reacción ante una alerta temprana frente a incidentes se demuestra como estratégica en el mantenimiento de la integridad tanto de individuos como de empresas y estados. Nadie está excluido del riesgo, por este motivo la necesidad de concienciación de estos riesgos es de obligado cumplimiento.

Las manifestaciones en la red del crimen organizado, del proselitismo terrorista, de la acción terrorista, del ataque contra los activos intangibles de las empresas mediante el espionaje a través de *advanced persistent threats,* y del riesgo de los ciudadanos, especialmente los jóvenes frente al acoso bajo sus distintas manifestaciones, ha hecho que palabras como *ciberseguridad, ciberterrorismo, ciberataques, ciberdefensa, ciberacoso*... se instalen en nuestra semántica diaria.

Los procesos de convergencia de las distintas seguridades ya es algo cotidiano. La realidad presenta situaciones para resolver esas aparentes contradicciones. La Ley de Protección de Infraestructuras Críticas genera un espacio de diálogo entre los responsables de seguridad de las organizaciones para consolidar un único interlocutor frente a riesgos que provienen de dos espacios distintos, «el físico y el lógico», pero esa categorización tiene menos sentido cuando lo que realmente importa es la prevención de los riesgos y la gestión de las amenazas, cuando se pone el objetivo en lo que nos une más que en lo que nos separa. No hay espacios limitativos ya que la **seguridad** sí es una tarea de todos.

Los años de análisis sobre este tipo de cambio social que empezamos algunos en el año 1982 y que en los últimos años hemos venido anticipando nos han permitido «evangelizar» sobre los riesgos inminentes que se cernían sobre nuestro día a día si no nos concienciábamos de la necesidad de entender y prevenir los riesgos y convertirlos en oportunidades para, entre otras cosas, generar en España un tejido industrial de

primer orden que pudiera poner a disposición de las empresas, de las personas y de la Administración unas tecnologías «marca España» que posibilitaran la percepción de la Seguridad como elemento constitutivo de nuestro día a día.

Vivimos en un mundo complejo y contradictorio que está evolucionando cada vez más rápidamente, en el que el volumen y la multiplicidad de la información convierten a cada individuo, a cada empresa y a cada país en agente y árbitro de un juego que a menudo le supera. Sabemos más y más rápido y sobre más cosas, siendo conscientes, al mismo tiempo, de que la vulnerabilidad está en relación directa con el volumen del flujo de información recabado y de que la realidad virtual a veces gana por la mano a la verdadera.

En una economía globalizada, controlar lo antes posible la información es la clave para poder organizar el mercado y el mundo a voluntad. La capacidad de comprender nuestro entorno con el fin de disponer de la información necesaria para aprovechar las oportunidades que se presenten y evitar los posibles peligros es una disciplina de gestión, es un planteamiento de gestión estratégica.

La economía del conocimiento está llamada a remplazar a la economía tradicional. Mientras tanto, las tecnologías de la información transforman las organizaciones, modifican el entorno en el que se toman las decisiones y dan lugar a nuevas formas de pensar y actuar. El estado actual de conciencia nacional de *ciberseguridad* es, cuando menos, manifiestamente mejorable. Lo cual no es de extrañar dado que el grado de compromiso de la sociedad española con la seguridad y defensa dista mucho de ser óptimo y la *ciberseguridad* es un concepto que ha empezado a llegar al público no especializado hace relativamente poco tiempo.

Para la protección de la seguridad económica de nuestro país, sería necesario considerar a las empresas españolas que proveen tecnologías para la *ciberseguridad* y la inteligencia, por el carácter sensible de sus investigaciones y debido a que las tecnologías desarrolladas son españolas, compañías que deben ser consideradas de interés estratégico de la misma forma que otras son consideradas en otros países, donde se ha creído fundamental posicionarse en este espacio de carácter estratégico.

Entre las funciones que desarrollan estas compañías, se encuentran la de proporcionar información de los riesgos y las amenazas del entorno global actual, ayudando al responsable de la toma de decisiones a vigilar las tendencias y la información susceptibles de afectar a su organización, con el fin de alertarla y advertirla. Una de las soluciones que permiten controlar la sobreabundancia de información consiste en recurrir, por supuesto, a la asimilación del ciclo de información, pero sobre todo a herramientas informáticas de control, monitorización y alerta temprana ante cualquier alerta considerada de interés.

En este sentido, la Estrategia Europea de *Ciberseguridad* ha definido que, para el desarrollo de recursos industriales y tecnológicos para *ciberseguridad*, se promoverá la creación de un mercado único para productos de seguridad. En 2014 se pondrá en marcha un programa para la investigación y desarrollo de tecnologías de seguridad, centrándose en las tecnologías emergentes (se nombra la informática forense y la nube). Además, se incentivará el consumo de productos «seguros» dentro de la UE. Las medidas de incentivación serán el fomento de la gestión del riesgo, adopción de estándares y soluciones de seguridad.

Los procesos de convergencia de la *ciberseguridad, ciberterrorismo, ciberactivismo* y *ciberespionaje,* hacen imprescindible el desarrollo en nuestro país tanto de capacitación personal como de consolidación empresarial de las compañías que realizan servicios en la prevención de todo este tipo de situaciones, tal y como están desarrollando los países de nuestro entorno. Países que se están tomando muy en serio que quien tenga la capacidad de influencia en este quinto espacio será el que detente realmente un principio de soberanía en la toma de sus decisiones como país. Entre las funciones que desarrollan, se encuentran la de proporcionar información de los riesgos y las amenazas del entorno global actual, ayudando al responsable de la toma de decisiones a vigilar las tendencias y la información susceptibles de afectar a su organización, con el fin de alertarla y advertirla. Una de las soluciones que permiten controlar la sobreabundancia de información consiste en recurrir, por supuesto, a la asimilación del ciclo de información, pero sobre todo a herramientas informáticas de control e incluso de traducción.

Para alcanzar una reducción drástica del *cibercrimen*, la UE aboga por endurecer la legislación, desarrollando leyes específicas para «tipos de *cibercrimen*», junto con la creación de alianzas para su persecución. Por las características de los *cibercrímenes*, se requiere disponer de conocimientos especializados y medios tecnológicos para su investigación. Desde la UE se percibe un desequilibrio de capacidades entre los países miembros. Para la eliminación de estas diferencias desde la UE, se financiarán programas dentro de los países miembros para la identificación de fortalezas y carencias en las capacidades para la investigación del *cibercrimen*. De la misma forma, la OSCE, en la reciente reunión sobre nuevas técnicas de investigación contra el crimen organizado y la lucha antiterrorista, aboga por la colaboración y el desarrollo de capacidades tecnológicas y humanas en este sentido. También Europol, a través del EC3 *(European Cybercrime Center)*, desarrolla las capacidades de formación, desarrollo tecnológico e investigación, utilizando la red de Centros de Excelencia en Formación en Ciberseguridad, (ECTEG *European Cybercrime Training & Education Group*) financiados por la Comisión Europea, como el CNEC español, donde está presente el Ministerio del Interior, el Instituto de Ciencias Forenses y de la Seguridad de la UAM y S21sec, como em-

presa privada impulsora del proyecto de colaboración público-privado. El Consejo de Europa, en el Convenio sobre la *Ciberdelincuencia* de Budapest de 2001, manifiesta en su preámbulo la necesaria colaboración en materia penal de los firmantes en la lucha contra la delincuencia informática, considerada una amenaza transnacional.

El *cibercrimen* se ha convertido en uno de los principales problemas para la estabilidad económica de empresas y países. La industria del robo de información para financiar actividades de crimen organizado y terrorismo se ha convertido en un pingüe negocio para las redes de criminalidad organizada. Para defender los intereses legítimos de empresas, ciudadanos y países, algunas empresas se especializan en la recuperación de datos. Este servicio puede convertirse en algo indispensable en un mundo en el que la información interna de la empresa pasa a encontrarse casi totalmente en formato digital.

Una de las dimensiones de la *ciberinteligencia* es la de proteger los activos de la empresa. Ahora bien, estos activos son múltiples y están muy diversificados, hasta el punto de que resulta muy difícil garantizar una cobertura completa. Desde el robo de datos confidenciales contenidos en soporte informático hasta los atentados terroristas contra instalaciones de producción, pasando por la devaluación de la reputación o la imagen de la empresa, los gastos se multiplican cada vez más para las empresas.

