INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

INTRODUCCIÓN A LA PROTECCIÓN EN INTERNET

MÓDULO 2: AMENAZAS Y RIESGOS DE INTERNET

INTECO-CERT

Instituto Nacional
de Tecnologías
de la Comunicación

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

ÍNDICE

Módulo 2 – Estructura y contenido del módulo

En el primer módulo de este curso realizamos un breve recorrido a través del origen y evolución de Internet. Esto nos ha servido como punto de partida para comprender mejor cómo eran y cómo son las amenazas y riesgos que podemos encontrar en Internet y cómo ha sido su evolución hasta llegar al momento actual.

Como vimos, una de las principales motivaciones que están detrás de los incidentes de seguridad que se dan en la actualidad es la obtención de beneficio económico. Es más, detrás de muchos de estos incidentes de seguridad hay grupos criminales perfectamente organizados. De hecho, ya se habla de una industria del cibercrimen.

A lo largo del presente módulo, vamos a describir de forma detallada algunas de esas amenazas y riesgos actuales. Proporcionaremos al alumno información sobre cómo protegerse y la haremos en forma de enlaces a información que INTECO-CERT pone a disposición del usuario a través de su página web.

Como veremos, existen muchas amenazas y muy variadas pero afortunadamente también contamos con una gran gama de herramientas de seguridad gracias a la potente industria de la seguridad. No obstante, el usuario sigue siendo una pieza crítica y totalmente necesaria en la cadena de la seguridad y es fundamental que esté concienciado y formado.

Por otro lado, nos adentraremos en los problemas de la seguridad en las redes sociales, en las que los usuarios están expuestos a múltiples riesgos y amenazas. Por ello, es imprescindible hacer un uso adecuado de estos servicios y de otros que podemos encontrar en Internet.

Finalmente, hablaremos de un concepto llamado «seguridad en la nube», que hace referencia al hecho de que las organizaciones, las empresas y los usuarios tengan cada vez más información en Internet.

Los contenidos de este módulo se estructuran en los siguientes bloques formativos:

- **Amenazas y riesgos actuales**. Describiremos un conjunto de amenazas y riesgos que podemos encontrar en Internet, proporcionando recomendaciones y guías para protegernos.

- **Redes sociales**. Conoceremos cómo es la seguridad en el ámbito de las redes sociales, cuáles son las amenazas y riesgos que podemos encontrar en estas redes y cuáles son las medidas que debemos tomar para protegernos y hacer un uso adecuado de las mismas.
- **La seguridad en la nube**. Finamente, trataremos el concepto de «seguridad en la nube» y cómo afectan los nuevos usos y paradigmas de Internet y de la información a la seguridad, tanto de los usuarios como de las empresas y las organizaciones.

Amenazas y riesgos actuales

Las amenazas y riesgos que vamos a describir a continuación son las más representativas de las que podemos encontrar en Internet en la actualidad. Algunas de ellas llevan con nosotros desde los inicios de Internet y, en cambio, otras son completamente nuevas. De cualquier forma, trataremos de dar una visión lo más amplia posible de todas las amenazas existentes.

Al final de cada apartado, introduciremos un enlace a información sobre cómo protegerse de estas amenazas, información que INTECO-CERT pone a disposición de los ciudadanos y las empresas y proporcionaremos algunas recomendaciones básicas sobre cómo protegerse.

Subculturas

La amenaza

Las subculturas han existido desde del inicio de la tecnología. El ejemplo más conocido son los *hackers* pero, en realidad, existen muchos grupos que han nacido en torno a la tecnología, como los *phreakers*, una subcultura enfocada a las redes de telefonía, o los *crackers*, capaces de saltar las protecciones de los programas, o los *spamers*, responsables de inundar los buzones de correo electrónico con mensajes basura. Algunos ejemplos de subculturas son:

- ***hackers*** - acceden sin autorización a sistemas
- ***phreakers*** - ceden y utilizan sin autorización las líneas telefónicas
- ***crackers*** - rompen la protección de los programas para que puedan ser usados ilegalmente
- ***hacktivistas*** - utilizan las tecnologías de la información como medio de protesta y pueden llegar a causar graves problemas a organizaciones y empresas
- ***spamers*** - utilizan el correo electrónico como medio para el marketing no deseado y llegando al mayor número de posibles usuarios

Las subculturas siempre han tenido un lado oscuro o peligroso, aunque lo cierto es que algunas también han sido muy beneficiosas para los avances de Internet e incluso para la seguridad.

Una prueba de esto es que existen los denominados «*hackers* de guante blanco». Son personas que aprovechan su gran conocimiento de la tecnología para ayudar a empresas y usuarios a detectar fallos de seguridad e informar posteriormente de estos aunque, en muchas ocasiones, su labor altruista no sea bien vista.

Ejemplo

Kevin Mitnik ha sido considerado uno los mayores *hackers* de la historia. Después de causar muchos incidentes de seguridad, finalmente fue detenido y pasó cinco años en la cárcel. Cuando salió de prisión, creó su propia empresa de seguridad y hoy en día ayuda a otras empresas y organizaciones a luchar contra los riesgos y amenazas de seguridad.

