CCN-CERT

BP/08

Buenas Prácticas en Redes Sociales

INFORME DE BUENAS PRÁCTICAS

JULIO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: julio de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Índice

1. Sobre CCN-CERT

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es **contribuir a la mejora de la ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de **conseguir un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

2. Introducción

2.1 El ciberespacio como territorio habitado

Las redes sociales son donde se configura la identidad virtual. Pueden ser: individuos, colectivos, empresas o instituciones. Está compuesta por: un alias, una imagen personal y una declaración biográfica.

El ciberespacio es un dominio de intercambios sociales que está creciendo exponencialmente cada año y que se ha establecido como un territorio propio en el que individuos, colectivos, empresas e instituciones llevan a cabo actividades.

Se trata de un territorio compuesto básicamente por identidades y objetos conectados a través de internet. En 2020, se estima que habrá 50 mil millones de objetos conectados a Internet de las Cosas (IoT), interactuando con las personas a través de sus identidades digitales.

Con todo, no es solo a nivel cuantitativo que los seres humanos han pasado a "habitar" el ciberespacio, sino que el ciberespacio es un territorio virtual donde los humanos "hacen vida": interactúan, se comunican, realizan intercambios sociales, comerciales, políticos o religiosos y, en definitiva, acaban "siendo y estando".

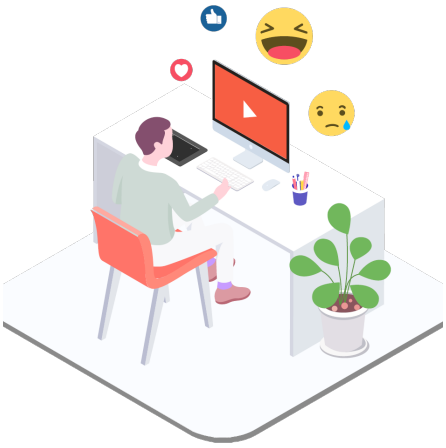
Más allá de la presencia general en la web, en las redes sociales es donde se configura la identidad virtual que una persona empleará en sus vivencias, en su vida en el ciberespacio.

Esa identidad digital está compuesta por un nombre (por un alias o por varios); por una imagen personal (tipo avatar), que representa al individuo en una o varias redes sociales; y por una declaración

biográfica, basada en una serie de referencias personales o laborales como localización geográfica, estudios o trabajo

.

Lo que es más importante, asociado a esas referencias hay un volumen significativo de contenidos en texto, imagen, audio o vídeo, donde una persona muestra su comportamiento, sus afinidades, sus intereses y, en definitiva, una traza más o menos detallada de su vida personal, social y, a menudo, laboral.



2.2 ¿Qué son las redes sociales?

En el momento en que se constituyen grupos de individuos que comparten lazos sociales personales o vínculos de interés hacia cualquier dominio económico, religioso, político, de ocio o de otro tipo, ya está configurada una red social. Por tanto, la relación social de los seres humanos en red existe desde que el ser humano se comunica e interactúa con otros.

Sin embargo, la eclosión de las redes sociales como concepto global y cotidiano, asociado a millones de seres humanos con independencia de su geografía de residencia o de su cultura de procedencia, es inherente a la aparición y crecimiento exponencial de los intercambios sociales a través de internet, de la web o, en definitiva, del ciberespacio.
Podría decirse que las redes sociales en el ciberespacio son el equivalente digital o virtual al conjunto de relaciones personales, laborales o sociales que habitualmente mantienen los seres humanos en su vida física.

En las redes sociales, en el ciberespacio, se mantiene una agenda de amigos o conocidos, se conversa con ellos y se comparten intereses y aficiones. Las redes sociales acaban estando configuradas para compartir experiencias digitales masivas; por ejemplo, puede acudirse virtualmente a un concierto de música o asistir a una clase universitaria impartida en otro país distinto al de residencia física del usuario.

2.3 ¿Para qué usan las redes sociales los bienintencionados?

La motivación principal para inscribirse en una red social, por lo menos en aquellas donde es necesario crear un perfil, es mantenerse en contacto con amigos y conocidos[1] o acceder a contenidos de interés para el usuario. Es decir, la motivación principal para las redes sociales es la interacción con otros miembros de la comunidad (círculos familiares, de amistad, profesionales, etc.).

Las redes sociales, como herramienta de comunicación masiva, permiten la ampliación de relaciones y la formación de identidad. Tras la creación por parte de Randy Conrads del sitio web *classmates.com* en 1995, para mantener contacto con sus ex compañeros de instituto, las redes sociales han registrado un crecimiento vertiginoso, favorecido por el desarrollo de aplicaciones y soluciones de conectividad basadas en dispositivos móviles.

1. Fuente: "Informe de resultados Observatorio de Redes Sociales". The Cocktail Analysis. Cuarta oleada, 2011. Abril 2012

2.3 ¿Para qué usan las redes sociales los bienintencionados?

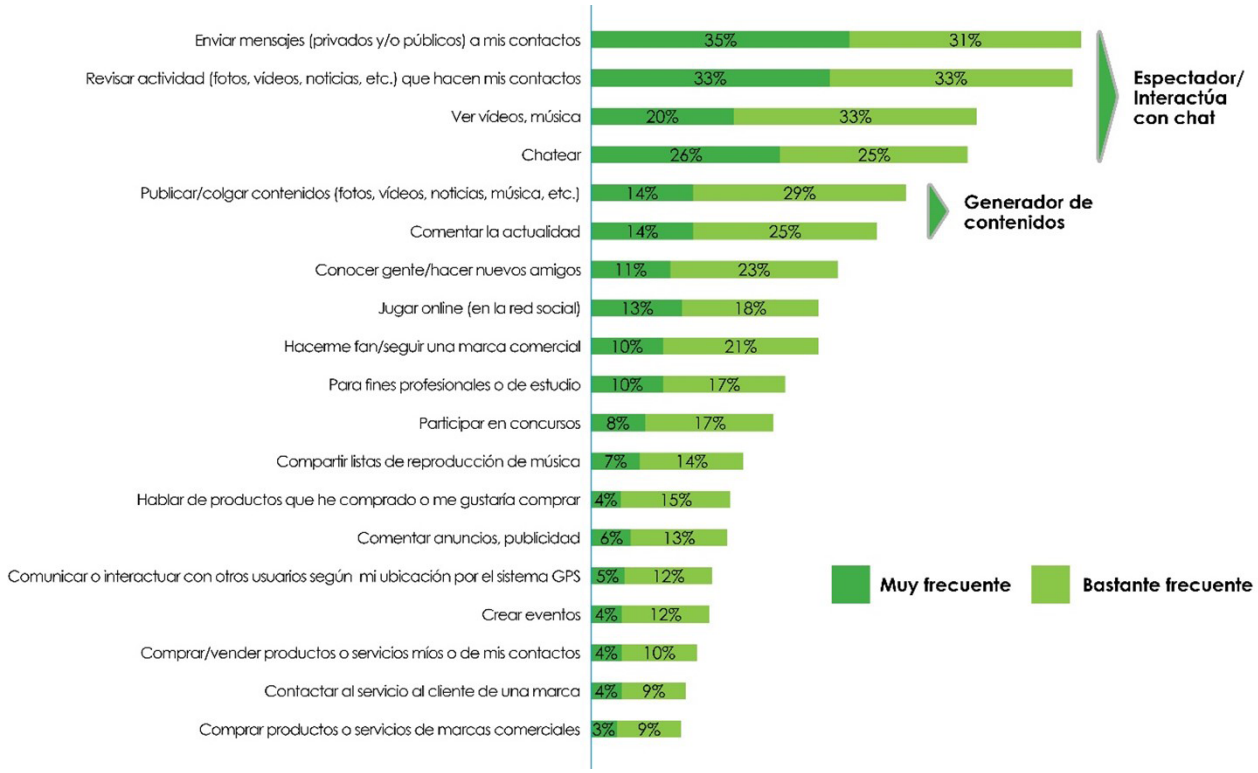


Figura 1- Motivos de pertenencia a redes sociales (estudio iab Spain)

2.4 ¿Para qué usan las redes sociales los malintencionados?

Las enormes posibilidades que brindan las redes sociales y su uso masivo llevan aparejados una serie de riesgos de diversa índole, tanto en el ámbito privado y personal como en el profesional.

Ante la creciente tendencia a utilizar este tipo de redes como medio para el desarrollo de ciberataques es de vital importancia estar protegido, realizar un uso adecuado y utilizar un entorno seguro durante su empleo.

En general, los actores que emplean las redes sociales como puerta de entrada para realizar ciberataques y comprometer la seguridad de los usuarios aprovechan tres (3) tipos de vulnerabilidades implícitas a la propia "arquitectura social" de las redes:

2.4 ¿Para qué usan las redes sociales los malintencionados?

Sobreexposición de información personal. La sobreabundancia de información personal, que los usuarios difunden a través de sus perfiles en redes sociales, constituye una atractiva materia prima para que los cibercriminales utilicen esa información con propósitos dañinos.