Interpol, en su lucha contra el crimen cibernético, declara que:

> *Cybercrime is one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, Internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets and various email scams such as phishing.*
>
> *The global nature of the Internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace. The use of the Internet by terrorists, particularly for recruitment and the incitement of radicalization, poses a serious threat to national and international security.*
>
> *In addition, the threat of terrorism forces authorities to address security vulnerabilities related to information technology infrastructure such as power plants, electrical grids, information systems and the computer systems of government and major companies.*

La formación, inicial y continua, desempeña por tanto un papel clave en la política pública de *ciberinteligencia*. Para que la iniciativa de *cibersegu-*

ridad traiga como resultado la toma de medidas apropiadas, se requiere formar a especialistas capaces de dirigir políticas de *ciberinteligencia* en las empresas y de elaborar las herramientas correspondientes.

La formación de todos los agentes, por un lado, y de una cantidad adecuada de especialistas, por el otro, supone un avance importante de la enseñanza superior en el plano de la *ciberinteligencia*. Esto se ha de traducir en la constitución de un referente de formación, seleccionando dos ejes de trabajo –la formación inicial y la formación continua– con un objetivo común: lograr que la mayor cantidad posible de responsables de seguridad recurran a la *ciberinteligencia* como método de análisis y de tratamiento de los desafíos, tanto desde la perspectiva de la influencia como de la vigilancia y la protección de los activos.

La voluntad de dotar a España herramientas y métodos óptimos para la práctica de la *ciberseguridad* en los años venideros implicaría numerosas necesidades de investigación en la intersección de las ciencias humanas, lingüísticas, económicas, sociales, políticas y jurídicas, así como de las ciencias y tecnologías de la información y de la comunicación.

Considerar los aspectos claves que configuran una Estrategia Nacional de Seguridad como la recientemente aprobada en España, determinada por su concepción como política de Estado, permite avanzar decididamente en el posicionamiento de nuestro país en el espacio geopolítico internacional. La Estrategia se articula en torno a cinco capítulos en los que se ofrece un concepto de seguridad nacional, se sitúa la seguridad de España en el mundo, se identifican los riesgos y amenazas actuales, se trazan a partir de esta base los objetivos y las líneas de acción estratégicas en los ámbitos de actuación prioritarios para España y se configura un nuevo Sistema de Seguridad Nacional.

Es fundamental considerar que, para garantizar la seguridad de un país, es preciso tener en cuenta el entorno internacional y la competitividad, la *ciberseguridad* y las organizaciones, la gestión de la información y de los conocimientos, la protección y la defensa del patrimonio informático y de los conocimientos, y, finalmente, la influencia y la contrainfluencia.

Los dominios conectados globalmente como el ciberespacio están siendo desafiados de forma creciente por actores tanto estatales como no estatales. Los actores no estatales, como grupos terroristas, traficantes o delincuencia internacional organizada, están interesados en explotar estos dominios, mientras que ciertos estados desarrollan actividades encaminadas a reducir la libertad de movimiento internacional.

Una característica del mercado es la omnipresencia de la información, que constituye una verdadera materia prima estratégica en todos los sentidos. Por este motivo, los desafíos a los que se enfrenta una organización son dos: por un lado, el de recopilar información mediante he-

rramientas especiales, con el fin de contrastarla con otros datos y aprovecharla en el momento oportuno, y, por otro, el de proteger los datos estratégicos de los que dispone.

La economía del conocimiento está llamada a remplazar a la economía tradicional. Mientras tanto, las tecnologías de la información transforman las organizaciones, modifican el entorno en el que se toman las decisiones y dan lugar a nuevas formas de pensar y actuar. Su creciente nivel de importancia ha suscitado desde hace tiempo el interés de organismos internacionales del máximo nivel, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), que considera Internet como un «elemento fundamental para impulsar el desarrollo económico y el bienestar social, así como para fortalecer la capacidad de las sociedades para mejorar la calidad de vida de sus ciudadanos».

A nivel nacional, se debe tratar de establecer un dispositivo de organización flexible y de gran capacidad de reacción, incluso en caso de emergencia, capaz de movilizar los recursos de todos los servicios que lo componen y dotado de los conocimientos y experiencia necesarios para cumplir su tarea con todas las garantías. Incluyendo todas las capacidades de respuesta tanto públicas como privadas.

La aspiración de las empresas a extenderse a mercados extranjeros requiere un proceder metódico y riguroso. La definición del plan estratégico o la elaboración del entramado jurídico y financiero de una operación de exportación o de la creación de una sucursal local exigen una lectura global de la situación geoestratégica y de negocio del país objetivo. El apoyo a las empresas en sus acciones estratégicas genera un círculo virtuoso de evaluación del riesgo y la adopción de las medidas pertinentes para minimizarlo, convirtiendo los riesgos en ventajas competitivas.

Vivimos en un mundo complejo y contradictorio que está evolucionando cada vez más rápidamente, en el que el volumen y la multiplicidad de la información convierten a cada individuo, a cada empresa y a cada Estado en agente y árbitro de un juego que a menudo le supera. Sabemos más y más rápido y sobre más cosas, siendo conscientes, al mismo tiempo, de que la vulnerabilidad está en relación directa con el volumen del flujo de información recabado y de que la realidad virtual a veces gana por la mano a la verdadera.

La decisión de nuestro país, manifestada el día 21 de mayo de 2013 por parte del presidente Rajoy, de dotar a España de un Sistema de Inteligencia Económica supone un hito fundamental en el proceso de concienciación de la necesidad de este modelo de gestión estratégica del país. En palabras del presidente, «facilitará la detección y prevención de actuaciones contrarias a los intereses económicos, financieros, tecnológicos y comerciales de España en sectores estratégicos».

El concepto de sector estratégico se debe someter a una revisión, ya que estratégico tradicionalmente ha estado vinculado con unas compañías de gran tamaño. Este aspecto necesita ser revisado desde el prisma de nuestra capacidad de generar negocio en el exterior, el desarrollo de tecnologías (por ejemplo, la gestión del agua) y el reforzamiento del I+D+i nacional, fomentando una verdadera compra innovadora en nuestra Administración que sirva de elemento tractor para el sector y de influencia en el exterior, reforzando las capacidades comerciales de todos los miembros, no solo de nuestro cuerpo de diplomacia sino de todos los representantes de los distintos ministerios en nuestras delegaciones. Las actividades orientadas a la diplomacia económica y el reforzamiento de nuestra política de I+D en seguridad y *ciberdefensa*, enmarcadas en la actividad del Estado, posibilitan cambios fundamentales en nuestra presencia en los ámbitos internacionales, permitiendo un mayor nivel de acceso a la toma de decisiones en contratos internacionales y fortaleciendo el posicionamiento estratégico no solo de nuestras empresas sino también, por añadidura, de nuestro país.

La capacidad de influencia y contrainfluencia debe estar sustentada en capacidad disuasoria creíble. Para este fin, es necesario contar con un plan estratégico a corto, medio y largo plazo que, a la vez que nos permita tener éxitos inmediatos, genere una cultura de éxito y optimismo que cambie la dinámica de resignación y pesimismo instaurada en nuestra sociedad. La necesidad de éxitos y transmitirlos de la forma adecuada, tanto en el ámbito doméstico como internacional, nos permitirá desarrollar unas acciones de influencia que deben ser consideradas de Estado, independientes de los cambios de gobierno de uno u otro signo.

> *La seguridad nacional es un servicio público objeto de una política de Estado, que, bajo la dirección y liderazgo del presidente del Gobierno, es responsabilidad del Gobierno, implica a todas las Administraciones Públicas y precisa la colaboración de la sociedad en su conjunto.*
>
> *Estrategia Nacional de Seguridad.*

Las conclusiones de nuestro trabajo van en línea con los tiempos. Es necesario un planteamiento de concienciación en materias de *ciberseguridad* de la sociedad civil y de la Administración acerca de los riesgos que les amenazan. La necesaria colaboración de las diferentes Administraciones Públicas y de la sociedad civil es fundamental para la formación de una conciencia nacional de *ciberseguridad.* A pesar de lo doloroso de las crisis, quizás sean estas las que permitan cambios de estructuras que en tiempos de bonanzas se consideran impensables. Las estructuras burocráticas tienden a su perpetuación independientemente de aquellos que las habitan, perviviendo en el tiempo. Las crisis sistémicas proveen el cambio y la evolución: gracias a la crisis indagamos en la salida de ella y nos convertimos en críticos de nuestra forma tradicional de comportamiento.