Kevin Mitnik. Fuente: Wikipedia

Por otro lado, el termino *hacker* no ha estado siempre asociado a actividades delictivas. Su significado original está asociado a personas amantes de la tecnología que trataban de aprender lo máximo posible llevando más allá los límites de esas tecnologías.

En los inicios de Internet, las motivaciones que solían estar detrás de muchas de las actividades de las subculturas era la búsqueda del prestigio que les reportaba dar a conocer sus hazañas en su círculo de colegas tras, por ejemplo, haber conseguido acceder de forma no autorizada a un sistema o una red.

En la actualidad, esas motivaciones son mucho más peligrosas y menos «románticas». Por ejemplo, los *spakers*, que aprovechan sus conocimientos como *hackers* para acceder de forma no autorizada a bases de datos en Internet con el objetivo de obtener información y direcciones de correo electrónico que luego son vendidas a los *spammers* o grupos criminales que usan esa información para el envío masivo de correos electrónicos o para otros propósitos.

El riesgo

Los riesgos que se derivan de estas subculturas son muchos y variados. En multitud de ocasiones éstas son la causa de nuevos avances relacionados con Internet y la tecnología pero también, en ocasiones, son la raíz de graves incidentes de seguridad. Vamos a comentar algunos de ellos:

- En el caso de los *hackers* es el acceso no autorizado a sistemas. Una vez dentro, se puede dar el robo de información, la manipulación del sistema introduciendo algún tipo de programa de control o monitorización o creando una puerta trasera. De esta forma, el *hacker* puede acceder en cualquier otro momento o vender ese acceso a otro, obteniendo así beneficio económico.

Los *hackers* han conseguido acceder a todo tipo de sistemas desde servidores y sistemas militares, pasando por universidades, hasta portales en Internet o empresas, con objetivos diversos. En la actualidad, los casos de *hacking* suelen tener por objetivo el robo de información.

- En el caso de los *crackers* sus peligros asociados se basan en que consiguen romper las protecciones de los programas o dispositivos, de forma que éstos pueden ser usados de forma ilegal, sin el pago de la licencia. El riesgo, en este caso, no es tanto el hecho de que rompan las protecciones sino que, en muchas ocasiones, el software pirata es usado como vía o camino para entrar en los ordenadores de un usuario o una empresa, instalando algún tipo de *malware*.

Ejemplo

Los *crackers* son personas con conocimientos muy avanzados en programación. Mediante procesos muy elaborados son capaces de romper las protecciones más sofisticadas que ha creado la industria. Un ejemplo de ello es el teléfono de Apple, que era considerado uno de los dispositivos más seguros y finalmente pudo ser pirateado.

- Los activistas crean peligro porque pueden inutilizar la web de una compañía como acción de protesta, por ejemplo, mediante el uso de un ataque por denegación de servicio. Esto se conoce como «sentadas en la red».

Ejemplo

Durante las reuniones del G20, donde se reúnen los países más poderosos del mundo, se llevan a cabo multitud de protestas por grupos antiglobalización. En estas manifestaciones es muy común que grupos de *hacktivistas* realicen acciones de protesta no sólo en el mundo real, sino también a través de Internet.

Cómo protegerse

Protegerse de estas amenazas, y de sus consecuencias, pasa por algunas de las siguientes recomendaciones:

- utilizar cortafuegos y herramientas de protección anti*malware*
- realizar una adecuada configuración de las cuentas de usuario, estableciendo permisos y contraseñas robustas
- utilizar software legal
- verificar y analizar el contenido que se descargue de las redes de intercambio P2P
- utilizar sistemas de detección de intrusión y de prevención de intrusión

Estos y otros consejos pueden ayudarnos a protegernos de diversos riesgos que provienen de estas subculturas. No obstante, hay muchas y sus actividades son tan amplias que necesitaremos hacer uso de todas las herramientas de seguridad disponibles, sobre todo si deseamos proteger una organización.

Pero no estamos solos en esta tarea. A través de la OSI, la Oficina de Seguridad del Internauta, disponemos de mucha información que nos ayudará a conocer, entre otras cosas, las amenazas relacionadas con estos grupos, y también a través de la página web de INTECO-CERT.

El *malware*

La amenaza

El software ha tenido siempre una faceta muy útil ya que quienes desarrollan y crean programas y aplicaciones, lo hacen con el objetivo de ayudar al usuario, a una empresa o una organización a automatizar tareas, almacenar datos, etc.

Pero el software también tiene una faceta menos ventajosa ya que a veces se crea con propósitos más oscuros y dañinos. A este software, de forma general, se le conoce como *malware*. Su ejemplo más famoso y conocido por todos son los virus a los que podemos considerar como el primer tipo de *malware* de la historia.