Autopistas de información. La propia fluidez y apertura inherente a la comunicación convierte a las redes sociales en auténticas autopistas de información por las que circulan comunicaciones socialmente inocuas y legítimas, así como contenidos vinculados a diversos tipos de código dañino. Este malware no es específico de las redes sociales, pero aprovecha la fluidez de la comunicación social en red para distribuirse y extender su infección al mayor número de usuarios posible.

Utilización masiva. Con un índice de penetración del 42% de la población mundial (3.196 millones de personas) , las redes sociales son el vehículo perfecto para acceder a un gran número de personas, potenciales víctimas de un ciberataque.

2. Global Digital Report 2018 (https://digitalreport.wearesocial.com)

2.4 ¿Para qué usan las redes sociales los malintencionados?

La utilización malintencionada de redes sociales más habitual se inscribe en las siguientes categorías:

- **Ingeniería social:** consiste en el diseño de mecanismos o esquemas de engaño, destinados a hacer que los usuarios lleven a cabo determinados comportamientos que les van a perjudicar, lo que permite a los cibercriminales obtener un beneficio ilícito.

  La ingeniería social recurre a las pautas conocidas del comportamiento humano para diseñar procesos de conducta *online*, que inciten a los usuarios realizar determinadas acciones, accedan a determinados contenidos, proporcionen información en diferentes contextos o compartan datos sensibles.

- **Robo de identidad:** para ello, aprovechan la información personal difundida por los usuarios en redes sociales.

- **Ciberacoso o cyberbullying:** se vale de la capacidad de una persona para acosar psicológicamente a otra, gracias a la información que obtiene de su víctima mediante sus perfiles en redes sociales, y es especialmente grave cuando implica a menores de edad y se da en el entorno de la escuela[3]. Algunas formas específicas de ciberacoso son:

  - **Sexting:** consiste en el envío por internet, especialmente a través de smartphones (aplicaciones como WhatsApp facilitan esta práctica), de fotografías y vídeos con contenido sexual, filmados o grabados por su propio protagonista. Es una práctica cada vez más común entre jóvenes y puede derivar en acoso o en extorsión si el receptor de las fotografías tiene intenciones maliciosas.

  - **Grooming:** método basado en un conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de internet, y conseguir así su control a nivel emocional, con el fin último de obtener concesiones de índole sexual.

- **Perjuicio reputacional:** en el ámbito personal, social o laboral, derivado de contenidos en redes sociales que pueden perjudicar las relaciones de una persona en esos ámbitos.

- **Publicidad dañina o engañosa:** difundida y suministrada a través de redes sociales, en numerosas ocasiones con propósitos de fraude o de difusión de código dañino.

3. https://www.anar.org/wp-content/uploads/2017/04/INFORME-II-ESTUDIO-CIBERBULLYING.pdf

2.4 ¿Para qué usan las redes sociales los malintencionados?

Criminalidad en el mundo físico: se vale de información obtenida en redes sociales para realizar conductas delictivas en el ámbito físico, como robos en vacaciones, aprovechando información publicitada en redes sociales, o secuestros, con el fin de obtener un rescate según el "nivel de vida" de una persona observado en sus redes sociales.

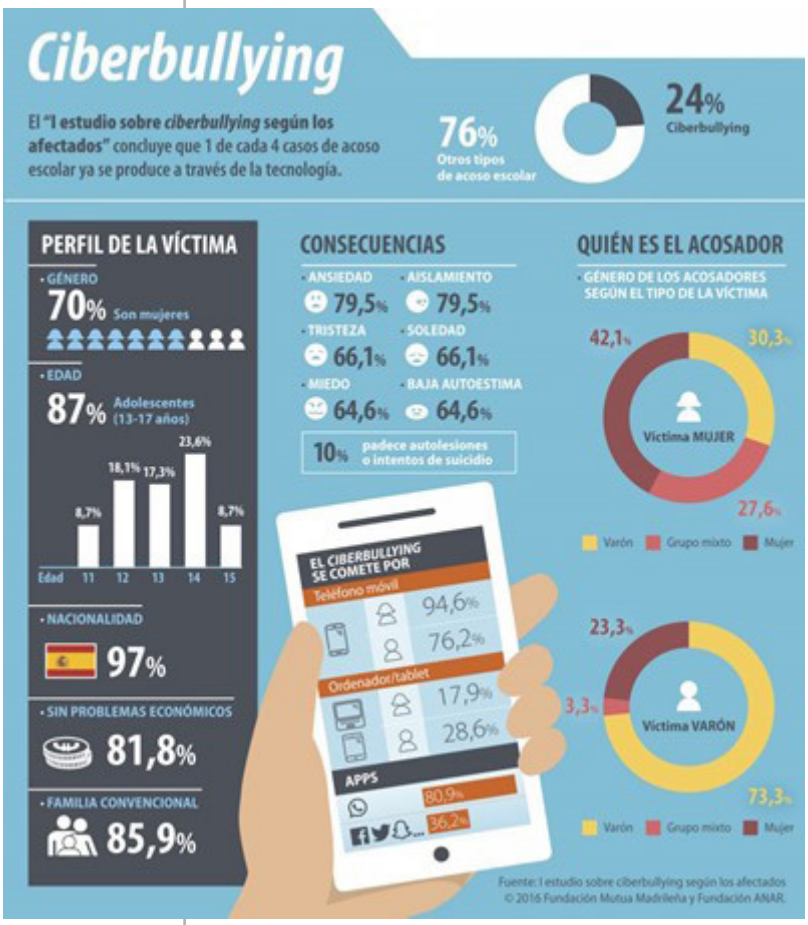


Figura 2.- Fundación ANAR

Distribución de malware: para ello, emplean las autopistas de información interpersonal que representan las redes sociales. Los grupos cibercriminales utilizan las redes sociales sencillamente como canales de distribución de todo tipo de código dañino. No buscan explotar vulnerabilidades de programación o de configuración en las propias redes sociales, sino descargarse en los dispositivos de los usuarios (sobremesas, teléfonos móviles, tabletas) y, una vez allí, actuar explotando vulnerabilidades de las *apps* y del *software* que hay instalado en ese dispositivo.

Los modos más habituales de distribución de código dañino en redes sociales son:

2.4 ¿Para qué usan las redes sociales los malintencionados?

Phishing y Pharming. El *phishing* es un tipo de ataque en el que se utiliza la ingeniería social para obtener de los usuarios información personal, principalmente de acceso a servicios financieros. Para alcanzar el mayor número posible de víctimas e incrementar las posibilidades de éxito, utilizan el correo basura o "*spam*" para distribuirse. Una vez que el correo llega al destinatario, facilitan enlaces a sitios web modificados de bancos y empresas financieras, para que se introduzcan datos personales como números de cuenta bancaria, contraseñas, números de seguridad social, etc.

Por su parte, el *pharming* es un redireccionamiento de peticiones legítimas de nombre de dominio a un sitio web falso o fraudulento, mediante la explotación del sistema DNS (secuestro o envenenamiento del DNS).

Asimismo, también se emplean técnicas de phishing, suplantando páginas de inicio en plataformas de redes sociales, para recopilar información e intentar acceder a otros servicios que utiliza la víctima, al ser habitual compartir el mismo usuario y contraseña en la mayoría de los servicios que se ofrecen en internet.

Enlaces maliciosos. Estos tipos de ataques suelen aparecer bajo la fórmula "mensaje más enlace", siendo el enlace el que lleva al usuario al contenido malicioso. En el caso de un ataque en Facebook, por ejemplo, se suele utilizar el muro de la víctima, donde se coloca un mensaje, un privado (inbox) o una foto en la que el usuario aparece etiquetado.

En el caso de Twitter, este tipo de ataques se realiza a través de una mención, un mensaje privado o mediante acortadores de enlaces, que emplean esta plataforma, y que son aprovechados en campañas de spam y redireccionamiento.

Videos prometedores. Uno de los "anzuelos" más comunes para un ataque en redes sociales, al igual que ocurre en el correo electrónico, es la promesa de ver un vídeo impactante, como el que prometía mostrar la muerte de Osama Bin Laden.

Al cliquear en estos vídeos, se muestra información en el perfil de la red social, publicando este mismo vídeo u otro similar, sin el consentimiento de la víctima.

2.4 ¿Para qué usan las redes sociales los malintencionados?

Un estudio de TrendMicro[4] sugiere que los grupos cibercriminales preparan esquemas de engaño (campañas de *phishing*) sobre acontecimientos mediáticos entre las dos (2) semanas anteriores y las tres (3) horas posteriores al mismo. Además, cabe destacar que hasta un 13 % de usuarios ha sido víctima de robo de identidad a través de redes sociales; que un 69 % de adultos y un 88 % de adolescentes son expuestos de alguna forma a acoso o crueldad en redes sociales; o que casi cinco (5) millones de personas anuncian habitualmente sus planes de viaje en redes sociales.