Para asegurar la resiliencia del ciberespacio, uno de los pilares básicos en la Estrategia Europea de Ciberseguridad, la UE aboga por una legislación y mejora de la concienciación en materia de seguridad. En el ámbito de la legislación, propone la creación de autoridades, a nivel nacional de cada estado miembro, de seguridad de las redes y de la información (sus siglas en inglés NIS). Las entidades a nivel UE ya han sido creadas y tendrán un papel de coordinación, sirviendo de puente entre las diferentes entidades a nivel nacional. Así mismo, la UE estima necesario la regulación de la gestión de los sectores de la energía, transporte, banca, bolsa y proveedores de servicios de Internet desde la perspectiva de hacer una gestión apropiada del riesgo y de informar sobre incidentes de seguridad que impacten en la continuidad de sus servicios esenciales y suministro de bienes. De esta forma, se ha desarrollado en España la Ley 8 /2011 de Protección de Infraestructuras Críticas, la cual, en su preámbulo, recoge la voluntad por parte del legislador de armonizar con la doctrina europea e internacional en esta materia:

> *Los estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.*
>
> *En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.*
>
> *Hasta tal punto es así, que cualquier interrupción no deseada –incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados– podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.*
>
> *Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección, se hace imprescindible, por un lado, catalogar el conjunto de aquellas que prestan servicios esenciales a nuestra*

sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones... una comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa Europeo de Protección de Infraestructuras Críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network, CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114 del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos estados que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las comunidades autónomas.

En consecuencia, y dada la complejidad de la materia y su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las

> *estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a este como órgano responsable del sistema.*
>
> *La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquellas. Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.*

En Estados Unidos, el presidente Obama, consciente del riesgo que conllevan los *ciberataques* a las infraestructuras críticas, firmó en febrero de 2013 un decreto con fuerza de ley de *ciberseguridad* que permite al Gobierno compartir información sobre *ciberamenazas* con empresas privadas, específicamente proveedores de infraestructura, haciendo hincapié en la necesidad que tiene el país de enfrentar la amenaza de los *ciberataques*. Obama también llamó al Congreso a aprobar nuevas leyes para darle a nuestro Gobierno una mayor capacidad de asegurar nuestras redes y desalentar los ataques.

> *Sabemos que los hackers roban la identidad de las personas y se infiltran en los correos privados. Sabemos que países extranjeros y empresas roban nuestros secretos corporativos. Ahora nuestros enemigos también están buscando obtener la habilidad de sabotear nuestra red eléctrica, nuestras instituciones financieras y nuestros sistemas de control aéreo. No podemos mirar hacia atrás en el futuro y preguntarnos por qué no hicimos nada ante las amenazas reales a nuestra seguridad y economía.*

La *ciberseguridad* va relacionada inherentemente al riesgo. Por lo que respecta al concepto de riesgo, podemos afirmar que es un constructo social, dinámico y cambiante que requiere para su prevención y miti-

gación de dos herramientas básicas, el conocimiento y la comunicación (información y formación). Es un proceso que permite identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de las amenazas, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse, incluyendo la comprensión que en términos sociales se requiere de la participación de los diversos estratos, sectores de interés y grupos representativos de conductas y modos de vida (incluso de ideologías y de perspectivas del mundo, la vida o la religión) para comprender cómo se construye un riesgo social, colectivo, con la concurrencia de los diversos sectores de una región, sociedad, comunidad o localidad concreta.

En el ámbito de las tecnologías de la información, hace tiempo que se ha asumido la necesidad de convivir con un nivel de riesgo ya que la seguridad total o absoluta no existe. El grado de complejidad de las tecnologías de la información y las comunicaciones ha aumentado considerablemente y cada vez es más difícil administrar el riesgo adecuadamente y, por tanto, controlarlo. En todos estos casos lo que se requiere es revisar el análisis de riesgos del nuevo escenario y tomar rápidamente decisiones correctivas que mitiguen el impacto y permitan salir lo antes posible del escenario de crisis en que nos hemos visto envueltos.

En definitiva, el nuevo enfoque supone, por una parte, realizar los análisis de riesgos entendiendo los ataques posibles (tiempo, capacidad del atacante, progreso del ataque) y, por otra parte, disponer de una capacidad de gestión que pueda informar adecuadamente a los que tienen que tomar decisiones preventivas y reactivas de forma que protejamos no los componentes, sino los servicios finales, sean relativos a la administración electrónica o a los servicios públicos esenciales que, a fin de cuentas, están fuertemente interrelacionados.

Hay que ser sensibles a las responsabilidades, individuales y colectivas, en el campo de la *ciberseguridad*. Las personas poseen una percepción de lo que es la «seguridad ciudadana», de su necesidad y de las implicaciones que una deficiente seguridad ciudadana puede tener para su vida diaria y el ejercicio de sus derechos. Ello viene dado por el conocimiento que poseen sobre las amenazas a esta seguridad, derivadas fundamentalmente de las actividades delictivas más comunes.

Además, en la sociedad de la comunicación en la que vivimos, la alarma social y el estado de opinión pública subsiguiente harían muy difícil para las autoridades la pervivencia de una situación degradada de la seguridad ciudadana. De lo anterior se deduce que es necesario mantener la seguridad ciudadana y que la conciencia de seguridad de la población es importante para mantenerla. Por otra parte, esta conciencia requiere necesariamente del conocimiento de las amenazas a su seguridad por parte de los ciudadanos. La necesidad de crear en el ciudadano una con-

ciencia de *ciberseguridad* es un elemento fundamental de toda estrategia de *ciberseguridad*. Se trata, como se ha dicho anteriormente, de ser conscientes de las amenazas y la complejidad del ciberespacio, así como de asumir las responsabilidades individuales en el campo de la *ciberseguridad*. En resumen, se trata de concienciar al ciudadano para que «habite» el ciberespacio haciendo un uso seguro de las numerosas posibilidades que se le ofrecen.

Si empezamos a nivel nacional, es lógico que el Gobierno se muestre concienciado y sienta la necesidad –y así lo ha mostrado en diferentes ocasiones en los últimos años mediante la publicación de diferentes documentos oficiales sobre política y estrategia de seguridad nacional, en los que hace mención de la seguridad informática– de desarrollar una estrategia nacional de *ciberseguridad* y de fomentar la cultura de *ciberseguridad* y la *ciberurbanidad*. Bajo esta premisa, se desarrolló la Estrategia de Seguridad Nacional de 2011, que sirvió de base para la Estrategia Nacional de Seguridad de mayo de 2013. Pero no es suficiente que el Gobierno esté concienciado, es necesario que todos los altos cargos recogidos en la Ley 5/2006, de 10 de abril, *de regulación de los conflictos de intereses de los miembros del Gobierno y de los altos cargos de la Administración General del Estado* (AGE), y los cargos directamente subordinados a los mismos estén concienciados para que sea factible hacer campañas de concienciación en la AGE susceptibles de tener éxito. La necesidad de comunicación y conocimiento (toma de conciencia) es mayor en los niveles jerárquicos superiores del personal de las Administraciones Públicas, incluido el nivel político, pues la toma de decisiones en relación con la *ciberseguridad* debe tener una buena ubicación para que las prioridades puedan ser adecuadas y el eterno equilibrio entre seguridad y eficacia pueda ser alcanzado.

Derivada de la política de *ciberseguridad*, debe establecerse una estrategia e iniciar campañas de concienciación de *ciberseguridad.* El Spanish Cyber Security Institute (SCSI), en su informe *La ciberseguridad nacional, un compromiso de todos,* deja muy claro que el estado de concienciación en *ciberseguridad* de la sociedad civil es muy bajo, y sobre las campañas desarrolladas por el INTECO, el CCN y el propio SCSI, «de momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil», y enumera una serie de causas que divide en cuatro grupos: «organizacionales, operacionales, jurídicas y políticas». De entre las causas enumeradas en el citado informe, quiero resaltar las siguientes:

> *Escaso protagonismo de los actores privados en materia de ciberseguridad. La ciberseguridad nacional, hoy en día, es un sistema cerrado y exclusivo de los actores gubernamentales. En la actualidad, más del 80% de las infraestructuras críticas de nuestro país son propiedad, están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales). Por tanto, la aportación del sector privado al proceso de construcción de la ciberseguridad nacional resulta esencial.*

Ausencia de una política estatal en materia de ciberconcienciación y cibereducación. Muchos países de nuestro entorno están desarrollando ambiciosas políticas en materia de ciberconcienciación y ciberseguridad como eje fundamental para la creación de una cultura de ciberseguridad. Estas políticas han sido desarrolladas e impulsadas, en primera instancia, por el sector privado y, posteriormente, han recibido un fuerte apoyo gubernamental.