En este sentido, se suele decir que en 1984 se adoptó el término virus como concepto informático aunque, curiosamente, el primer virus de ordenador no fue desarrollado para PC sino para Mac. Al parecer, fue creado dos años antes, en 1982, bajo el nombre «Elk Clonner», por Rich Skrenta, que lo desarrolló en un Apple II. A partir de ese momento, el *malware* no ha dejado de evolucionar y diversificarse. En la actualidad, el *malware* es capaz de realizar multitud de tareas y acciones de forma totalmente automatizada y sin intervención humana.

Ejemplo

Uno de los primeros casos de propagación de *malware* a través de una red de ordenadores fue protagonizado por el gusano «Morris», creado por Robert Tappan Morris en 1988, y que consiguió infectar y bloquear miles de ordenadores.

R. Tappan Morris. Fuente: Wikipedia

Algunos tipos de *malware* se comportan como pequeños ejércitos totalmente organizados y coordinados que reciben y ejecutan órdenes, como es el caso de las redes de *botnets* u ordenadores zombis.

Otros están pensados para ser indetectables, como los *rookits*, que se utilizan para conseguir controlar un ordenador y disponer de acceso a él de forma completamente invisible y sin que el usuario se percate. A continuación, indicamos algunos de los muchos tipos de *malware* que podemos encontrar en la actualidad:

- con capacidad de propagación: virus, gusanos
- diseñados para acompañar programas benignos: troyanos
- diseñados para proporcionar acceso a sistemas: puertas traseras o *backdoors*
- relacionados con la publicidad: *spyware, adware, hijakers*
- relacionados con el robo de información personal: *keyloggers, stealers*
- relacionados con llamadas telefónicas: *dialers*
- ataques o tareas distribuidas: *botnets*

A pesar de que existen muchos tipos distintos de *malware*, la tendencia actual es que éste cada vez se hace más complejo y multipropósito, de forma que es más difícil distinguir entre sus distintas variantes.

Ejemplo

En 2009, un *malware* de tipo gusano conocido como «*Downadup*», «*Conficker*» o «*Kido*» logró mantenerse como una de las tres principales amenazas mundiales durante un largo periodo. Su diseño y compleja programación, así como sus diversas capacidades, lo convirtieron en un modelo para los ciberdelincuentes.

El *malware*, a pesar del tiempo que lleva con nosotros, sigue siendo uno de los mayores problemas de seguridad a los que se enfrentan los usuarios y las organizaciones pero, afortunadamente, existen soluciones y formas de minimizar sus consecuencias.

El riesgo

Como hemos comentado, el *malware* actual está diseñado para cumplir múltiples funciones, que suponen un riesgo potencial para el usuario. Veamos algunas:

- robo de credenciales bancarias (*phishing*)
- secuestro de un ordenador
- envenenamiento de DNS y redirección a páginas fraudulentas
- envío de correo no deseado (*spam*)
- espionaje y control
- creación de redes para ataques distribuidos (*botnets*)
- explotación de vulnerabilidades (*exploits*)
- ataques de denegación de servicio (DoS)

Estos son sólo algunos ejemplos de lo que puede hacer el *malware* actual. El *malware* sigue aumentando, cada vez es más sofisticado y más difícil de detectar. Además, se está produciendo una profesionalización en la creación de *malware,* con grupos perfectamente organizados, que buscan beneficio económico mediante el chantaje, el secuestro de ordenadores, el envío de *spam*, el *phishing*, etc.

¿Cómo protegerse?

En la actualidad, protegerse del *malware* precisa contar con una herramienta de seguridad fundamental, como las *suites* de seguridad para Internet, que incorporan herramientas de protección para muchos tipos de *malware* y otro tipo de amenazas. Además, están preparadas para evitar la entrada de *malware* y su propagación por diversos medios, como

puede ser el correo electrónico, las páginas web infectadas con código malicioso, los soportes de almacenamiento como las memorias *USB* o incluso del *malware* que llega a través de las redes sociales o del P2P.

Hoy en día es fundamental contar con herramientas integrales de seguridad pero, sobre todo, que éstas cuenten con un servicio de actualización constante. Una herramienta que no esté convenientemente actualizada, pierde su eficacia y su capacidad de protección.

En la web de INTECO-CERT ofrecemos a los usuarios un catálogo de utilidades y herramientas de seguridad gratuitas. Puede encontrarlas en el enlace al apartado de Útiles Gratuitos.

Además de estas herramientas, es importante seguir algunos consejos, como los que le ofrece INTECO-CERT en el siguiente enlace al apartado de Buenas Prácticas.

Unido a todo esto, siempre hay que tener presente que el internauta es responsable del uso adecuado que hace de los recursos y, por tanto, no basta con tener soluciones de seguridad sino que, además, es fundamental utilizar los recursos correctamente y de manera responsable.

Ingeniería social

La amenaza

Todos los días vemos como se producen denuncias de usuarios de Internet que han sido estafados, que han sido víctimas de lo que se conoce como *phishing* o que su identidad ha sido suplantada para cometer un delito.

Este tipo de incidentes de seguridad están dentro de una categoría conocida como ingeniería social. Es un término muy amplio que se aplica a la manipulación de personas y de organizaciones para conseguir un fin que, en muchas ocasiones, está relacionado con la obtención de beneficio económico.