Figura 3.- Información compartida en redes sociales (TrenMicro)

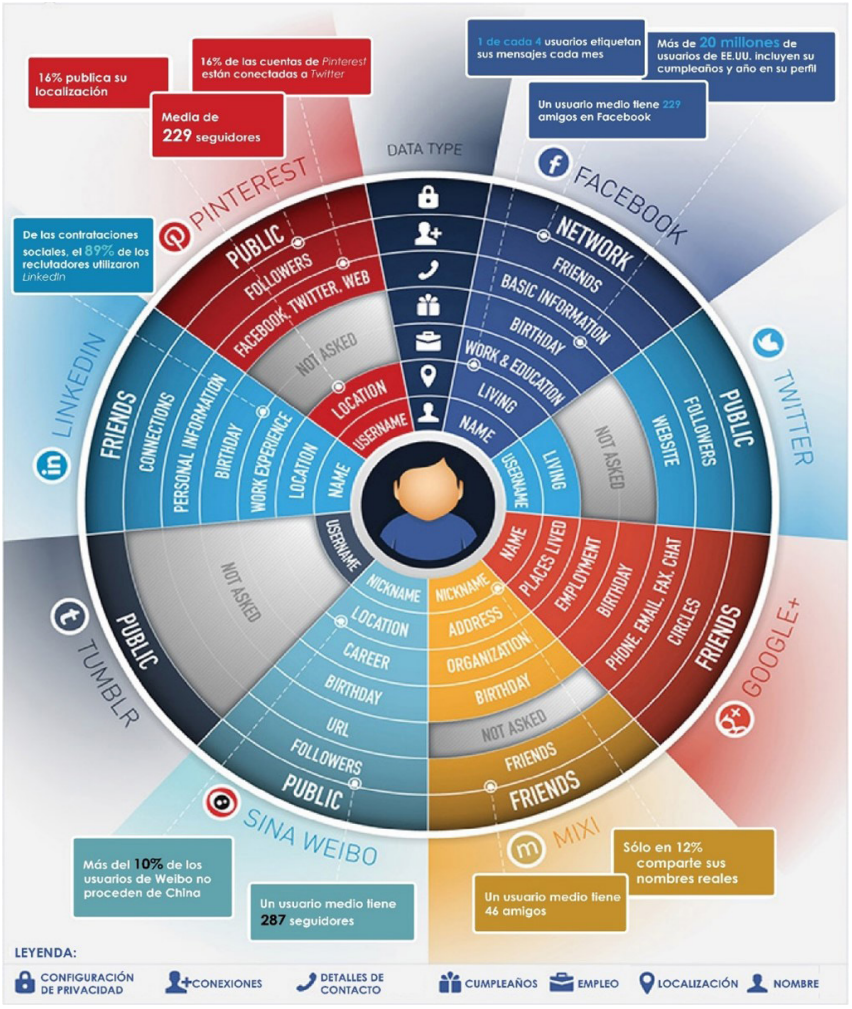
En internet, muchos de los riesgos a los que están expuestos los sistemas y sus usuarios tienen que ver con vulnerabilidades en servidores web, gestores de contenidos, configuraciones de bases de datos o de paneles de acceso. Es común, por ejemplo, que una vulnerabilidad en el diseño de programación de un servidor web sirva a un atacante para obtener acceso ilegítimo a la base de datos de usuarios de esa web y robar todos sus datos personales.

Por otro lado, el código dañino puede ser muy variado en su diseño y en sus funciones (troyanos para robar información personal, herramientas de acceso remoto para tomar el control de dispositivos, ransomware para extorsionar, adware para fraude…), pero todos tienen un elemento común, una especie de código genético que todo malware posee: estará diseñado para explotar una o varias vulnerabilidades generalmente

4. http://blog.trendmicro.com/trendlabs-security-intelligence/the-risks-of-posting-in-social-networks/

en el software y, en menor medida, en el hardware de dispositivos principalmente conectados a una red, siendo internet la más accesible.

Hay una clara diferencia entre las vulnerabilidades que presentan las redes sociales y las que exponen los dispositivos conectados a internet. Las redes sociales constituyen un canal privilegiado, por su conectividad interpersonal, para que el código dañino sea difundido y llegue a infectar a dispositivos vulnerables de los usuarios. Es decir, la vulnerabilidad que los creadores de malware explotan en las redes sociales es la propia conectividad intrínseca a la estructura interpersonal de la red.



Hay una clara diferencia entre las vulnerabilidades que presentan las redes sociales y las que exponen los dispositivos conectados a internet. Las redes sociales constituyen un canal privilegiado, por su conectividad interpersonal, para que el código dañino sea difundido

y llegue a infectar a dispositivos vulnerables de los usuarios. Es decir, la vulnerabilidad que los creadores de malware explotan en las redes sociales es la propia conectividad intrínseca a la estructura interpersonal de la red.

Aunque las redes sociales tengan vulnerabilidades relacionadas con la programación de su software o su diseño, que permitan a un atacante obtener un acceso ilícito a información personal o comprometer la seguridad del usuario, no suele ser lo habitual. A veces se difunde una vulnerabilidad de una red social que permitiría a un atacante, por ejemplo, acceder a información privada de los usuarios o modificarla. No obstante, estas vulnerabilidades ocasionales en redes sociales no suelen ser su talón de Aquiles, ni llamar la atención de los cibercriminales hacia ellas.

En general, el malware de mayor predominio está desarrollado para explotar vulnerabilidades en el software de las aplicaciones (programas) o apps de los dispositivos físicos de los usuarios (teléfonos, tabletas…). En este contexto, las redes sociales se emplean principalmente como vehículos de difusión y transmisión de código dañino con el objetivo de infectar dispositivos de usuarios que están conectados a internet.

En ese empleo malintencionado de las redes sociales como vehículos de propagación de amenazas, los autores se valen principalmente de dos (2) características inherentes a las redes sociales: la sobreabundancia de información personal y la amplia volumetría de datos. En ambos supuestos, el factor clave es el comportamiento de los usuarios en las propias redes sociales a través de sus identidades virtuales y de su interacción con el resto de usuarios.

3. Buenas prácticas en el uso inteligente de las redes sociales

El mayor riesgo que suponen las redes sociales no está asociado al modo en que su software está programado, ni a la debilidad o fortaleza de sus conexiones cifradas con los usuarios. El mayor riesgo de las redes sociales está principalmente relacionado con el comportamiento de sus usuarios:

Extremo inteligente: el uso inteligente de las redes sociales implica sacarles el máximo partido para relacionarse con amigos y contactos, compartir información o intereses, y expresar sentimientos y emociones en el ciberespacio; pero, al mismo tiempo, es necesario adoptar rutinas de protección que no distan mucho, en su filosofía, de las mismas que cualquier persona adoptaría en el espacio físico.

Habitualmente, las personas no dejan sus casas abiertas ni expuestas a intrusos, no cuentan intimidades a desconocidos, no dejan sus coches abiertos en la calle o procuran no caminar aislados en la oscuridad de una zona desconocida. Estas conductas, que suponen un modo inteligente de prevenir riesgos en el espacio físico, también tienen su correspondencia en el ciberespacio.

Extremo vulnerable: el comportamiento vulnerable implica descuido y desprotección en la información personal y sensible que se difunde y que se comparte públicamente; en el porcentaje de intimidad que se divulga, accesible tanto a conocidos como desconocidos; y en la aceptación de contenidos sospechosos que pueden conducir a distintos tipos de malware. En definitiva, el comportamiento vulnerable supone salir desprotegido al ciberespacio, como si se transitara descalzo por un camino repleto de cristales rotos.

Al igual que en el mundo analógico, en el ciberespacio no se deben compartir datos personales con desconocidos. Asimismo, se ha de ser muy precavido con los datos que los desconocidos compartan.

El usuario es el "talón de Aquiles" puesto que, aunque el software y los dispositivos hardware puedan dotarse de las últimas medidas de ciberseguridad, al final dependerá de él, de su consciencia de seguridad y de su propia protección para resguardarse. La ingeniería social pretende explotar precisamente esa debilidad potencial del componente humano en las redes sociales, en vez de atacar directamente al software o al hardware para vulnerar la seguridad de un sistema.

La ingeniería social recurrirá al engaño y a la simulación para mostrar a los usuarios escenarios que en realidad no son lo que parecen: anuncios en redes sociales que al cliquearlos conducen a la descarga de malware; avisos fraudulentos simulando provenir de entidades bancarias que conducen a formularios diseñados para robar credenciales de tarjetas de crédito; o trucos publicitarios más o menos burdos para lograr suscribir fraudulentamente al usuario a servicios SMS de tarificación especial.

Figura 4.- Buenas prácticas en el uso inteligente de las redes sociales

Minimizar los riesgos en redes sociales no es muy distinto a reducirlos en el espacio físico: el comportamiento del usuario aumentará o disminuirá el ecosistema para que las amenazas operen maliciosamente. Las buenas prácticas de comportamiento en redes sociales pueden contribuir a reducir o anular las intenciones maliciosas.

El comportamiento inteligente de un usuario comienza en el momento de definir su propia identidad en el ciberespacio, de decidir cómo se quiere mostrar, cómo quiere llamarse, qué aspecto ofrecer o qué intereses compartir; en definitiva, decidir quién va a ser en el ciberespacio.