En este caso, cabe destacar una doble función, por un lado, concienciar y educar al conjunto de la ciudadanía de los riesgos del ciberespacio y, por otro, identificar futuros talentos en el campo de la ciberseguridad dentro de la comunidad escolar y universitaria.

En España, INTECO y el CCN disponen de programas de ciberconcienciación y ciberseguridad. Desde el sector privado, organismos como el ISMS Forum Spain han lanzado su propia campaña de ciberconcienciación bajo la denominación protegetuinformacion.com. De momento, estas iniciativas tienen una repercusión insuficiente en la sociedad civil.

Ausencia de políticas específicas para el I+D+i nacional en materia de ciberseguridad. No existen políticas, programas o iniciativas para el I+D+i de ámbito nacional que promuevan y faciliten actividades en materia de ciberseguridad, lo que contrasta con el gran protagonismo que a nivel europeo el nuevo marco de trabajo del Horizonte 2020 (continuación del 7.º Programa Marco) otorga a la ciberseguridad.

Las labores de concienciación desarrolladas por las empresas privadas tienen una difusión limitada, empujan a la iniciativa pública, pero es, una vez más, la colaboración público-privada en esta materia es la que puede permitir que no sea un esfuerzo limitado en el tiempo sino que se convierta en una estrategia continuada que vaya íntimamente relacionada con riesgos y amenazas en continuo desarrollo.

En la actualidad, los ciudadanos y muchas empresas tienen intereses que defender frente al *cibercrimen*, fundamentalmente estafas, fraudes, acoso, robo de información, incluida información comprometedora, y similares, pero hay muy poco interés en la defensa colectiva de los intereses de todos. Además, como se ha repetido anteriormente, hay poca conciencia de las amenazas que nos rodean como colectividad en el ciberespacio y menos aún de que podemos ser usados por esas amenazas para encubrirse. Como las amenazas son difíciles de percibir por su propia naturaleza, los ciudadanos tienen dificultades para sentir la necesidad de conciencia de *ciberseguridad.* Sí que pueden percibir algo más la amenaza que supone el *cibercrimen* por su incidencia en su imagen y en su propia economía.

Para desarrollar una conciencia de *ciberseguridad,* es necesario conocer las amenazas y los riesgos y asumirlos, en el sentido de aceptarlos y

enfrentarlos, nunca en el sentido de conformidad y pasividad ante los mismos: comunicar las incidencias, formar en materias de *ciberseguridad* y la necesaria adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio.

Las escuelas, institutos y universidades juegan un papel primordial en la creación de conciencia de *ciberseguridad*, que será nacional cuando alcance a la mayor parte de la población. Para conseguir la participación de los docentes, es necesario primero concienciarlos y formarlos en *ciberseguridad*, aunque los resultados de la actividad de las instituciones de enseñanza se verán a medio y largo plazo. La conciencia de *ciberseguridad* puede plasmarse en buenas prácticas informáticas o en algo más amplio que podría llamarse *ciberurbanidad* o *cibereducación* y que sería una extensión de las normas y usos de la buena educación al ciberespacio.

Para obtener resultados a corto plazo, es imprescindible que las instituciones de la sociedad civil y los medios de comunicación en todos sus formatos se involucren. Para ello es necesario que los dirigentes de esas instituciones se conciencien de la necesidad de la *ciberseguridad*. En cuanto a los medios de comunicación, los dirigentes tienen un doble papel: concienciarse y concienciar al personal que trabaja en sus medios.

El papel de la sociedad civil es fundamental en la concienciación a corto plazo de todos los ciudadanos y complementa a la obtenida a medio y largo plazo. La necesidad de concienciación ha sido reconocida en la Estrategia Nacional de Seguridad recientemente aprobada, la cual tiene entre sus líneas estratégicas relacionadas con la *ciberseguridad* «la implantación de una cultura de *ciberseguridad* sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento».

Los esfuerzos de concienciación deberían seguir haciendo hincapié en la disponibilidad de información clara que pueda ser entendida por todos los participantes y, en especial, por aquellos que carecen o poseen mínimos conocimientos técnicos. Dada la constante naturaleza cambiante del *malware*, las actividades de concienciación deberían ser revisadas o actualizadas regularmente para que siguieran siendo efectivas, lo que ayudaría a mejorar la conducta y prácticas *online* de usuarios así como su capacidad para protegerse de los *ciberataques*.

Los programas de «concienciación» no solo deben concienciar a las personas sino también formarlas y mostrar suficientes casos prácticos en los que se pueda apreciar. Aumentar la concienciación no es un ejercicio único, es un proceso continuo que provoca un cambio cultural que con el tiempo se irá integrando en el día a día del organismo. Para que un programa de concienciación en seguridad tenga éxito, hay dos elementos

clave que son necesarios: la participación de la dirección y el establecimiento de objetivos claros y medibles. Tanto en la empresa privada como en la empresa pública ha de seguirse una línea clara y definida en materias de concienciación y formación.

Los mensajes de concienciación de seguridad necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes, que se han recibido y entendido, se debe tener en cuenta las particularidades de cada organización y su entorno de trabajo.

El enfoque puede diferir de una organización a otra, pues la forma más eficaz de aumentar la concienciación en una organización dependerá de la cultura de la organización. Llegados a este punto, y sabiendo que el factor humano es siempre el eslabón más débil de la cadena de la seguridad, toca abordar cómo las empresas pueden difundir a lo largo de toda su organización los conceptos de *ciberseguridad* analizados en los apartados anteriores para asegurarse de que los diferentes miembros de la misma disponen del conocimiento adecuado, según su rol y responsabilidad, para asegurar una adecuada conciencia de la situación de la empresa en el ciberespacio que permita a esta garantizar su éxito en este nuevo medio.

Para ello, se debe analizar cómo se puede implantar un programa de concienciación de *ciberseguridad* como herramienta mediante la cual difundir el conocimiento sobre los riesgos de *ciberseguridad* y las posibles contramedidas para paliarlos, para así asegurar la consecución de los objetivos de concienciación citados anteriormente. Una campaña de concienciación orientada a los empleados debe tener presente los diferentes aspectos del problema de la *ciberseguridad.* Aunque cualquier acción es positiva, es realmente necesario que se planifiquen y detallen los objetivos a conseguir.

La concienciación y la formación ayudan a desarrollar una estrecha relación de trabajo entre las áreas y unidades de los organismos y los departamentos TIC, proporcionando un lenguaje y procesos comunes que se pueden utilizar para desarrollar una protección efectiva de los activos de la organización. Aumentar la concienciación es potencialmente la acción más valiosa en la tarea continua de la seguridad. Aumentar la concienciación consigue que todo el personal pertinente tenga suficiente conocimiento de los riesgos y del impacto potencial en el negocio o función de los fallos de seguridad. Los profesionales y los ciudadanos necesitan saber qué hacer para prevenir los ataques y qué hacer en caso de un incidente.

Es esencial que cualquier programa de concienciación de seguridad en un organismo esté correctamente planificado, ya que una sucesión de intentos mal planificados y mal ejecutados pueden obstaculizar los programas de seguridad. Tener un objetivo específico de concienciación centrará los esfuerzos de difusión del mensaje clave en el público apro-

piado y permitirá medir el éxito del programa. Integrar la seguridad en cualquier organización conlleva tiempo y el mejor enfoque es centrarse en los mensajes clave y construir lentamente y en profundidad la concienciación.

En el caso de la seguridad en la Administración Pública, se cuenta con el ENS (Esquema Nacional de Seguridad) que introduce los elementos comunes que han de guiar la actuación en materia de seguridad de las tecnologías de la información. Su finalidad es crear la confianza necesaria en el uso de la administración electrónica por parte de los ciudadanos y permitir el cumplimiento por parte de la Administración de la obligación de prestar acceso electrónico y trámites públicos. En el ENS, se concibe la seguridad como una actividad integral en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

En la Administración Pública española hay comparativamente pocos recursos diseñados específicamente para la formación en seguridad. Los esfuerzos de concienciación deberían seguir haciendo hincapié en la disponibilidad de información clara que pueda ser entendida por todos los participantes y, en especial, por aquellos que carecen o poseen mínimos conocimientos técnicos. Dada la constante naturaleza cambiante del *malware*, las actividades de concienciación deberían ser revisadas o actualizadas regularmente para que siguieran siendo efectivas, lo que ayudaría a mejorar la conducta y prácticas *online* de usuarios así como su capacidad para protegerse de los ataques digitales.

