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.

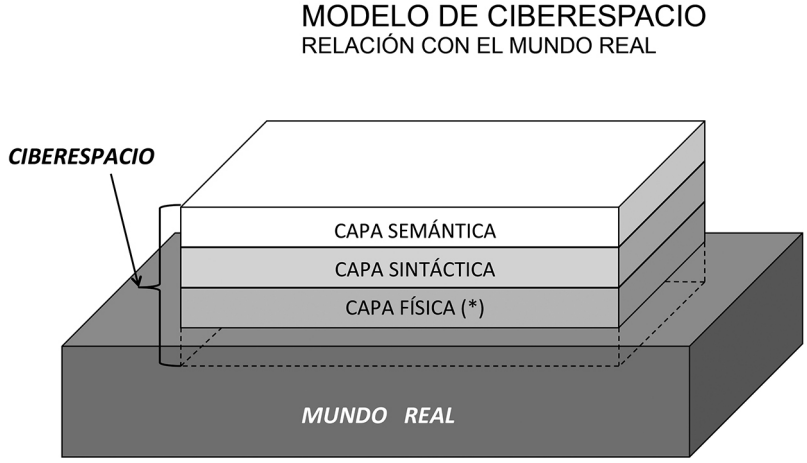
El modelo del Ejército de los Estados Unidos (4) es un modelo de tres capas (física, lógica y social) construido por cinco componentes (geográfico, red física, red lógica, *ciberpersonas* y personas reales). La capa física incluye el componente geográfico y el componente de red física; la capa lógica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

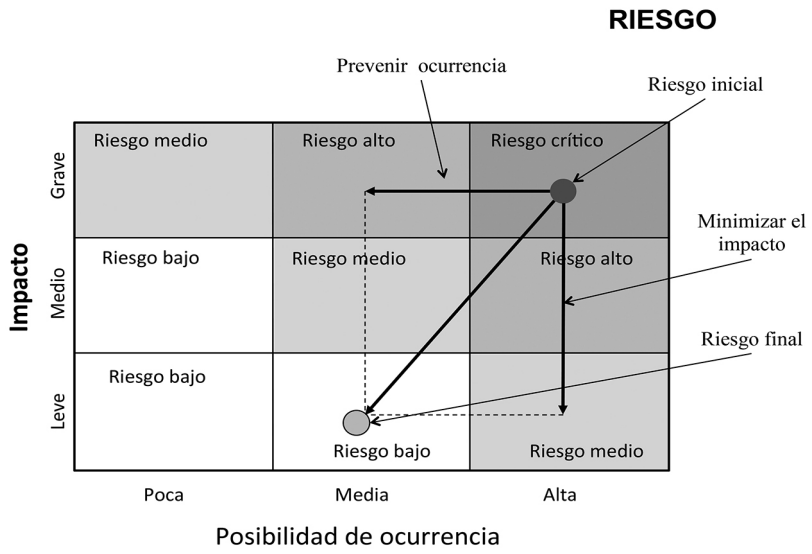


Figura 2.2: Riesgo (una rama del árbol de activos)

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

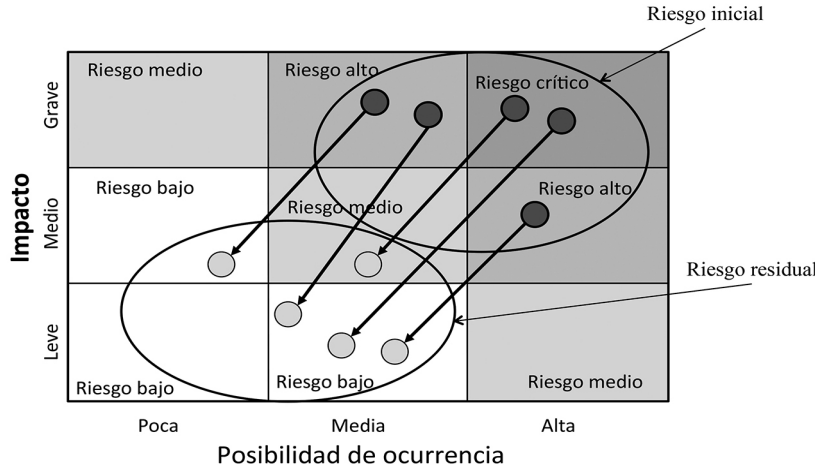


Figura 2.3: Reducción del riesgo del conjunto.

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.