En realidad, usamos ingeniería social constantemente, por ejemplo, para conseguir un trabajo, para lograr una cita o para vender un producto. La ingeniería social es un arma muy eficaz en muchos ámbitos de la sociedad. Posiblemente uno de los campos en los que más se utiliza sea el de la comunicación, muy centrado en la publicidad. Los publicistas son expertos en ingeniería social con la idea de conseguir vender un producto o servicio.

Hoy en día, la ingeniería social se ha convertido en una de las principales armas de los ciberdelincuentes y es utilizada para cometer todo tipo de estafas, robar información, suplantar identidades, etc.

Ejemplo

Un grupo de ciberdelincuentes aprovecha un desastre natural para engañar a los usuarios y propagar un *malware*, solicitando dinero a cambio de ayudar a las víctimas.

La ingeniería social es una de las amenazas más peligrosas a las que se enfrenta cualquier usuario de Internet actualmente, puesto que el gran número de incidentes de seguridad que se dan demuestra que este tipo de ataques cada vez son más sofisticados y elaborados y, por otro lado, que es relativamente sencillo conseguir engañar a un usuario.

El riesgo

Los riesgos que se pueden derivar de la ingeniería social son tremendamente peligrosos. Muchas de las acciones de ingeniería social se aprovechan de la buena fe de los usuarios, de sus creencias o de sus gustos y aficiones.

En muchas ocasiones, noticias o desastres que han sucedido son utilizados para enviar un correo falso en el que se solicita ayuda pero que incorpora algún enlace a una página falsa, infectada o incluso el propio correo contiene algún tipo de *malware* que el usuario descarga creyendo que está haciendo algún bien o ayudando a alguien.

En la actualidad recibimos mucha información por diversos medios, no sólo a través del ordenador sino también del teléfono móvil. De esta forma, cualquier vía a través de la que pueda llegar información se convierte en una herramienta para realizar ingeniería social y, por tanto, para engañar al usuario. Algunos ejemplos son:

- Es muy habitual un tipo de engaño realizado con correos electrónicos que simulan ser correos bancarios legítimos, en los que se nos solicita información como la clave de acceso u otros datos.
- Las ofertas de trabajo falsas en las que se nos ofrecen trabajos aparentemente muy bien remunerados, pero que en muchas ocasiones buscan posibles víctimas que

puedan ser usadas como intermediarios en operaciones ilegales o fraudulentas, o que nos solicitan el envío de dinero como paso previo a una posible contratación.

- Los correos que nos recuerdan alguna tragedia o desastre natural y que, usando la buena fe de los usuarios, solicitan dinero o que accedas a determinado enlace para así contribuir en la ayuda.

Todas éstas y otras muchas formas de ingeniería social son cada vez más habituales. Los ciberdelincuentes no dejan de idear nuevas formas de engaño cuyo objetivo, como ya hemos comentado, suele ser la obtención de beneficio económico.

La protección

Protegerse de este tipo de amenazas requiere una combinación de soluciones de seguridad que pueden detectar páginas falsas, direcciones de correo que están catalogadas como peligrosas, correos electrónicos fraudulentos y por supuesto, el sentido común.

En este sentido, al igual que ocurre con el *malware*, es muy importante contar con una solución integral de seguridad para Internet que cuente con herramientas de protección antifraude o analizadores de URL, listas negras y blancas o sistemas basados en reputación.

Pero, además, y, sobre todo, necesitamos de nuestro sentido común, que es probablemente el arma más poderosa con la que contamos, para protegernos de este tipo de amenazas.

Es fundamental estar atentos a toda la información que recibimos a través de Internet, por ejemplo, aquella que proviene en forma de correos electrónicos, páginas web, mensajes de móvil o contactos en una red social. Cualquier vía de comunicación puede ser aprovechada por un ciberdelincuente para tratar de engañarnos.

A continuación, desde INTECO-CERT proporcionamos información para protegernos contra el fraude y la ingeniería social, a través del siguiente enlace al apartado de Fraude en Internet.

Finalmente, debemos indicar que los usuarios deben ser muy cuidadosos con la información personal que publican en Internet. Este tipo de datos son muy valiosos para los ciberdelincuentes, que los explotan y que los pueden utilizar en nuestra contra, mediante el engaño, la estafa o la suplantación de nuestra identidad o de la de un amigo o conocido.

Como veremos, la ingeniería social es uno de los mayores riesgos a los que nos enfrentamos en las redes sociales, tema que trataremos en el siguiente apartado de este módulo.

Redes sociales

Uno de los aspectos más interesantes y atractivos de Internet para cualquier usuario es la capacidad de poder comunicarse con cualquier persona en cualquier parte del mundo, hacerlo en cualquier momento y, además, por diversos medios como el chat, la videoconferencia o las redes sociales.