La conciencia de *ciberseguridad* está presente a nivel internacional: todos los países están desarrollando su política de *ciberseguridad* y los organismos internacionales implicados en la seguridad están desarrollando normativas y políticas que permitan afrontar este nuevo escenario donde los desarrollos normativos son escasos y las acciones presentan situaciones no contempladas históricamente. Es comúnmente aceptado que el desarrollo de las tecnologías de la información y las comunicaciones ha hecho del ciberespacio un recurso vital para el desarrollo de la sociedad actual ya que favorece la relación entre personas, empresas y Administración, convirtiéndose en el punto crítico para la prestación de servicios esenciales para el ciudadano.

La necesidad de colaboración entre estados es fundamental ante un aumento del nivel de exposición a sus amenazas y vulnerabilidades. Por tanto, la relevancia de las redes de comunicaciones en el mundo actual lleva asociada, de manera inseparable, la necesidad de protegerlas ante los incidentes de cualquier naturaleza que puedan alterar su operación, ya que las consecuencias de la interrupción o alteración de las redes de

comunicaciones podrían afectar gravemente a funciones sociales fundamentales, tal y como reconoce la recientemente aprobada Estrategia Nacional de Seguridad: «España está expuesta a los *ciberataques,* que no solo generan elevados costes económicos sino también, y lo que es más importante, la pérdida de confianza de los ciudadanos en unos sistemas que, en la actualidad, resultan críticos para el normal funcionamiento de la sociedad».

Esto se ha reflejado a nivel internacional en las correspondientes estrategias nacionales de *ciberseguridad*. El coste estimado del *cibercrimen* a nivel mundial para el 2012 se ha estimado en tres trillones de dólares. Los fenómenos delictivos y de ataque son transnacionales, así que la colaboración entre países para combatir estas amenazas es fundamental. Ataques contra las empresas y contra los países nos hacen replantearnos nuestras políticas de seguridad y defensa; los ataques contra la soberanía nacional de cada país obligan a replantearse los procedimientos de defensa y de respuesta ya que el escenario ha cambiado sensiblemente.

Es necesario desarrollar normas que permitan el respeto a los derechos fundamentales de libertad de expresión y asociación y que protejan el derecho a la propiedad intelectual de empresas, de personas y de Estados; desarrollo de normas que permitan la lucha contra los *ciberdelincuentes*, asegurando el estado de derecho y evitando la creación de santuarios para estos delincuentes. Parece existir una práctica unanimidad a la hora de indicar la necesidad de negociar acuerdos internacionales que regulen el ciberespacio; peor parece la existencia de diferencias insalvables en cuanto a qué deberían incluir esos acuerdos, el carácter de los mismos y las organizaciones de referencia.

Más de una docena de organizaciones internacionales –incluyendo las Naciones Unidas, el G-8, la OTAN, el Consejo de Europa, OSCE, el foro Cooperación Económica Asia-Pacifico, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, la Unión International de Telecomunicaciones (UIT) y la Organización Internacional de Normalización (ISO)– están involucradas en *ciberseguridad*. EE. UU. y Rusia tienen sus propias organizaciones de referencia, el Consejo de Europa y OSCE en el caso norteamericano y Naciones Unidas en el ruso, y ambos se bloquean respectivamente en sus propuestas. En cualquier caso, no debemos perder la esperanza de que las grandes *ciberpotencias* lleguen a un acuerdo que permita fomentar la confianza y aumentar la transparencia reduciendo los crecientes riesgos asociados con los cada vez más numerosos y cada vez más complejos *ciberataques*.

En cualquier caso, se tienen que mantener unos valores esenciales, como es que todo país tiene el derecho a la autodefensa contra actos de agre-

sión en el ciberespacio, autodefensa enfocada en el mantenimiento del funcionamiento de la red global y en la mejora de la *ciberseguridad.*

Otros elementos a tener en cuenta a la hora de redactar normas son: interoperabilidad global, estabilidad de la red y libre flujo de información, acceso fiable a todo individuo y presencia de grupos distintos del Gobierno en la gobernanza de Internet, abierta a actores no gubernamentales.

La *ciberamenaza* se extiende y acrecienta por una falta de normativas internacionales, la dificultad a la hora de atribuir ataques, barreras de acceso débiles y una facilidad relativa para desarrollar capacidades de ataque potentes. Nuestra capacidad de operar en el ciberespacio dependerá de la colaboración entre agencias estatales, no gubernamentales, industria y actores internacionales en el desarrollo de nuevas capacidades, organizaciones y normas, de manera que seamos capaces de proporcionar un amplio abanico de posibilidades para asegurar nuestro propio acceso y uso del dominio del ciberespacio y permitir la persecución de los actores maliciosos. Es necesario mejorar las capacidades de detección, disuasión, bloqueo de acceso y defensa en varias capas (1).

Afirma la OCDE en su informe sobre *Futuros Shocks Globales* (2):

> *A menos que el ritmo de los avances en la ciencia forense cibernética alcance la creciente facilidad de despliegue y la sofisticación de los ciberataques deliberados, seguirá siendo extremadamente difícil para las víctimas conocer la identidad de un atacante –problema de la atribución–. Esto quiere decir que una doctrina de defensa basada en la disuasión es menos probable que tenga éxito, y que ciertas partes malignas que actualmente carecen de la capacidad para poner en marcha un ataque a gran escala con éxito en el futuro pueden hacerlo.*

Otro informe, también publicado por la OCDE, *Reducción del riesgo sistémico en ciberseguridad*, afirma que la cooperación internacional es una de las claves para reducir los riesgos de *ciberseguridad*. Los ataques contra los sistemas conectados a la Internet pública pueden originarse en cualquier parte de esa red. Los fallos en las infraestructuras de información esenciales en una nación pueden transmitirse en cascada en los sistemas dependientes en cualquier parte, pero aunque muchos organismos internacionales han emitido declaraciones de principios de apoyo mutuo y protección, no existe un mecanismo sustantivo de gobernanza internacional para resolver crisis relacionadas con el ciberespacio distintas de la estructura FIRST/CERT dominada por ingenieros (3).

Para establecer una política de ciberespacio coherente a nivel internacional y promover los valores de la UE es necesario continuar trabajando en

la línea de la denominada Convención de Budapest, en la que se acordó la aplicación de las leyes internacionales al ciberespacio. En cuanto a la promoción de los valores de la UE, se apoyará a terceros países en su deseo de dar acceso a las personas a Internet. Además, se hará un seguimiento de aquellos productos que puedan ser utilizados para la vigilancia o censura de forma masiva.

Las principales mejoras que se podrían hacer sería aumentar el número de estados que han ratificado el Convenio sobre la *Ciberdelincuencia* y fortalecer los mecanismos de cooperación internacional y desarrollo de capacidades. Sería particularmente útil que países con un gran número de usuarios de Internet, como Rusia y China, ratifiquen la Convención sobre la *Ciberdelincuencia*. Pero esto puede requerir flexibilidad por parte de los estados parte actuales para responder a las preocupaciones sobre soberanía de Rusia y otros. La OSCE, la mayor organización de seguridad del mundo, ha estado activa en la *ciberseguridad*, principalmente desde la perspectiva de *ciberterrorismo*. En 2010, en un taller OSCE sobre un enfoque global para mejorar la *ciberseguridad,* los delegados coincidieron en que la función de la OSCE en la *ciberseguridad* mundial necesita ser redefinida:

> *Preocupados por la complejidad de las actividades maliciosas en línea, la OSCE ha decidido intensificar la acción mediante la mejora de la cooperación internacional en la lucha contra el uso de Internet con fines terroristas, para considerar la adopción de todas las medidas apropiadas, para proteger las infraestructuras críticas y redes de información vitales contra la amenaza de ciberataques, al considerar ser parte e implementar sus obligaciones en virtud de los instrumentos legales internacionales y regionales existentes; y para explorar la posibilidad de una participación más activa de las instituciones de la sociedad civil y el sector privado en la prevención y lucha contra el uso de Internet con fines terroristas (4).*

Se han definido cinco prioridades en la Estrategia de Ciberseguridad de la UE: conseguir *ciberresiliencia*, reducir drásticamente el crimen organizado, desarrollar una política en *ciberdefensa* y capacidades en materia de seguridad, desarrollar recursos industriales y tecnológicos para *ciberseguridad* y establecer una política de ciberespacio coherente a nivel internacional y promover los valores de la UE.