3.1 Paso 1: Definir la identidad en el ciberespacio

3.1.1 Constituyentes de una identidad virtual

La identidad en redes sociales no está compuesta únicamente por el nombre o el alias, el screen name o el username, que se emplea para abrir una cuenta en cualquiera de las plataformas disponibles (Twitter, YouTube, Facebook, Instagram, Snapchat, WhatsApp, LinkedIn, etc.). La identidad es todo aquello que "identifica de manera estable" a una persona, algo así como los rasgos permanentes que hacen que una persona sea ella misma (individualización) y sea distinguible de las demás (diferenciación) en redes sociales.

Haciendo un paralelismo entre el ciberespacio y el espacio analógico, la identidad analógica podría estar compuesta por un nombre, tal vez un apodo, un trabajo, unos estudios, un lugar de residencia y otros elementos que se toman como referencia social para definir de manera estable a un individuo –su familia, sus aficiones…–. Información que es trasladable al ámbito virtual del ciberespacio, donde los usuarios en redes sociales quedan definidos por el nombre y alias que adoptan, por la imagen que sitúan como perfil, por la declaración de *bio* (biográfica) que escriben o por las redes sociales en las que tiene presencia.

Asimismo, hay otros parámetros, constituidos por los contenidos compartidos a través de los perfiles que definen la identidad de un individuo en redes sociales de una forma más dinámica, menos estática y, por tanto, más variable.

3.1.1 Constituyentes de una identidad virtual

A diferencia del espacio analógico, lo que se define en redes sociales acerca de un individuo quedará archivado en los hipervínculos de internet, en la memoria del ciberespacio, probablemente para siempre.

En redes sociales la personalidad de un individuo, es decir la *expresión comportamental de su identidad*, se traduce a través de **contenidos**, de la manera en la que la persona se expresa por medio de mensajes que comunican acciones, pensamientos o sentimientos. Por tanto, los contenidos que se comparten comunican *rasgos de personalidad,* traducen las esencias de la identidad de un individuo a comportamientos en relación con las otras personas **(relaciones interpersonales)** y con el entorno.

A diferencia del espacio analógico, lo que se define en redes sociales acerca de un individuo quedará archivado en los hipervínculos de internet, en la memoria del ciberespacio, probablemente para siempre. Incluso, en el caso de los menores, se sabe que el 81% de los bebés tiene presencia en internet a través de sus padres . Es el denominado "*sharenting*", un anglicismo proveniente de *share* –compartir- y *parenting* –paternidad-, que señala la práctica, cada vez más común, por parte de los padres de compartir fotos, vídeos e información acerca de sus hijos en redes sociales. En muchos casos, sin ser conscientes, se facilitan detalles de los hijos que favorecen el robo de identidad o impactar en el tiempo sobre el honor y la reputación del menor.

En este sentido, una buena práctica sería preguntarse:

- **¿Qué pretendo socialmente al constituirme un perfil en redes sociales?**
- **¿Qué imagen de mí mismo quiero mostrar a los demás en redes sociales para lograr ese propósito que pretendo?**
- **¿Quién quiero ser o cómo quiero que los demás me vean cuando visiten mi perfil en redes sociales?**
- **¿Puede causarme algún problema ahora o en el futuro el contenido que subo a mi perfil?**
- **¿Estará de acuerdo mi amigo, compañero de trabajo o padre de otro niño en que suba alguna fotografía?**
- **¿Cuándo mis hijos sean mayores estarán de acuerdo en que su vida esté en internet desde su más tierna infancia?**

3.1.2 Lo que soy, lo que parezco ser, lo que podría ser: riesgos sobre la identidad en el ciberespacio

En el mundo analógico o físico la identidad individual es conocida, en mayor o menor medida, por uno mismo y por aquellas personas con las que nos relacionamos más de cerca: familia, amigos, compañeros de trabajo, etc.

En el ciberespacio, los perfiles personales que se constituyen en redes sociales están basados en información incompleta y, principalmente, en la ausencia de contacto interpersonal físico, pudiendo llevarse nuestros contactos una impresión equivocada o distorsionada de nuestra identidad, más basada en lo que *parezco* ser que en lo que realmente soy.

En muchas ocasiones, *parecer ser algo distinto a lo que soy* es un efecto que busca intencionadamente una persona cuando define un perfil en redes sociales, tal vez tratando de ofrecer una imagen mejorada o destacando algún aspecto concreto que potenciar.

En otras ocasiones, la información que uno mismo o sus contactos difunden hace que podamos ser involuntariamente *otra identidad distinta de la que somos* o de la que queremos voluntariamente parecer ser, por manipulación o utilización ilícita por terceras partes.

La información descriptiva sobre una identidad puede tener una presencia en redes sociales que no se ajusta a los deseos de la persona. Los riesgos de que se produzcan estos **efectos indeseados de pérdida de control de una persona sobre su identidad en el ciberespacio** se incrementan en las siguientes circunstancias:

La cantidad de detalles personales disponibles en el ciberespacio incrementa el riesgo de que sean utilizados maliciosamente: a mayor disponibilidad de datos, mayor probabilidad de utilización ilícita con intenciones maliciosas.

5. https://usolovedelatecnologia.com/sharenting/

3.1.2 Lo que soy, lo que parezco ser, lo que podría ser: riesgos sobre la identidad en el ciberespacio

Cuando el **nombre completo del sujeto** (nombre y dos apellidos) es publicado en uno o varios perfiles en redes sociales, la posible utilización ilícita aumenta cuanto más característico estadísticamente sea el nombre del sujeto.

En primer lugar, con un nombre como "Epifanio Torreblanca Altaguardia" es más fácil rastrear en internet información adicional sobre un sujeto, no así si hay que *googlear* "Juan Sánchez", donde se obtendrán miles de resultados. En segundo lugar, cuando se realiza suplantación de identidad, un nombre diferenciador es más útil que un nombre común, puesto que el diferenciador, si además va acompañado de información adicional de verificación, produce un efecto psicológico de mayor credibilidad.

Aunque parezca no intuitivo, es más atractivo robar una identidad altamente diferenciable como "Epifanio Torreblanca Altaguardia" que "Juan Sánchez".

Cuando se divulga la **localización exacta del domicilio** de la persona a través de redes sociales. El nombre y el domicilio de un sujeto son dos rasgos principales de su identidad administrativa, que en manos malintencionadas puede ser información muy útil para realizar fraudes de suplantación de identidad.

La exposición del **número de DNI o de pasaporte**, junto al nombre de una persona, puede emplearse para la falsificación de identidades que se hagan pasar por el sujeto que ha divulgado su DNI o pasaporte.

Al transmitirse en abierto, a través de cualquier red social, un **número de cuenta corriente bancaria o de tarjeta de crédito**. Los grupos cibercriminales tienen diseñados procedimientos para trasladar inmediatamente a tarjetas físicas los números de tarjeta obtenidos fraudulentamente en el ciberespacio.

Siempre es recomendable no transmitir números de cuentas bancarios o tarjetas de crédito, puesto que una vez que el mensaje está circulando ya ha dejado de estar bajo control, por mucho que redes sociales como Facebook o Twitter, o sistemas de mensajería interna como WhatsApp, tengan sus conexiones cifradas.

Distribuyéndose el **número de matrícula de un vehículo** propiedad del sujeto. La matrícula del vehículo, junto al nombre del sujeto obtenidos en el ciberespacio, podría emplearse en diversos procedimientos de estafa. A veces googleando un número de matrícula se obtiene la dirección postal de una persona, o al menos su posible área de residencia debido a una sanción administrativa que ha sido publicada.

3.1.2 Lo que soy, lo que parezco ser, lo que podría ser: riesgos sobre la identidad en el ciberespacio

- Difundiéndose la **dirección de correo electrónico** junto al nombre de la persona que tiene asignada esa dirección. Su difusión descontrolada puede derivar en que esa dirección sea empleada como origen o destino de campañas de spam o de phishing.

- Cuando amigos o contactos de una persona difunden, sin mala intención, **información identificativa de otra** –como la dirección de su domicilio, la matrícula de su vehículo, su nombre completo u otros datos sensibles–. Esta difusión puede realizarse mediante texto, pero también mediante imágenes o etiquetados. Por ejemplo, una persona que no tiene perfiles en redes sociales puede ser etiquetada a nombre completo, por otra que sí lo tenga, en una fotografía donde ambos posan con el vehículo del primero, dejando a la vista la matrícula completa.

La información sobre la identidad, que un usuario aporta en redes sociales, puede crear escenarios favorables a perder el control sobre la misma, siendo aprovechada por personas o grupos con intenciones maliciosas para suplantar su identidad, para deformarla o hacerla parecer algo distinto a lo que es.

Con el fin de maximizar las posibilidades de control sobre la propia información en el ciberespacio, una de las buenas prácticas recomendadas es pensar antes de inscribirse en una red social: pensar qué se pretende con la presencia en esa red social, qué imagen se quiere dar y qué parte o partes de la vida se tiene intención de compartir socialmente, muchas veces con desconocidos.