Las redes sociales se han convertido en una de las últimas revoluciones en el mundo de Internet. Han llevado un paso más allá el concepto de comunicación, pasando al siguiente nivel, el de la participación, la colaboración o el de compartir todo aquello que tiene que ver con nuestras vidas personales o nuestra actividad profesional.

Un mapa de las redes sociales actuales.

La información en Internet ha evolucionado en varias etapas, que indicamos a continuación:

- **Primera fase**. Se inicia con el nacimiento de Internet y llega hasta mediados de los años 90. Es probablemente la fase más larga. Durante la misma, la mayoría de la

información que se publicaba en Internet provenía de fuentes muy concretas, como investigadores, universidades, algunas empresas y los primeros buscadores.

- **Segunda fase**. Con la llegada de las redes de banda ancha, entre mediados y finales de los 90, se inicia una etapa en la que mejoran enormemente los contenidos en Internet. Se produce una explosión de la Red con millones de nuevos usuarios y empresas conectados y aparecen servicios de publicación de contenidos, entre ellos los *blogs*. La web 2.0 da sus primeros pasos. De esta forma, la información en Internet comienza a ser generada por los propios usuarios y, por otro lado, muchos medios de comunicación inician su paso al mundo virtual.
- **Tercera fase**. En esta fase, la web 2.0 alcanza su madurez y aparecen cientos de nuevos servicios en Internet donde cualquiera puede publicar todo tipo de información. En esta etapa, que dura hasta la actualidad, el usuario se vuelve el protagonista indiscutible en la generación de contenidos. Se popularizan las redes sociales y el tipo de información que se publica en Internet comienza a cambiar. Comenzamos a publicar información personal relacionada con todos los ámbitos de nuestra vida.
- **Cuarta fase**. Podríamos afirmar que nos encontramos en sus inicios. Se comienzan a aplicar nuevos paradigmas, como la información en la nube, la virtualización, la web semántica, los sistemas operativos web, la masificación de los dispositivos móviles inteligentes permanentemente conectados a Internet o la aparición de nuevos dispositivos y ordenadores que están revolucionando la forma que tenemos de conectarnos y usar Internet.

Hablaremos más sobre esta cuarta fase y cómo afecta a la seguridad, pero ahora nos centraremos en las redes sociales, que han marcado un antes y un después en Internet. Uno de los mayores cambios que se ha producido es que los usuarios no sólo generan contenido, sino que ese contenido tiene, en muchas ocasiones, un ámbito y un carácter muy personal.

Una de las consecuencias de este cambio en la clase de información que publicamos ha sido el tipo de incidentes de seguridad, puesto que como ya se ha comentado, la información personal es enormemente atractiva para los grupos criminales organizados y los ciberdelincuentes o personas sin escrúpulos que buscan venganza, difamación o daño de imagen.

La amenaza

Existen redes sociales para todos los gustos ya que no son más que un reflejo de la sociedad. Desde siempre los seres humanos hemos buscado relacionarnos y conocer personas con las que tenemos cosas en común, ya sea en el ámbito profesional o personal. Las redes sociales han conseguido hacer realidad ese sueño, pero también han traído consigo muchos riesgos y amenazas cuando no las usamos de forma responsable.

La principal amenaza relacionada con las redes sociales es que éstas son gestionadas y controladas por empresas que, a veces, realizan un uso inadecuado de los datos y la información que publicamos en estas redes.

Por ejemplo, nuestros datos pueden ser vendidos para ser utilizados en campañas de marketing dirigido o estudios de mercado. Otras veces son cedidos a compañías que los usan para otros propósitos…

Hay dos problemas fundamentales asociados a los datos que se publican en las redes sociales:

- por un lado, el usuario, en muchas ocasiones, desconoce qué ocurre realmente con sus datos y quién tiene acceso a ellos
- por otro lado, se publica todo tipo de información de carácter personal, muy íntimos, como pueden ser datos de salud, de ideología, de creencias, de hábitos sexuales, etc.

La publicación indiscriminada de información personal supone un riesgo enorme para el usuario que se encuentra desinformado, indefenso y, a veces, confiado porque piensa que nadie está interesado en su información. ¡Nada más lejos de la realidad!

El riesgo

Los riesgos que podemos encontrar en las redes sociales son muy variados y pueden traernos consecuencias insospechadas. Veamos algunos ejemplos.

- **Daño o perjuicios a terceros**. Publicar información o fotografías sin permiso, o sin valorar los riesgos, puede suponer perder una amistad o dañar una relación de pareja. Podríamos pensar que esto son sólo meteduras de pata, pero en el ámbito de

las redes sociales, este tipo de errores comunes pueden ser causa de venganzas o incluso de denuncias por parte de los afectados. Podemos causar mucho daño con los datos que publicamos si no sopesamos lo que estamos publicando.

- **Pérdida del trabajo**. Hay veces que las redes sociales son utilizadas para buscar información sobre los empleados de una organización para conocer sus hábitos, lo que piensan de su empresa, sus comentarios, etc. Esto ha derivado, en ocasiones, en personas que han perdido sus trabajos porque la información que es publicada la puede ver todo el mundo. Ha habido casos en los que un amigo o un conocido ha llegado a denunciar o filtrar dicha información a la empresa del afectado, lo que ha supuesto que éste haya sido despedido.