Así es recogido en el informe del secretario general de la OSCE:

> *Desde 2009, la OSCE ha promovido un enfoque más amplio de la ciberseguridad. Este enfoque se basa en el entendimiento de que el uso generalizado de Internet por los terroristas, traficantes y delincuentes hace cada vez más difícil el desarrollo de respuestas eficaces a las amenazas transnacionales sin promover un ciberespacio más seguro. Un enfoque integral de la ciberseguridad debe: (a) fortalecer la segu-*

ridad nacional; (b) hacer frente a los delitos cibernéticos; (c) inhibir la utilización de Internet por terroristas; (d) responder a una amplia variedad de riesgos y amenazas, incluyendo peligros político-militares; (e) permitir a las autoridades competentes la protección de una amplia gama de objetivos que van desde el usuario particular de Internet a las infraestructuras críticas, y (f) salvaguardar la Internet como un espacio de libre expresión y de reunión.

Uno de los elementos fundamentales de la *ciberseguridad* es la *ciberdefensa.* España acaba de formar el Mando de Ciberdefensa: mediante Orden Ministerial 10/2013, se crea dentro del Estado Mayor de la Defensa el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD). La *ciberdefensa* pasará así a ocupar un lugar importante en la actividad de las Fuerzas Armadas, de forma similar a como ocurre ya en otros países que cuentan con organismos similares, estando a la cabeza de todos ellos el US Cyber Command creado por el Pentágono en 2009 frente a lo que Washington ha definido como el «campo de batalla del futuro».

El ámbito de actuación del MCCD son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la defensa nacional. La misión del MCCD es el planeamiento y la ejecución de las acciones relativas a la *ciberdefensa* militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional. Las funciones serán las siguientes:

- Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.
- Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.
- Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques.
- Obtener, analizar y explotar la información sobre *ciberataques* e incidentes en las redes y sistemas de su responsabilidad.
- Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional.

- Dirigir y coordinar, en materia de *ciberdefensa*, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional.
- Cooperar, en materia de *ciberdefensa*, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de *ciberseguridad* en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.
- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de *ciberdefensa*.

Se configura la *ciberdefensa* como un elemento fundamental de los intereses del Estado. La necesidad de una conciencia de *ciberdefensa* en España será un trabajo a realizar después del lanzamiento del proyecto a finales del verano. La concienciación en esta materia corresponderá al Mando de Ciberdefensa, así como los planes de capacitación y el desarrollo de las tecnologías a utilizar.

Me gustaría terminar la reflexión volviendo a la Estrategia Nacional de Seguridad recogiendo su primer párrafo del prólogo: «la seguridad es un fundamento esencial para el desarrollo de una sociedad libre», y cito a Félix Arteaga quien, con referencia a la Estrategia, afirma:

> *Las estrategias son documentos con vocación transformadora de las políticas públicas cuya labor comienza –y no termina– con su aprobación, por ello en su valoración se debe diferenciar el contenido de la misma de los mecanismos de puesta en marcha que, a la larga, serán los que demuestren la validez o irrelevancia del documento aprobado. En relación con el contenido, la nueva Estrategia es bastante continuista respecto a la anterior, lo que refleja una vocación de consenso político y de visión de Estado a propósito de la seguridad nacional entre los dos grandes partidos políticos digna de destacar en estos días. Coinciden en identificar como riesgos el terrorismo, los conflictos armados, el crimen organizado, la inseguridad económica y financiera, las «ciberamenazas», los flujos migratorios no controlados, las armas de destrucción masiva, la vulnerabilidad energética y de los servicios e infraestructuras críticas o las emergencias y catástrofes naturales; a los que se añaden ahora el espionaje y la inseguridad marítima. Las coincidencias muestran una visión compartida del contexto estratégico que se prolonga en las líneas estratégicas para afrontar esos riesgos.*

Ambas estrategias comparten una visión integral de la seguridad, transversal, transfronteriza, abierta a nuevos actores públicos y privados para proporcionar la libertad, la seguridad, el bienestar y el funcionamiento de los servicios que precisan los ciudadanos. También comparten la insuficiencia de las estructuras y procedimientos de coordinación existentes para afrontar problemas complejos, por lo que acercan la responsabilidad a la Presidencia del Gobierno:

> *Es desde las más altas instancias del Estado desde donde se pueden marcar las estrategias a seguir y el desarrollo de estas, siendo el modelo de gobernanza un punto clave para su eficaz puesta en funcionamiento. La Agenda Digital para España es un elemento fundamental para desarrollar la confianza en el uso de Internet y de las tecnologías de la comunicación, el desarrollo de las infraestructuras, la inversión en I+D español y su internacionalización, y el desarrollo de una política de compra innovadora desde la Administración.*

Cabe destacar la Estrategia de *Ciberseguridad* Europea aprobada el 7 de Febrero de 2013, basada en cinco principios fundamentales: los valores esenciales de la Unión Europea, que se deben aplicar «tanto en el mundo digital como en el físico», la protección de derechos fundamentales, libertad de expresión, datos personales y privacidad, acceso para todos, gobierno eficiente y democrático de los grupos de interés y responsabilidad compartida.

> *El concepto de seguridad en el siglo XXI debe ser amplio y dinámico para cubrir ámbitos concernientes a la seguridad del Estado y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico y abarcan desde la defensa del territorio a la estabilidad económica y financiera o la protección de las infraestructuras críticas.*
>
> *Por otra parte, la respuesta a los riesgos y amenazas que comprometen la seguridad en nuestros días precisa de cooperación tanto en el plano nacional como en el multilateral. Las respuestas unilaterales y aisladas no son eficaces, por su carácter incompleto y parcial, frente a unos retos que exigen un enfoque multidisciplinar y una acción conjunta. Solo esta perspectiva abarca todos los aspectos potencial o realmente afectados.*
>
> *Los cambios y tendencias relativos al entorno de la seguridad, sus dimensiones y las respuestas que pide su preservación son factores que inciden en la visión de la seguridad nacional. España se sitúa junto a los países más avanzados en la materia y concibe la seguridad de una manera integral, acorde con las transformaciones globales que repercuten en el Estado y la vida diaria del ciudadano. En esta línea, la crisis financiera y económica que actualmente afecta a España, a la zona euro y a parte importante de las economías mundiales represen-*

ta uno de los mayores retos para la seguridad nacional y extrema la necesidad de ser eficientes en la respuesta.

Estrategia Nacional de Seguridad

Una política de Estado no solo debe ser abordada desde los poderes públicos; es fundamental, y en este caso de forma particular, colaborar con el sector privado en el entendimiento y el desarrollo de esta política que nos afecta a todos, puesto que la seguridad es una tarea compartida. El desarrollo de la Estrategia Nacional de Ciberseguridad necesitará de la implantación de una cultura de *ciberseguridad* sólida, concienciando a los ciudadanos, a las empresas y a la Administración de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento. Del mismo modo, siguiendo la política de *ciberseguridad* de la UE, se fomentará el desarrollo de tecnologías nacionales a través de un programa de I+D, así como la capacitación de profesionales en estas materias.