3.2 Paso 1: Definir la identidad en el ciberespacio

3.2.1 Identidad: proteger nuestra imagen y reputación en el ciberespacio

La reputación digital es "googlear" su nombre para que dicen de esa persona en Internet o en la redes sociales, empresas, universidades y otros colectivos. Es muy difícil borrar o modificar contenidos de las redes sociales.

La reputación digital, la imagen positiva o negativa en el ciberespacio, depende muy a menudo de los contenidos que uno mismo (o conocidos) sitúa en redes sociales. Y esa imagen, una vez constituida en el ciberespacio, es difícil de borrar o modificar pues, como se advierte constantemente, cuando un contenido entra en internet es muy complicado hacer que desaparezca de este ecosistema.

La reputación digital, e incluso el perfilado de los rasgos sobre comportamiento o personalidad de un sujeto, son elementos cada vez más tenidos en cuenta en el ciberespacio. No es únicamente que para hacernos una idea de una persona que acabamos de conocer en el mundo analógico lo primero que hagamos sea "googlear" su nombre para ver qué se dice de ella en internet o qué dice ella de sí misma en sus redes sociales; empresas, universidades y otros colectivos recurren cada vez más a la observación, o incluso al análisis profesional de las redes sociales como elemento de criba o aceptación.

No hay que olvidar que los usuarios son los que tienen el primer control sobre el contenido que se divulga en redes sociales de manera que, aplicando un mínimo de reflexión sobre lo que se hace, antes de hacerlo, se podrá prevenir consecuencias indeseadas sobre la identidad publicada.

Como regla general, en el momento de aportar la información básica sobre la identidad al constituir un perfil en redes sociales, es recomendable tener en cuenta los siguientes aspectos:

3.2.1 Identidad: proteger nuestra imagen y reputación en el ciberespacio

Nombre de pantalla o de perfil. Sobre el nombre de pantalla, lo primero que tendría que pensar un usuario es si va a utilizar un alias digital o, en cambio, el mismo nombre que tiene en el mundo analógico. Si se elige un alias, se ha de tener en cuenta que este estará vinculado a la persona y, por tanto, definirá de alguna forma su identidad digital. Por tanto, otras personas podrán extraer juicios a priori, sin conocer a dicha persona, únicamente basándose en el alias.

Si se elige el nombre del usuario, es conveniente no aportar toda la información sobre el nombre, principalmente si ese nombre es muy diferenciador. Cuanto más diferencial sea el nombre de una persona al completo, más facilidad tendrán personas con intenciones maliciosas para apropiárselo. En general, es recomendable utilizar el nombre de pila y el primer apellido, sin exponer segundos nombres o segundos apellidos.

Hay que tener en cuenta que, aunque un perfil en redes sociales esté definido como absolutamente privado por el sujeto, al menos su nombre de pantalla, su nombre de usuario y su icono de perfil serán totalmente públicos.

Nombre de usuario. Es el nombre corto con el que se efectúa el registro en una red social. Habitualmente está compuesto por caracteres alfanuméricos y no puede coincidir con el de otro usuario registrado.

Una buena práctica para evitar que nuestro nombre de usuario pueda ser utilizado por personas o grupos con intenciones maliciosas es **evitar hacerlo coincidir con el nombre de usuario de nuestra dirección de correo electrónico habitual.**

Aunque es una costumbre habitual que una persona intente mantener un mismo nombre de usuario en varias redes sociales –que puede coincidir con un alias como si fuera un rasgo identificativo para esa persona en el ciberespacio–, hacerlo igual que el usuario de nuestra dirección de correo electrónico habitual facilita a un individuo o grupo cibercriminal obtener nuestra dirección de correo electrónico.

Esta práctica se conoce como **guessing method** (el método de adivinar) y es común en prácticas fraudulentas o ciberataques, basados en obtener masivamente direcciones de correo electrónico, como el phishing o la distribución masiva de correos basura o con timos **(scamming)**.

La obtención de la denominación de una dirección de correo electrónico de una persona también es un paso muy útil para la suplantación de la identidad digital de una persona.

Figura 5.- Ejemplo de nombre de usuario ya registrado en Twitter

Si una persona utiliza en sus cuentas de Skype, Facebook, Twitter e Instagram el usuario '*amapola*', aunque no haya comunicado nunca públicamente su dirección de correo electrónico habitual y la mantenga protegida en su privacidad, si esa dirección de correo electrónico es amapola@gmail, amapola@hotmail o amapola@yahoo, un cibergrupo o individuo con intenciones maliciosas la *adivinará* en cuestión de segundos.

Icono o imagen de perfil. Es la representación visual de la identidad de una persona en redes sociales, secundariamente acompañada en algunas plataformas por la denominada "imagen de portada".

La buena práctica más evidente en la gestión de imágenes de perfil en redes sociales se deriva de entender que los iconos de perfil, al igual que las declaraciones biográficas o el alias que utilicemos en redes sociales, van a hablar de uno mismo en el ciberespacio.

Figura 6.- Ejemplo de icono de perfil e imagen de portada en Facebook

Por tanto, la manera más inteligente de emplear los iconos de perfil en redes sociales, a efectos de proteger y gestionar **la reputación digital**, es pensar muy bien qué se quiere transmitir sobre uno mismo a través de las imágenes identificativas en redes sociales.

Lo primero a tener en cuenta antes de situar una imagen representativa de manera estable en redes sociales, como el icono de perfil, es pensar que a partir del momento en que se **suba**, ya se habrá perdido el control sobre ella. En ese contexto, hay que considerar que las imágenes pueden ser descargadas, manipuladas y circuladas por otras personas con intenciones desconocidas.

Una recomendación general adicional es no situar como iconos de perfil imágenes de naturaleza administrativa oficial; por ejemplo, la fotografía del Documento Nacional de Identidad, del pasaporte o de una tarjeta identificativa laboral, pues este tipo de imágenes facilitan la labor a personas que pretendan falsificar documentos suplantando nuestra identidad.

Localización. La mayoría de redes sociales tienen habilitado un campo en el momento de la inscripción del perfil para situar la localización del sujeto. En este caso, no se trata de la localización del usuario en cada momento, sino de su localización habitual, por ejemplo, la ciudad en la tiene su domicilio, en la que nació, la ciudad en la que trabaja o con la que se siente identificado por cualquier circunstancia.

Además, redes sociales como Facebook o Instagram permiten añadir una etiqueta de localización individualmente a cada contenido que se divulga a través del perfil.

La buena práctica más evidente para perfiles personales en redes sociales es no consignar direcciones postales específicas como localización del usuario del perfil. Empresas, negocios o instituciones tienen de manera habitual su dirección postal localizada a través de mapa en redes sociales, lo cual facilita sus relaciones de negocio o de contacto. En cambio, los perfiles personales que comuniquen su dirección postal en redes sociales pueden exponerse a riesgos e imprevistos.

Una banda criminal especializada en la localización y sustracción de vehículos de alta gama podría emplear la información obtenida en redes sociales para, con algo más de indagación, situar la posición habitual del vehículo y robarlo. Lo mismo puede ocurrir con lugares de domicilio característicos.

Declaración biográfica. En la mayoría de redes sociales es habitual que en la descripción general del perfil haya reservado un espacio para que el

usuario haga una declaración, que la mayoría de las personas emplean para autodescribirse.

Es bastante habitual consignar la profesión del usuario en redes sociales destinadas a contactos personales (como Facebook o Twitter), sin contar con las redes sociales concretamente destinadas a promover los contactos profesionales o laborales, como LinkedIn o Viadeo.

No por ser una práctica habitual está carente de riesgos, tanto conectados al mundo analógico y físico como generados y desarrollados en el ciberespacio. A los consabidos riesgos de suplantación de la identidad, que se facilitan cuantos más datos concretos de un sujeto estén disponibles en sus redes sociales, se une la posibilidad de que la declaración de la profesión de un sujeto en redes sociales sea el vector de ataque utilizado por un grupo cibercriminal para convertirlo en objetivo de diseminación de malware.

Si dicho grupo conoce qué personas están ocupando determinados puestos en una empresa y dispone de su dirección de correo electrónico, los usuarios podrían convertirse en objetivo de una operación de **phishing** dirigido con propósitos de robo de información empresarial sensible, de instalación en la empresa de alguna herramienta software para infiltrarse en los sistemas de información corporativos o simplemente para infectar la red de la empresa con código dañino como el ransomware[6].

Número de teléfono o correo electrónico. Aunque tanto el teléfono como el correo electrónico son datos de contacto que el usuario tiene que consignar obligatoriamente cuando se constituye un perfil en la mayoría de las redes sociales, esos datos permanecen privados, sin exposición pública, únicamente accesibles por el sujeto y por la empresa a la que el usuario los ha cedido en las condiciones de prestación de servicio que el usuario acepta al inscribirse.

Es recomendable **hacer lo que casi nadie hace:** leerse las condiciones de prestación de servicio de esa red social, donde se establecerá si los datos privados comunicados por el usuario, al constituirse un perfil en la red, serán o no compartidos con otras empresas y bajo qué condiciones.