- **Difamación o calumnias**. Las redes sociales pueden ser usadas para llevar a cabo campañas de difamación y calumnias. Debemos tener en cuenta que Internet es un medio en el que la información fluye a una enorme velocidad. Una vez que algo es publicado y difundido, es realmente difícil hacer que desaparezca. En el caso de las redes sociales, lógicamente ocurre igual. La velocidad a la que se puede propagar un rumor, una fotografía comprometedora o una mentira es enorme. Pocas veces pensamos en las consecuencias que puede tener un simple clic de ratón.

- **Menores y redes sociales**. Las redes sociales se han convertido en un lugar perfecto para los delincuentes sexuales que se hacen pasar por amigos o jóvenes con perfiles falsos, con el objetivo de engañar o acosar a menores. El concepto de amistad en las redes sociales se difumina. Los menores son un grupo de riesgo en este sentido, puesto que son mucho más influenciables que otro tipo de usuarios.

Éstos son sólo algunos de los riesgos que nos podemos encontrar en las redes sociales. Combatirlos es una tarea fundamental y muy necesaria puesto que este tipo de incidentes pueden tener consecuencias directas tanto para nuestro entorno personal como profesional.

La protección

La protección en las redes sociales frente a los riesgos a los que estamos expuestos en ellas pasa por una labor de concienciación y formación. A diferencia de otras amenazas y riesgos, donde la solución es principalmente técnica y podemos hacer uso de soluciones de seguridad muy potentes y versátiles que facilitan enormemente la tarea de la protección, en las redes sociales la protección empieza por el propio usuario y termina también con él.

Por ello, vamos a proporcionar una serie de recomendaciones e información que ayudará al usuario a hacer un uso adecuado y seguro de las redes sociales. Veamos algunas de estas recomendaciones.

- **Política de uso y privacidad**. Las redes incorporan una política de uso y privacidad que es fundamental conocer. Ésta se encuentra disponible a través de la página web de la red social, en un apartado destinado a la política de privacidad. Es muy importante conocer esta política puesto que describe los usos y responsabilidades que tiene la empresa que gestiona la red social sobre la información publicada.
- **Nivel de privacidad**. Cuando creamos una cuenta en una red social, el primer paso que debemos realizar, después de haber leído la política de privacidad, es configurar el nivel de privacidad. Éste permite controlar quién ve la información que publicamos en la red social. Configurar el nivel de privacidad es especialmente importante en el caso de los buscadores. Es decir, cuando publicamos información en una red social es posible que sea visible no sólo para las personas que pertenecen a esa red social sino que incluso el contenido que publica el usuario puede ser indexado y utilizado por los buscadores de Internet que están fuera de la red social. De esta forma, es posible buscar datos de una persona en Google y encontrar información que ha publicado en su red social. Para evitar estos y otros problemas de privacidad, lo ideal es que, al principio, sobre todo si desconocemos el funcionamiento, bloqueemos todos los permisos y, poco a poco, vayamos dando visibilidad a los contenidos que publiquemos, pero de forma controlada.

- **Amigos y conocidos**. Uno de los mayores peligros de las redes sociales se deriva del hecho de que en una red social parece que todo el mundo puede ser amigo nuestro. Al igual que ocurre en la realidad, no es lo mismo un amigo, un conocido o un compañero de trabajo. Son conceptos completamente distintos y las implicaciones de cada uno de esos tipos de usuarios que nos podemos encontrar en una red social, también son totalmente distintas. En este sentido, es muy recomendable, establecer distintos grupos de usuarios, en los que podamos agrupar y diferenciar a nuestros amigos de otros que no lo son.
- **Información personal**. La información que podemos publicar en una red social es muy variada, pero cuando se trata de datos personales, al igual que ocurre con los amigos y conocidos, es muy importante saber diferenciar. No es lo mismo publicar una fotografía tomando algo con los amigos, que una imagen con nuestra pareja o un comentario a un amigo. Por regla general, cuanta menos información personal publiquemos, mejor. No obstante, si vamos a publicarla es fundamental pensar antes qué tipo de información estamos publicando y cuáles pueden ser las consecuencias de hacerlo, sabiendo que desconocemos en qué manos puede caer.
- **Información de terceros**. En las redes sociales es muy habitual publicar información de amigos, puesto que nos hacemos muchas fotografías cuando estamos tomando algo o celebrando un acontecimiento. El problema de publicar información en la que aparecen terceros, que pueden ser amigos o no, es que no siempre pensamos en las consecuencias no deseadas que pueda traer. Por tanto, debemos tener en cuenta que la información que publicamos en una red social, en ocasiones, está relacionada no sólo con nosotros sino también con muchas otras personas.

Para saber protegerse en las redes sociales, el usuario puede encontrar más información en el siguiente enlace, que podrá encontrar junto con más datos de interés en la Oficina de Seguridad del Internauta.