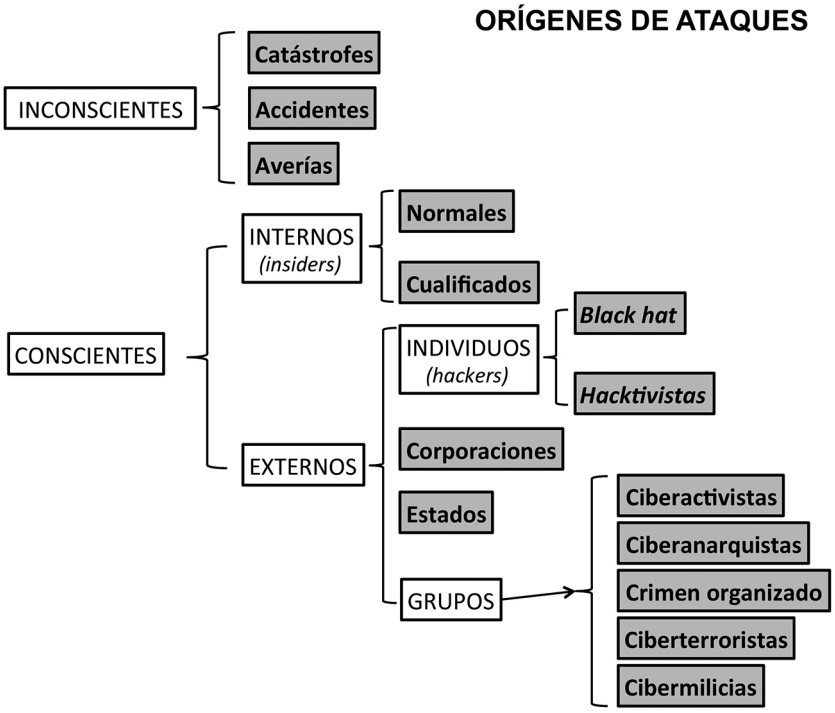


Figura 2.4: Orígenes de ataque.

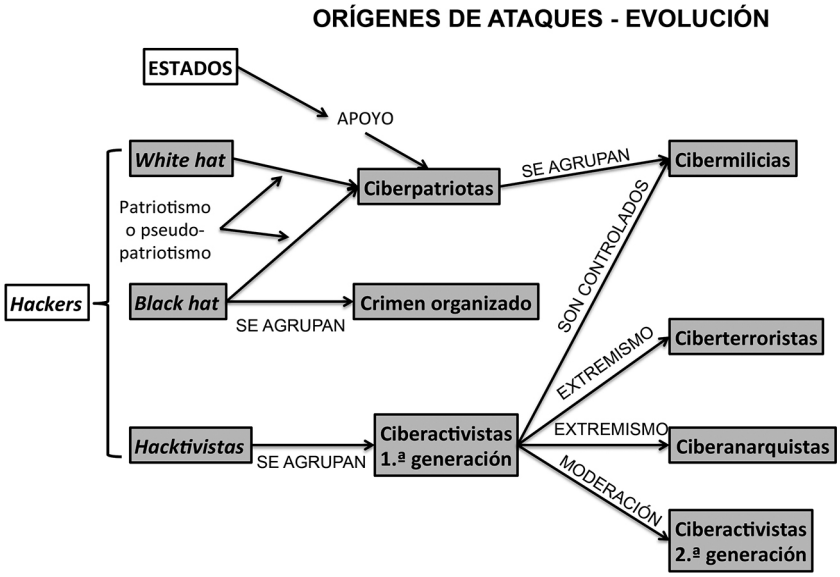


Figura 2.5: Orígenes de ataque, evolución.

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.

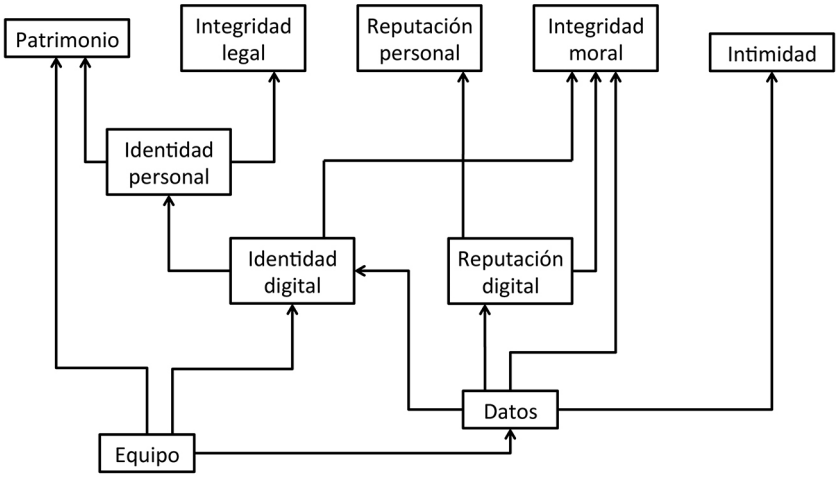


Figura 2.6: Árbol de activos.

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.