Las organizaciones cibercriminales operan continuamente con **rastreadores automáticos** de internet (harvesters o recolectores), cuyo propósito es detectar y almacenar direcciones de correo electrónico y números de teléfono en bases de datos que posteriormente serán vendidas, al mejor postor, en el mercado negro cibercriminal.

6. El ransomware es un tipo de virus o software malicioso cuyo propósito es bloquear el acceso del usuario a su propia información almacenada en un dispositivo, ordenador, tableta o teléfono, generalmente cifrando esa información y solicitando un rescate económico del usuario para liberarla.

3.2.2 Seguridad: proteger el acceso al perfil en las redes sociales

El nombre de usuario, o la dirección de correo electrónico, y una contraseña son las credenciales de acceso de un usuario a una red social. Específicamente, la contraseña es el elemento que protege al usuario contra accesos ilegítimos e intentos de acceder a su información privada y a sus contactos en la red social.

Una de las causas principales de accesos ilegítimos a información sensible, que debería de estar protegida, es la **debilidad de las contraseñas** elegidas por los usuarios para proteger esa información[7].

Entre las contraseñas más comunes en accesos a servicios a la web, incluidas las redes sociales, destacan "123456", "qwerty" o la propia palabra "password". Estas claves tan simples ofrecen una protección nula ante un atacante para acceder ilegítimamente a un servicio web, vulnerando los derechos del usuario.

Hay redes sociales que obligan a introducir determinados caracteres alfanuméricos en las contraseñas (combinaciones de mayúsculas y minúsculas, de números y de letras, o de caracteres adicionales como el asterisco, la almohadilla o la barra baja), y la mayoría informa con un código de color (verde y rojo) sobre la fortaleza de la contraseña que el usuario está eligiendo para constituir un perfil en una red social.

Pero, ¿qué se consideran **contraseñas fuertes o seguras**? De manera ideal, las contraseñas seguras son aquellas que tienden a ser generadas aleatoriamente, es decir, que su adivinación o previsibilidad por alguien que la desconozca se corresponde con una muy baja probabilidad. Una contraseña fuerte será larga en extensión; combinará números, letras y caracteres especiales de una manera que evite cualquier patrón y tendrá la desventaja para el usuario de que será muy difícil de memorizar.

Las contraseñas más comunes son "123456", "qwerty" o la propia palabra "password". Estas claves tan simples ofrecen una protección nula ante un atacante para acceder ilegítimamente a un servicio web, vulnerando los derechos del usuario.

7. Por ejemplo, un informe de enero de 2017: https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

3.2.2 Seguridad: proteger el acceso al perfil en las redes sociales

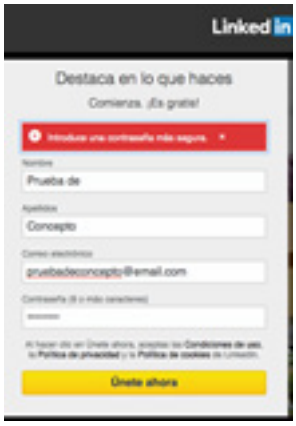


Figura 7.- Ejemplo de intento de inscripción con contraseña débil en LinkedIn

Habitualmente una contraseña débil es predecible porque sigue un patrón (una o varias palabras seguidas o no de un número, secuencias numéricas, fechas significadas para el sujeto). Casi siempre ocurre que una contraseña insegura es débil porque ha sido pensada para ser recordada por el sujeto y no para tener unas mínimas garantías de solvencia en cuanto a proporcionar seguridad.

Se consideran como buenas prácticas en los accesos a un perfil personal en redes sociales las siguientes actuaciones:

1. **Adoptar consciencia personal de autoprotección.** La empresa está obligada a mantener unos estándares de seguridad para proteger la red, en sus componentes hardware, software y humano (sus propios trabajadores), con la que presta servicio, pero llega hasta el límite en donde la protección de la seguridad del usuario recae en el propio usuario.

   Por muy segura que sea una red en el ciberespacio, será tan débil como su componente más inseguro, generalmente el ser humano. Si una red social proporciona cifrado, autenticación con contraseña y se preocupa de auditar continuamente su seguridad para evitar tener vulnerabilidades explotables por atacantes, pero un usuario deja desprotegido el acceso a su perfil por una contraseña débil, será fácil que un tercero no autorizado logre acceso ilegítimo a ese perfil.

   Por tanto, el primer factor para que un usuario aporte protección a sus propios perfiles en redes sociales es que sea consciente de que debe de preocuparse y ocuparse de su propia seguridad haciendo uso de los mecanismos que la red pone a su disposición.

2 **Utilizar contraseñas pseudo-aleatorias.** Es decir, componer las contraseñas utilizando números, letras y caracteres especiales de forma que no sigan patrón alguno y que sean suficientemente largas (seis caracteres o más; cuanto más larga una contraseña, más disminuyen las probabilidades de romperla). Por ejemplo, una contraseña fuerte sería "89Jy$+_'1VwqÇ#", al mezclar todo tipo de caracteres sin seguir ningún patrón.

Obviamente, una contraseña de este tipo es difícil no sólo de recordar, sino también de teclear continuamente por el usuario común. Por tanto, habrá que adoptar otras tácticas para evitar tener que recordar y teclear complejas contraseñas que son seguras, pero "hacen la vida imposible".

Una forma es tener anotada las contraseñas de acceso a las diferentes redes sociales en un fichero de texto, a su vez protegido por una contraseña, archivado en el dispositivo a utilizar (ordenador, teléfono, tableta), con acceso también protegido por contraseña.

Otra manera es tener activada en el navegador de internet la función **"recordar contraseña"** para los accesos autenticados más habituales. Esta opción es razonablemente segura únicamente si el acceso al dispositivo está protegido por contraseña.

Una tercera forma es utilizar "gestores de contraseñas" que son aplicaciones o programas que instalamos en nuestros dispositivos y que se encargan no sólo de almacenar las contraseñas para nuestros servicios en red, sino de generarlas con garantías de seguridad, y de integrarse con los navegadores web para autenticarnos en nuestros servicios. Si el "gestor de contraseñas" es un software con seguridad auditada y actualizada por su fabricante y tenemos el acceso al gestor protegido por una contraseña fuerte, será un método razonablemente seguro

.

Estas tres (3) opciones de almacenar contraseñas requerirán que el usuario memorice, al menos, una contraseña difícil **(contraseña maestra)**: la de acceso al dispositivo, al fichero de contraseñas o al gestor de contraseñas.

3 **No utilizar la misma contraseña para varias redes sociales.** De esta manera, si la contraseña de acceso a una red del usuario queda comprometida, el resto permanecerán seguras (salvo que la contraseña comprometida sea la denominada contraseña maestra).

4 **No usar contraseñas con formato lee[t8] sobre palabras comunes.** El mundo hacker comenzó en su infancia a comunicarse adoptando ese lenguaje y, por tanto, los diccionarios de software para ataques por fuerza bruta pueden incorporar las variaciones leet de las palabras más comunes.

8. Leet: sustitución de letras por números o caracteres especiales

Si se le añaden mayúsculas y caracteres especiales al principio y final, como el dólar o la barra, se tiene una contraseña robusta y fácil de recordar por mnemotecnia al tener un color y número favorito encadenados en leet por una almohadilla: "$R0j0#s13T3/"

5 **No usar contraseñas que contengan datos personales**, como fechas de nacimiento o aniversarios, lugares importantes, motes o segundos nombres. Un atacante probará con toda la información personal que conozca de un usuario si está intentando adivinar su contraseña.

6 **Alternativamente, emplear autenticación en dos pasos.** Redes sociales como Twitter, Facebook o Google tienen implantada la opción de verificación en dos pasos para el acceso de los usuarios a su perfil desde sus dispositivos.

Además de la contraseña (primer paso), se pedirá que introduzca un código numérico (segundo paso) enviado generalmente por SMS al número de teléfono que el usuario tiene registrado en ese perfil de la red social. En todos los casos de autenticación en dos pasos será imprescindible que el usuario haya inscrito su número de teléfono en su perfil de la red social.

Figura 8.- Menú de configuración de autenticación de dos pasos en Facebook

3.2.3 Privacidad: lo que se muestra y lo que se oculta

En redes sociales, la privacidad es el parámetro que regula lo que el usuario muestra y oculta públicamente en redes sociales. La privacidad suele estar asociada, en la mayoría de las redes sociales, a dos tipos de información:

- La propia información descriptiva del perfil, por ejemplo, el correo electrónico de contacto, el número y la identidad de los amigos y contactos.
- Los contenidos individuales que el usuario divulga a través de mensajes, imágenes, audios, likes o comentarios en la red social.

Al constituir un perfil, cada empresa que gestiona una red social presenta al usuario unas "condiciones de servicio" en forma de varias decenas de páginas que se pide al usuario que "lea" antes de continuar y que finalmente "acepte", si está de acuerdo con esas condiciones. Ningún usuario puede abrirse un perfil en una red social sin aceptar las condiciones de servicio que le presenta la empresa gestora de la red social.

Las condiciones de servicio para que un usuario se inscriba en una red social tienen naturaleza de contrato legal vinculante entre las partes (entre el usuario y entre la empresa gestora de la red social, por ejemplo, Facebook Inc. o Twitter Inc.), y ese contrato regula las relaciones entre la empresa operadora y el usuario.