Seguridad en la nube

Internet no ha dejado de evolucionar desde sus inicios y aún continua haciéndolo. Prueba de ello es un nuevo paradigma que está provocando importantes y profundos cambios en el mundo de Internet y en el ámbito de las tecnologías de la información: el *cloud computing*.

Cloud computing significa «computación en la nube» y tiene que ver con el hecho de que cada vez más empresas y organizaciones externalizan una gran parte de sus infraestructuras TIC. Además, el aumento de velocidad de Internet y los avances que se han producido en las tecnologías web y los navegadores están posibilitando que muchas de las aplicaciones que usamos habitualmente ya no necesiten estar instaladas en nuestros ordenadores sino que, en realidad, podemos usarlas a través de un navegador.

Pero una de las mayores consecuencias del *cloud computing* es que las organizaciones han comenzado a externalizar, no sólo aplicaciones u otro tipo de recursos como ya se hacía con recursos humanos, instalaciones o infraestructura informática, sino también la información.

Durante mucho tiempo, la seguridad en las organizaciones se ha basado en el concepto de perímetro de seguridad. La idea de una organización aislada de Internet, y protegida mediante una barrera de seguridad, ha comenzado a desvanecerse ante los cambios que está trayendo consigo el *cloud computing*. Actualmente, las organizaciones comienzan a usar de forma cada vez más habitual aplicaciones y recursos que no están físicamente en

su propia organización. En muchos casos ni siquiera pertenecen a su propia organización, sino que son propiedad de otras que se los prestan como un servicio.

En la actualidad existen en Internet aplicaciones web para casi todo, desde montar un portal web o un gestor de contenidos, a la gestión de finanzas, el control de proyectos hasta la realización de facturación electrónica. Las ventajas de este enfoque son enormes, pero el problema radica en que mucha de la información con la que trabajan las empresas y que se utiliza en estos servicios está fuera de la organización, incluso fuera de su país con el problema legal que puede surgir.

En realidad, el *cloud computing* está relacionado con otros conceptos como la externalización, las aplicaciones como servicios, el *outsourcing*, la virtualización o los servicios gestionados. Animamos al lector a profundizar más en estos conceptos, que se salen del ámbito de este curso.

La amenza

El *cloud computing* supone enormes ventajas desde el punto de vista de la gestión, la eficiencia o la especialización para las organizaciones. Veamos un ejemplo.

Ejemplo

Imaginemos una empresa en la que toda la infraestructura la provee otra empresa, como si de un alquiler se tratara. En el caso de las aplicaciones que necesitan para su trabajo diario, como pueden ser aplicaciones de ofimática, de facturación, de contabilidad, etc., son aplicaciones web que proporcionan varias empresas, en forma de servicio, por el que se paga mensualmente.

La información que utiliza una organización no tiene por qué estar almacenada físicamente en sus oficinas, sino que puede estarlo en parte en las distintas aplicaciones web que se utilizan. Por tanto, la información estará situada fuera de nuestra organización.

Actualmente algunas de las aplicaciones más habituales que usamos, como las aplicaciones de ofimática, ya están disponibles en Internet como páginas web y, por tanto, como servicios. Esta tendencia está aumentando y cada vez más aplicaciones, que habitualmente eran instaladas en el puesto de trabajo, son convertidas a aplicaciones web, que se

encuentran físicamente fuera de las instalaciones de la empresa, lo que implica que la información o parte de ella también se encuentra fuera.

La información es el activo más importante que posee una organización. Si ésta ya no está físicamente almacenada en la propia organización, mantener los niveles de seguridad se vuelve una tarea compleja. Ya no dependemos únicamente de nuestros recursos, infraestructuras, políticas y normativas sino que estamos en manos de terceros.

Que la información se encuentre fuera de la organización no es un problema en sí mismo, sino una consecuencia de la evolución de las tecnologías de la información, pero plantea muchos riesgos desde el punto de vista de la seguridad para las organizaciones.

El riesgo

Imaginemos que una empresa, con el objetivo de reducir costes e infraestructuras, decide externalizar sus infraestructuras TIC. De este modo, pretende aprovechar las ventajas de contar con aplicaciones como servicio y basadas en tecnología web, de forma que ya no requiere instalar aplicaciones en sus ordenadores sino que sus empleados usan las aplicaciones que necesitan a través de un navegador.

En un escenario como éste, la información ya no está en la organización, está repartida por las distintas aplicaciones web, y por tanto, la información estará almacenada en los servidores y sistemas de la empresa que provee los servicios y aplicaciones.

Pero es más, imaginemos que utilizamos aplicaciones web de varias empresas. Aquí la información no sólo estará fuera de nuestra empresa sino que, además, estará repartida entre varias empresas, siendo almacenada en sus respectivos sistemas y servidores.

En un planteamiento como éste, hablar de perímetro de seguridad es confuso, puesto que ya no hay una barrera definida. La seguridad ya no depende exclusivamente de nuestra organización sino también de cada una de las empresas que nos dan servicio y que almacenan parte de los datos que pertenecen a nuestra empresa.