Bibliografía

1. *Estrategia Nacional Militar de los Estados Unidos de América.* Washington, EE. UU.: Joint Chief of Staff, 2011.
2. OCDE. *Future Global Shocks. Improving Risk Governance.* París: OCDE, 2011.
3. SOMMER, Peter y BROWN, Ian. *Reducing Systemic Cybersecurity Risk*. Informe OCDE, 2011.
4. OSCE_MC.DEC/7/06. *Decision No. 7/06. Countering the Use of the Internet for Terrorist Purposes.* Bruselas: OSCE, 2006.
5. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruselas: European Commission & High Representative of the European Union for Foreign Affairs And Security Policy, 2013.
6. KAGAN, Robert. *Paradise and Power: America and Europe in the New World Order.* Londres: Atlantic Books, 2004.
7. WEGENER, Henning. *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence Building Measures.* [En línea] 23 de agosto de 2012 [citado el 29 de marzo de 2013]. http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th/Wegener publication.docx.
8. BAILEY, Eric. *«Nothing Can Justify Torture»: An interview with Noam Chomsky on Obama's Human Rights Record.* [En línea] 12 de diciembre de 2012 [citado el 30 de marzo de 2013]. http://chomsky.info/interviews/20121212.htm.
9. *Cyberspace Policy Review.* Washington: The White House, 2011. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

10. *International Strategy for Cyberspace.* Washington: The White House, 2011.
11. BIDEN, Joseph R. *VP's remarks to London Cyberspace Conference.* Londres: The White House, 2011.
12. CLAPPER, James R. *Worldwide Threat Assessment of the US Intelligence Community 2013.* Washington D. C.: Office of the Director of National Intelligence, 12 de marzo de 2013.
13. ALEXANDER, Keith B. *Statement of general Keith B. Alexander Commander United States Cyber Command before the Senate Committee on Armed Services.* Washington: United States Cyber Command, 2013.
14. PELLERIN, Cheryl. American Forces Press Service. Cybercom Builds Teams for Offense, Defense in Cyberspace. [En línea] 12 de marzo de 2013 [citado el 30 de marzo de 2013]. http://www.defense.gov/news/newsarticle.aspx?id=119506.
15. KEHLER, C. R. *Statement of general C. R. Kehler Commander United States Strategic Command before the Senate Committee on Armed Services.* Washington: United States Strategic Command, 12 de marzo de 2013.
16. LEWIS, James Andrew. *Critical Questions for 2013: Global Challenges. What's Next in Cybersecurity?* [En línea] 25 de enero de 2013 [citado el: 30 de marzo de 2013]. Center for Strategic and International Studies. http://csis.org/publication/critical-questions-2013-global-challenges.
17. BUMILLER, Elisabeth. «Pentagon to Beef Up Cybersecurity Force to Counter Attacks», *The New York Times*. [En línea] 29 de marzo de 2013 [citado el 31 de marzo de 2013]. www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html.
18. GEERS, Kenneth. *Cyberspace and the changing nature of warfare.* [En línea] 27 de agosto de 2008 [citado el: 31 de marzo de 2013]. http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.
19. HEALEY, Jason y VAN BOCHOVEN, Leendert. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow.* Washington: The Atlantic Council of the United States, 2011.
20. PRINCE, Matthew. «The DDoS That Almost Broke the Internet». [En línea] 27 de marzo de 2013 [citado el 28 de marzo de 2013]. *Cloud Flare.* http://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet.
21. TIKK, Eneken. *Comprehensive legal approach to cyber security 2011.* Tarfu, Estonia: Faculty of Law, University of Tartu, 2011.
22. Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* [En línea] 16 de marzo de 2005 [citado el 31 de mar-

zo de 2013]. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

23. FROOMKIN, Michael. «Cybercrime Treaty Goes Live». *Discourse.net.* [En línea] 19 de marzo de 2004 [citado el 31 de marzo de 2013]. http://www.discourse.net/archives/2004/03/cybercrime_treaty_goes_live.html.
24. ARCHICK, Kristin. *CRS Report for Congress. Cybercrime: The Council of Europe Convention.* Washington: Congressional Research Service, 2004.
25. SCHJØLBERG, Stein y GHERNAOUTI-HÉLIE, Solange. *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for peace and Security in Cyberspace,* segunda edición. Oslo: AiTOslo, 2011.
26. [En línea] 16 de octubre de 2009 [citado el 31 de marzo de 2013]. EE. UU.: OSCE, 2013. https://dazzlepod.com/cable/09STATE107552/.
27. SCHNEIDER, Deborah. *United States Mission to the OSCE Cyber Security Keynote Address by Dr. Deborah Schneider, U. S. Department of State as delivered to the Joint FSC/PC.* Viena: OSCE, 2010.
28. SAFIRE, William. «The Farewell Dossier». *The New York Times.* [En línea] 2 de Febrero de 2004 [citado el 2 de enero de 2013]. http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?ref=williamsaire.
29. BROWN, Gary y POELLET, Keira. «The Customary International Law of Cyberspace», IV, 2012. *Strategic Studies Quarterly,* otoño de 2012, vol. 6, págs. 126-145.
30. STEPHENS, Bret. «The Limits of Stuxnet». *The Wall Street Journal.* [En línea] 18 de enero de 2011 [citado el 2 de enero de 2013]. http://online.wsj.com/article/SB10001424052748703396604576087632882247372.html.
31. PERTERMANN, Kerstin. *Conference Report: Challenges in Cybersecurity, Risks, Strategies, and Confidence-Building International Conference.* Hamburgo: Institute for Peace Research and Security Policy at the University of Hamburg, 2011.
32. VENTRE, Daniel. *La politique de cyberdéfense peut-elle être a-politique?* Paris: Ministère de la défense Délégation aux Affaires Stratégiques, 2013.
33. OBAMA, Barak. *Discurso sobre el estado de la Unión de Barack Obama.* Washington: The White House, 2013.
34. NEWMEYER, Kevin P. *Who should lead U.S. Cyber security efforts? PRISM*, 2012, vol. 3, n.º 2, págs. 115-126.
35. *Estrategia Española de Seguridad.* Madrid: Gobierno de España, 2011.
36. PÉREZ, Jesús. «Cómo Cyberbunker atacó a Spamhaus y casi se llevó a medio Internet por delante». *Security by Default.* [En línea] 28 de

marzo de 2013 [citado el 12 de mayo de 2013]. http://www.security-bydefault.com/2013/03/como-cyberbunker-ataco-spamhaus-y-casi.html.

37. VENTRE, Daniel. «Japon: stratégies de cyberdéfense, Multi-System and Internet-Security-Cookbook». *MISC,* 2012, n° 64, págs. 65-73.
38. BAGCHI, Sohini. «India needs more warriors in the cyber space». *Cxotoday.com.* [En línea] 3 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.cxotoday.com/story/india-needs-more-warriors-in-the-cyber-space/.
39. ZORZ, Zeljka. «India has a new National Cyber Security Policy». *Help net security organization.* [En línea] 10 de mayo de 2013 [citado el 12 de mayo de 2013]. http://www.net-security.org/secworld.php?id=14891.
40. FEDORENKO, Andrei. «The Fight Over the Draft. UN Convention on International Information Security». *Regulatory cyber security: The FISMA focus IPD.* [En línea] 15 de julio de 2012 [citado el 12 de mayo de 2013]. http://www.thecre.com/fisma/?p=2173.
41. *Information systems defence and security - France's strategy*. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 2011.

Composición del grupo de trabajo

Presidente:	**D. JUAN ANTONIO GÓMEZ BULE** *Presidente del Consejo Asesor de S21Sec*
Secretario-coordinador:	**D. JOSÉ TOMÁS HIDALGO TARRERO** *Coronel del Ejército del Aire*
Vocales:	**D. JOSÉ MANUEL ROLDÁN TUDELA** *General de división del Ejército de Tierra* *General jefe de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica*
	D. LUIS JIMÉNEZ MUÑOZ *Subdirector adjunto del Centro Criptológico Nacional* *Jefe del Área de Certificación del Organismo de Certificación*
	D. OSCAR PASTOR ACOSTA *Gerente de Seguridad de la Dirección de Seguridad y Defensa de ISDEFE*
	D. EMILIO SÁNCHEZ DE ROJAS DÍAZ *Coronel del Ejército de Tierra*

Relación de Monografías del CESEDEN

1. Clausewitz y su entorno intelectual. Kant, Guibert, Fichte, Moltke, Schlieffen, Lenin
2. Las Conversaciones de Desarme Convencional (CFE)
3. Disuasión convencional y conducción de conflictos: el caso de Israel y Siria en el Líbano
4. Cinco sociólogos de interés militar
5. Primeras Jornadas de Defensa Nacional
6. Prospectiva sobre cambios políticos en la antigua URSS. Escuela de Estados Mayores Conjuntos. XXIV Curso 91/92
7. Cuatro aspectos de la defensa nacional. (Una visión universitaria)
8. Segundas Jornadas de Defensa Nacional
9. IX y X Jornadas CESEDEN-IDN de Lisboa
10. XI y XII Jornadas CESEDEN-IDN de Lisboa
11. Anthology of the essays
12. XIII Jornadas CESEDEN-IDN de Portugal. La seguridad de la Europa Central y la Alianza Atlántica
13. Terceras Jornadas de Defensa Nacional
14. II Jornadas de Historia Militar. La presencia militar española en Cuba (1868-1895)