Todas las empresas que gestionan redes sociales tienen publicadas sus condiciones de privacidad, es decir, de cómo gestionan y tratan los datos que los usuarios están alojando en los servidores web de esas empresas cuando crean un perfil en la red social[9]. En esas condiciones de privacidad, se establece no solo la manera en que las empresas operadoras de las redes sociales comparten la información que les es aportada voluntariamente por los usuarios, sino también qué datos adicionales del usuario están recogiendo las empresas automáticamente, previa aceptación del usuario, sin que el usuario sea consciente.

9. Por ejemplo, Facebook [https://www.facebook.com/about/privacy/], Twitter [https://twitter.com/privacy?lang=es], Instagram [https://www.instagram.com/about/legal/privacy/?hl=es], Snapchat [https://www.snap.com/es/privacy/privacy-policy/]

3.2.3 Privacidad: lo que se muestra y lo que se oculta

Figura 9.- Empresas con las que Facebook declara compartir datos sobre sus usuarios

Por ejemplo, entre la información que Snapchat declara que recoge de sus usuarios, además de los contenidos que cada usuario divulgue y aporte en su interacción diaria con la red social, existen metadatos sobre contenidos divulgados, información sobre la actividad, información de la ubicación del sujeto (si el sujeto la tiene activada) o acceso a la cámara y fotos del sujeto almacenadas en su dispositivo, previa solicitud de permiso por parte de Snapchat.

Respecto a la privacidad de los contenidos divulgados por cada usuario en redes sociales, cada red tiene establecidas las posibilidades de proteger los contenidos total o individualmente para que solo sean accesibles por el propio sujeto y por sus contactos/amigos.

Por ejemplo, Facebook permite proteger con un filtro de privacidad cada contenido individual difundido en la red social, clicando en un desplegable asociado a cada contenido individual; sin embargo, Instagram o Twitter permiten definir la privacidad en el menú de configuración de cada perfil protegiendo todo el contenido de mensajes enviados por el usuario, de manera que sólo sean visibles para los seguidores (*followers*) del perfil, pero no disponen de la opción de configurar cada mensaje individualmente como privado.

3.2.3 Privacidad: lo que se muestra y lo que se oculta

Figura 10.- Menú desplegable en cada contenido individual de Facebook para su privacidad

Figura 11.- Opción de proteger con filtro de privacidad todos los mensajes en Twitter

Con relación a la privacidad de la información descriptiva del perfil de un usuario en redes sociales, algunas tienen posibilidad de configurar la visibilidad del perfil. La opción de que otras personas localicen un perfil, buscando por correo electrónico o número de teléfono, habitualmente viene activada por defecto en Facebook y Twitter en el menú de configuración del perfil.

Figura 12.- Configuración de la visibilidad del perfil en Facebook

3.2.3 Privacidad: lo que se muestra y lo que se oculta

Otra cuestión relevante que los usuarios de redes sociales han de tener en cuenta en el momento de reflexionar y actuar sobre la privacidad de su perfil es la geolocalización tanto del perfil como de sus contenidos.

Figura 13.- Configuración de la geolocalización de contenidos en Twitter

En Snapchat, por ejemplo, no está disponible de momento la opción de geolocalización por defecto, pero sí la función denominada "geofiltros", que permite a los usuarios utilizar etiquetas gráficas de lugares para mostrar dónde (la ciudad) se encuentran o con qué lugar se identifica el contenido compartido.

Figura 14.- Ejemplos de geofiltros en Snapchat

Otra funcionalidad, que las redes sociales han incorporado en los últimos tiempos, en relación con la privacidad de los usuarios, es el **cifrado de los mensajes y contenidos** que se comparten a través de la red social.

No obstante, el cifrado es una propiedad que no evita que cualquiera pueda leer o visualizar contenidos que nosotros compartimos con la intención de que sean públicos; el cifrado no está pensada para eso en el caso de las redes sociales. Lo que proporciona el cifrado es protección para evitar que, si un atacante con intenciones maliciosas

es capaz de interceptar el tráfico de datos entre el dispositivo de un usuario y su red social, el contenido de esos datos interceptados no aparezca en claro.

Algunas redes sociales de mensajería privada, como WhatsApp, tienen implantado por defecto el cifrado entre usuarios, de forma que la comunicación entre estos se cifra automáticamente. Otras redes sociales, como Facebook, proporcionan la posibilidad de configurar, dentro de la pestaña de seguridad, la utilización por parte del usuario de su propia clave de cifrado PGP para sus comunicaciones con otros usuarios.

Figura 15.- Pestaña de configuración del cifrado en la configuración de Facebook

Otro capítulo vinculado a la privacidad de la información personal de un usuario en redes sociales está relacionado con compartir la **libreta de contactos** que el usuario tiene en el dispositivo móvil con el que se conecta a esa red social, o la lista de contactos que el usuario tiene en otra red social.

En la mayoría de los supuestos, otorgar permiso a la red social para acceder a la libreta de direcciones del teléfono móvil es obligatorio, si se desea instalar la app de Android o de iOS y conectar a una red social. En algunos casos, como Facebook o WhatsApp, los permisos incluyen incluso la posibilidad de que la *app* "modifique" los contactos del usuario en la libreta de direcciones del teléfono, por ejemplo, añadiendo algún dato en algún campo concreto.

Figura 16.- Permisos que apps móviles de Snapchat, Facebook y WhatsApp solicitan respecto a contactos

Los contactos a los que la app de una red social accede en la libreta de direcciones no se insertan en el perfil del sujeto, salvo que el sujeto los "importe" y añada, y tampoco se divulgan, salvo que el sujeto realice expresamente esa acción a través de su configuración de privacidad. No obstante, todos esos contactos pasan a formar parte de la base de datos de vinculaciones de usuarios que mantiene la empresa gestora de la red social, legítimamente autorizada por los usuarios a través del contrato de condiciones de servicio.

3.2.4 Riesgos derivados de la seguridad y la privacidad

Tanto la privacidad como la seguridad de un perfil en redes sociales regulan el control del sujeto sobre la información compartida y el canal a través del cual se comparte. Los riesgos potencialmente asociados a la seguridad y a la privacidad serán aquellos que comprometan o hagan disminuir el nivel de control que tiene el usuario sobre su canal (su perfil) o la visibilidad de sus contenidos.

3.2.4 Riesgos derivados de la seguridad y la privacidad

La seguridad regula la capacidad que tiene el sujeto para evitar que otros usuarios accedan y, por tanto, controlen la información y el propio canal de comunicación (el perfil en la red social).

La privacidad interviene en regular qué contenidos compartidos por el propio sujeto en la red social se muestran, son visibles a otras personas en el ciberespacio, ya sean usuarios o no (internautas generales) de la red social.

Entre las amenazas y vulnerabilidades, es decir los riesgos, más directamente asociados a cuestiones de seguridad o de privacidad en redes sociales están:

- **Utilizar contraseñas débiles o basadas en datos personales** públicamente conocidos del usuario, como por ejemplo su cumpleaños, el nombre de su mascota, su grupo musical o su película favorita.

- **Compartir contraseñas con otras personas**, aunque sean de confianza. Por definición, compartir un secreto incrementa las probabilidades de que ese secreto sea desvelado, pues aumentan las fuentes a través de las cuales puede divulgarse.

- **Falta de consciencia de identidad en el ciberespacio.** Cuando un sujeto tiene varios perfiles en diversas redes sociales, los rasgos de su identidad en el ciberespacio no son función de cada uno de los perfiles aislados, sino de todos los perfiles en conjunto. Es decir, un usuario puede evitar declarar su localización o profesión en el perfil que tiene en Facebook, pero hacerlo en su cuenta en Twitter o en Instagram.

  Por tanto, lo recomendable es tomar consciencia de que toda la información sobre uno mismo que se divulgue a través de cualquier medio en internet será una pieza para componer el puzle en el que finalmente aparecerá el rostro de uno mismo. Un individuo con intenciones de "resolver el puzle" sólo tendrá que ir recogiendo pieza a pieza hasta que componga una imagen más o menos nítida del usuario.

- **Imágenes que exponen información no deseada.** Por ejemplo, son comunes fotografías de retrato personal o selfis en los que aparece un sujeto sobre el fondo de su oficina en el lugar de trabajo, de su domicilio o de cualquier otro lugar personal. En ocasiones, los fondos de esas imágenes, que no son el centro de la fotografía que se quiere compartir, revelan información identificativa del sujeto o de su empresa que tal vez el propio usuario no desea divulgar.

En estos casos, la recomendación es revisar aquellos contenidos identificativos (nombre de nuestra empresa, matrícula de nuestro vehículo o del vehículo de un amigo o familiar) que el usuario pretende mantener protegidos por privacidad.

Etiquetamiento de terceras personas. Se puede vulnerar la privacidad de las personas, incluso de aquellas que ni siquiera tienen perfiles en redes sociales, etiquetando su nombre en fotografías o imágenes.