En un escenario como éste, nos hacemos las siguientes preguntas: ¿cómo garantizamos la seguridad de esa información?, ¿cómo evitamos que pueda ser robada o vendida a la competencia?, ¿cómo aseguramos su disponibilidad en todo momento? y ¿cómo cumplir con la legislación vigente?

La protección

La protección de la información en los próximos años se convertirá en un reto tremendo, puesto que cada vez habrá más información que estará almacenada en nuestras instalaciones. Cada vez habrá más dependencia de otras organizaciones que nos proveerán aplicaciones e infraestructuras como servicios.

Cuando parte de nuestra seguridad dependa de la seguridad de otros, necesitaremos establecer acuerdos y contratos de servicio que incorporen las condiciones, garantías y niveles de servicio necesarios para garantizar a su vez la seguridad de nuestra información y, por extensión, la seguridad de nuestra organización desde todos los puntos de vista, como son legal, técnico o el organizativo.

El mantenimiento de la seguridad en este tipo de entornos se volverá muy complejo y será necesario disponer de nuevas soluciones de seguridad y nuevos sistemas de gestión de la seguridad adaptados a esta nueva evolución.

Resumen del módulo

Podemos resumir los contenidos de este módulo en las siguientes ideas, las más importantes, puesto que son muchos aspectos y cuestiones las que se han visto a lo largo de los distintos apartados:

- Las subculturas han existido desde el inicio de la tecnología. Los *hackers, crackers, hacktivistas, spamers o spakers* son sólo algunos de estos grupos.
- Las subculturas en torno a la tecnología tienen un lado oscuro pero, también, han propiciado avances y cambios importantes en Internet.
- Los riesgos derivados de las subculturas son amplios y diversos. Uno de los mayores riesgos en la actualidad es que muchos de estos grupos se han criminalizado. Detrás de ellos están grupos criminales organizados.
- El *malware* es una de las amenazas más antiguas. Se inició con la aparición del primer virus con capacidad para autorreplicarse. Rápidamente aparecieron otras variantes, como los gusanos o los troyanos.
- En la actualidad el *malware* es enormemente diverso, complejo y peligroso. Ya se habla incluso de una industria organizada, puesto que gran parte del *malware* actual es creado por criminales y profesionales del cibercrimen.
- Para protegerse contra el *malware* es fundamental contar con *suites* de seguridad integrales que ofrezcan protección contra todo tipo de *malware* y que, además, ofrezcan protección a través de múltiples vías de entrada, como el correo electrónico, la mensajería instantánea o el web.
- La ingeniería social consiste en manipular o engañar para conseguir un objetivo. En la actualidad es muy utilizada para cometer fraude o estafas.
- La ingeniería social se apoya en todo tipo de herramientas, como es el *malware* o el correo electrónico para logar mayor efectividad y conseguir sus objetivos.
- La protección frente a la ingeniería social pasa por contar con una solución de seguridad de Internet que nos proteja de paginas falsas, código malicioso, correos fraudulentos, etc.

- Por otro lado, la protección frente a la ingeniería social pasa por la concienciación y formación del usuario.
- Las redes sociales han supuesto una revolución en Internet. Cualquier usuario puede compartir información sobre su vida personal o profesional, sus gustos, aficiones, etc.
- Gran parte de la información que se publica en las redes sociales es información personal, lo que supone un enorme riesgo para los usuarios, pues esta información es muy codiciada por los ciberdelincuentes o los grupos criminales.
- La protección en las redes sociales recae de forma muy importante sobre el propio usuario y es necesario que esté formado y concienciado de todos los riesgos y amenazas.
- En las redes sociales debemos tener en cuenta el tipo de información que publicamos, en relación con los daños o perjuicios que podemos causar a terceros.
- Es necesario conocer la política de privacidad y uso de la red social. Además, hay que estar informado de cuál es el uso que se le da a nuestra información personal y quién tiene acceso a ella.
- También es fundamental establecer grupos y categorías en los contactos, así como tener en cuenta que no todos aquellos que están en una red social son amigos. No es lo mismo un amigo, que un conocido o un compañero de trabajo.
- Es necesario revisar con detenimiento el tipo de información personal que publicamos, no toda es igual, y las consecuencias que se pueden derivar de su publicación también pueden variar.
- La seguridad en la nube es un concepto que se deriva de un nuevo paradigma que se está imponiendo en Internet, el *cloud computing*.
- Cada vez más aplicaciones son convertidas en tecnología web, de forma que ya no necesitan ser instaladas en un puesto de trabajo sino que es posible acceder a ellas mediante un navegador.

- La consecuencia más importante del *cloud computing* es que la información ya no se encuentra en las organizaciones sino fuera, repartida por distintas aplicaciones y empresas que proveen dichas aplicaciones como servicio.
- La seguridad y la protección en un entorno de *cloud computing* pasa por establecer los acuerdos y contratos de servicios adecuados, en los cuales deben reflejarse las garantías, los niveles y la seguridad que tienen que cumplir dichos servicios.