15. La crisis de los Balcanes
16. La Política Europea de Seguridad Común (PESC) y la Defensa
17. Second anthology of the essays
18. Las misiones de paz de la ONU
19. III Jornadas de Historia Militar. Melilla en la historia militar española
20. Cuartas Jornadas de Defensa Nacional
21. La Conferencia Intergubernamental y de la Seguridad Común Europea
22. IV Jornadas de Historia Militar. El Ejército y la Armada de Felipe II, ante el IV centenario de su muerte
23. Quintas Jornadas de Defensa Nacional
24. Altos estudios militares ante las nuevas misiones para las Fuerzas Armadas
25. Utilización de la estructura del transporte para facilitar el cumplimiento de las misiones de las Fuerzas Armadas
26. Valoración estratégica del estrecho de Gibraltar
27. La convergencia de intereses de seguridad y defensa entre las Comunidades Europeas y Atlánticas
28. Europa y el Mediterráneo en el umbral del siglo XXI
29. I Congreso Internacional de Historia Militar. El Ejército y la Armada en 1898: Cuba, Puerto Rico y Filipinas
30. Un estudio sobre el futuro de la no-proliferación
31. El islam: presente y futuro
32. Comunidad Iberoamericana en el ámbito de la Defensa
33. La Unión Europea Occidental tras Ámsterdam y Madrid
34. Iberoamérica, un reto para España y la Unión Europea en la próxima década
35. La seguridad en el Mediterráneo. Coloquios C-4/1999
36. Marco normativo en que se desarrollan las operaciones militares
37. Aproximación estratégica española a la última frontera: la Antártida
38. Modelo de seguridad y defensa en Europa en el próximo siglo
39. V Jornadas de Historia Militar. La aviación en la guerra española
40. Retos a la seguridad en el cambio de siglo. (Armas, migraciones y comunicaciones)
41. La convivencia en el Mediterráneo Occidental en el siglo XXI
42. La seguridad en el Mediterráneo. Coloquios C-4/2000
43. Rusia: conflictos y perspectivas

44. Medidas de confianza para la convivencia en el Mediterráneo Occidental
45. La cooperación Fuerzas de Seguridad-Fuerzas Armadas frente a los riesgos emergentes
46. La ética en las nuevas misiones de las Fuerzas Armadas
47. VI Jornadas de Historia Militar. Operaciones anfibias de Gallípoli a las Malvinas
48. La Unión Europea: logros y desafíos
49. La seguridad en el Mediterráneo. Coloquios C-4/2001
50. Un nuevo concepto de la defensa para el siglo XXI
51. Influencia rusa en su entorno geopolítico
52. Inmigración y seguridad en el Mediterráneo: el caso español
53. Cooperación con Iberoamérica en el ámbito militar
54. Retos a la consolidación de la Unión Europea
55. Revisión de la Defensa Nacional
56. Investigación, Desarrollo e innovación (I+D+i) en la Seguridad y la Defensa
57. VII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Génesis de la España contemporánea
58. La seguridad en el Mediterráneo. Coloquios C-4/2002
59. El Mediterráneo: Proceso de Barcelona y su entorno después del 11 de septiembre
60. La industria de defensa: el desfase tecnológico entre la Unión Europea y Estados Unidos de América
61. La seguridad europea y las incertidumbres del 11 de septiembre
62. Medio ambiente y Defensa
63. Pensamiento y pensadores militares iberoamericanos del siglo XX y su influencia en la Comunidad Iberoamericana
64. Estudio preliminar de la operación: Libertad para Irak
65. Adecuación de la defensa a los últimos retos
66. VIII Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). La organización de la defensa de la Monarquía
67. Fundamentos de la estrategia para el siglo XXI
68. Las fronteras del mundo iberoamericano
69. Occidente y el Mediterráneo: una nueva visión para una nueva época
70. IX Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). Las bases de la potencia hispana
71. Un concepto estratégico para la Unión Europea

72. El vínculo transatlántico
73. Aproximación a las cuestiones de seguridad en el continente americano
74. Defensa y Sociedad Civil
75. Las organizaciones internacionales y la lucha contra el terrorismo
76. El esfuerzo de defensa. Racionalización y optimización
77. El vínculo transatlántico en la guerra de Irak
78. Mujer, Fuerzas Armadas y conflictos bélicos. Una visión panorámica
79. Terrorismo internacional: enfoques y percepciones
80. X Jornadas de Historia Militar. De la Paz de París a Trafalgar (1763-1805). El acontecer bélico y sus protagonistas
81. Opinión pública y Defensa Nacional en Iberoamérica
82. Consecuencias de la guerra de Irak en el Mediterráneo Occidental
83. La seguridad en el Mediterráneo. Coloquio C-4/2004-2005
84. Hacia una política de cooperación en Seguridad y Defensa con Iberoamérica
85. Futuro de la Política Europea de Seguridad y Defensa
86. Una década del Proceso de Barcelona: evolución y futuro
87. El conflicto árabe-israelí: nuevas expectativas
88. Avances en tecnologías de la información y de las comunicaciones para la Seguridad y la Defensa
89. La seguridad en el Mediterráneo. Coloquio C-4/2006
90. La externalización en las Fuerzas Armadas: equilibrio entre el apoyo logístico propio y el externalizado
91. La adhesión de Turquía a la Unión Europea
92. La seguridad en el Mediterráneo: complejidad y multidimensionalidad
93. La situación de seguridad en Irán: repercusión en el escenario regional y en el entorno mundial
94. Tecnología y Fuerzas Armadas
95. Integración de extranjeros en las Fuerzas Armadas españolas
96. El mundo iberoamericano ante los actuales retos estratégicos
97. XI Jornadas de Historia Militar. La enseñanza de la historia militar en las Fuerzas Armadas
98. La energía y su relación con la Seguridad y Defensa
99. Prospectiva de Seguridad y Defensa: viabilidad de una unidad de prospectiva en el CESEDEN

100. Repercusión del actual reto energético en la situación de seguridad mundial
101. La evolución de la Seguridad y Defensa en la Comunidad Iberoamericana
102. El Oriente Próximo tras la crisis de El Líbano
103. Los estudios de posgrado en las Fuerzas Armadas
104. Las fronteras exteriores de la Unión Europea
105. La industria y la tecnología en la Política Europea de Seguridad y Defensa
106. De la milicia concejil al reservista. Una historia de generosidad
107. La Agencia Europea de Defensa: pasado, presente y futuro
108. China en el sistema de seguridad global del siglo XXI
109. Naciones Unidas como principal elemento del multilateralismo del siglo XXI
110. Las relaciones de poder entre las grandes potencias y las organizaciones internacionales
111. Las nuevas guerras y la polemología
112. La violencia del siglo XXI. Nuevas dimensiones de la guerra
113. Influencia de la nueva Rusia en el actual sistema de seguridad
114. La nueva geopolítica de la energía
115. Evolución del concepto de interés nacional
116. Sesenta años de la OTAN ¿Hacia una nueva estrategia?
117. La importancia geoestratégica del África Subsahariana
118. El Mediterráneo: cruce de intereses estratégicos
119. Seguridad Nacional y estrategias energéticas de España y Portugal
120. Las armas NBQ-R como armas de terror
121. El futuro de las relaciones Latinoamérica-Estados Unidos
122. La influencia social del islam en la Unión Europea
123. África ¿nuevo escenario de confrontación?
124. Las nuevas guerras: globalización y sociedad
125. El impacto de la crisis económica en el área de la Seguridad y la Defensa
126. El ciberespacio. Nuevo escenario de confrontación
127. En una sociedad posheroica: la transformación del paradigma militar
128. Los ámbitos no terrestres en la guerra futura: espacio
129. Valores y conflictos. Las claves culturales en el conflicto del siglo XXI
130. Análisis prospectivo de las operaciones de multipolaridad

131. Nuevas guerras. Nuevas paces
132. Valores y conflictos. Aproximación a la crisis
133. Análisis y evaluación de la estabilidad del Magreb
134. África: riesgos y oportunidades en el horizonte de 2035
135. Enfoque integral de la seguridad en el espacio marítimo español
136. El liderazgo en las Fuerzas Armadas del siglo XXI

Las *Monografías del CESEDEN* están disponibles en las blibliotecas especializadas y en el Centro de Documentación del Ministerio de Defensa.