Es decir, a través del etiquetado, alguien que no tiene presencia voluntaria en redes sociales puede acabar teniendo presencia involuntariamente, quedando expuesta su privacidad, su nombre, su rostro y sus contactos y amistades. Para prevenir estos riesgos, se recomienda ser cautelosos con el etiquetado de personas en fotografías, solicitando el consentimiento previo de esa persona antes de etiquetar su nombre en una imagen que va a ser difundida en redes sociales.

Desvelar trayectorias geográficas. El etiquetado geográfico de contenidos, o geolocalización, podría permitir conocer un porcentaje significativo de trayectorias geográficas y, por tanto, realizar un control de itinerarios (mapa de tiempos y de lugares) sobre un usuario en redes sociales, que podría ser empleado maliciosamente.

Se recomienda desactivar por defecto las geolocalizaciones de perfiles y contenidos en redes sociales, activándolos particular e individualmente sólo para contenidos concretos.

Inadecuada configuración del perfil a la hora de darse de alta en la red social, en la medida en que no sea configurado correctamente el nivel de privacidad ofrecido por la propia plataforma. Conviene, de hecho, no elegir las opciones por defecto sino analizar detenidamente cada una de las configuraciones que se ofrecen para mostrar según qué contenido.

Obtención de datos personales con intenciones maliciosas. A mayor abundancia de información identificativa publicada, mayor probabilidad de que se utilicen esos datos para, por ejemplo, intentar responder a preguntas de seguridad y lograr una autenticación ilegítima con el fin de acceder al perfil.

Suplantación de identidad. Teniendo en cuenta que para registrarse en una red social basta con ser titular de una cuenta de correo electrónico, cualquier persona podría darse de alta bajo su nombre verdadero o el de cualquier otro.

Del mismo modo, si perdemos o nos roban el móvil y no está protegido, cualquiera que tenga acceso al mismo se puede hacer pasar por nosotros

en nuestras redes sociales (sobre todo aquellas en las que no hay que autenticarse, como WhatsApp). Por ello es preciso utilizar el bloqueo del terminal y, en caso de detectar que alguien ha suplantado nuestra identidad, denunciarlo.

3.3 Paso 3: Pensar antes de escribir

La naturaleza y el propósito de las redes sociales no es meramente crear un perfil con datos identificativos a modo de una guía telefónica moderna. El principio fundacional de una red social es relacionarse en red compartiendo contenidos.

Los contenidos compartidos son los que otorgan carta de naturaleza a una red social y lo que conforma sus características. Algunas redes están más centradas en la difusión de contenidos multimedia, como Instagram; otras son multipropósito, como Facebook; otras están más centradas en el mensaje rápido y breve, como Twitter; y algunas en componer un currículum vitae profesional, que nos permita establecer relaciones de naturaleza básicamente laboral, como LinkedIn. Esas diferentes orientaciones están determinadas por los contenidos que los usuarios comparten a través de una red social.

La relevancia de los contenidos compartidos en redes sociales reside, esencialmente, en que definen y caracterizan personal y profesionalmente al usuario que los comparte. Hasta tal punto, contenidos compartidos y usuarios que los comparten pueden considerarse mutuamente identificados, pues el auditorio global que habita el ciberespacio suele recurrir al perfil en una red social de una persona para hacerse una primera impresión de esa persona, mirando cómo se ha autodescrito en los identificadores personales, pero, sobre todo, observando qué tipo de contenidos comparte.

La relevancia de los contenidos compartidos en redes sociales reside en que definen y caracterizan personal y profesionalmente al usuario que los comparte. Tendremos que pensar antes de escribir contenidos que pueden perjudicar a través de la redes sociales

Por tanto, precisamente por su relevancia, al igual que se ha sugerido para la descripción de los identificadores personales en el momento de constituir una cuenta en una red social, es recomendable desarrollar un **mínimo instinto de ciberconservación**, una mínima cultura de pensar antes de escribir contenidos que difundir a través de las redes sociales.

3.3.1 Cesión de contenidos: lo que se comparte en la red

La buena práctica más inteligente que puede adoptar un usuario en lo relativo a la difusión de un contenido en redes sociales es tomar consciencia de que, en cuanto el contenido haya sido transmitido, el usuario ya ha perdido el control sobre ese contenido

Con independencia de cómo el usuario haya definido la privacidad de su perfil en una red social, este tiene que ser consciente de que una vez transmitido un contenido, en general, le habrá concedido a la empresa gestora de esa red social significativos derechos de uso sobre ese contenido.

Un elemento general de confusión respecto a los derechos legales sobre los contenidos transmitidos por un usuario en una red social deriva de la distinción (o falta de ella en términos de percepción por parte del usuario) entre propiedad de contenidos y uso de esos mismos contenidos:

- La **propiedad intelectual del contenido** divulgado a través de una red social la ostenta el usuario que lo comparte, salvo que ese contenido esté afectado por derechos de propiedad intelectual previos: por ejemplo, que el usuario esté compartiendo un contenido cuya propiedad intelectual ya está adscrita legítimamente a un tercero.

- El **derecho de uso de los contenidos** de los que un usuario es propietario legalmente puede cederse con amplias atribuciones de uso para la parte a la que le son cedidos esos derechos.

En esencia, por mucho que un usuario sea propietario de los derechos de un contenido, la firma de un contrato jurídicamente vinculante con una empresa que gestiona una red social implica necesariamente la cesión de los derechos de uso del contenido del que el usuario es propietario. El

usuario continúa siendo el propietario, pero la empresa gestora de la red social es usufructuaria, utiliza los contenidos con un amplio margen de maniobra, concedido legal y legítimamente por el usuario.

Básicamente, inscribir un perfil en una red social supone por parte de un individuo otorgar a una empresa, bajo un contrato jurídicamente vinculante entre partes, una licencia de cesión de derechos para una amplia gama de conductas de uso de contenidos e información personal del usuario. En este contexto, el usuario podrá ser propietario del contenido, pero **ha dejado de tener control** sobre su difusión.

En lo que respecta a la cesión de derechos de uso sobre los contenidos alojados en una red social, esa cesión a la empresa gestora de esa red social se realiza bajo contrato con una cláusula a cumplir por ambas partes.

Sin embargo, cuando un contenido es difundido por una red social definiendo su privacidad como pública (es decir, visible a todos los usuarios de esa red social y, en la mayor parte de los supuestos, a cualquier habitante del ciberespacio) el **usuario está cediendo implícitamente el control sobre la circulación y difusión de esos contenidos a cualquier habitante del ciberespacio.**

Cierto es que cuando los usuarios se inscriben en una red social se comprometen, por el contrato que representan las condiciones de servicio firmadas, a "cumplir las reglas del juego" y, por tanto, a ser respetuosos con los derechos de difusión limitados sobre los contenidos de otros usuarios.

Aunque un usuario haya marcado un contenido como difusión privada entre sus contactos, seguidores o amigos, una vez que se difunde ese contenido ya forma parte de la información que es accesible a otras personas, mayormente la lista privada de contactos, seguidores o amigos de la persona que ha divulgado el contenido.

De este modo, cualquiera de ellos puede refundir en abierto un contenido inicialmente marcado como privado por su difusor original, dando lugar a una "desprivatización" de la privacidad original. En redes sociales, la privacidad de los contenidos no es un parámetro absoluto que queda fijado cuando una persona define un contenido como privado, sino que **la privacidad de contenidos es un parámetro relativo e interactivo**, que depende de que otros usuarios, que reciben un contenido privado, lo continúen manteniendo como privado.

Por tanto, **antes de difundir** un contenido a través de un perfil en redes sociales, convendría hacerse las siguientes preguntas:

3.3.1 Cesión de contenidos: lo que se comparte en la red

¿Estoy revelando alguna información personal que me gustaría mantener privada sólo entre mi familia y amigos? Si la respuesta a esta pregunta es afirmativa, lo mejor es no difundir el contenido en redes sociales puesto que, aunque sea marcado como privado, puede ser redifundido voluntaria o inconscientemente por un contacto que haya accedido a ese contenido.

En este sentido, conviene tener presente que hay información personal, que podría poner en riesgo al usuario o a sus allegados, puesto que al revelarla públicamente podría ser utilizada maliciosamente por individuos o grupos cibercriminales para suplantación de identidad o ingeniería social, entre otros.

¿Alguien que viera ese contenido podría pensar que representa mi opinión o mi manera de ser, pensar o comportarme? Si la respuesta a la pregunta es afirmativa, se debe pensar nuevamente si el contenido representa al usuario y qué va a decir de él; no sólo en el plano personal, sino también en el laboral. Y no sólo ahora, también en un futuro, puesto que alguien podría formarse una opinión, basándose en contenidos en redes sociales, y tal vez esa opinión importe.

¿Hay probabilidades de que me vaya a arrepentir de difundir el contenido y quiera borrarlo inmediatamente después de enviarlo porque sea ofensivo o inapropiado? Si la respuesta a esta pregunta es afirmativa, mejor no enviar el contenido. Una vez que se ha emitido por una red social, pueden pasar segundos hasta que el contenido aparezca en el perfil de un contacto, que tarde otro segundo más en redifundirlo; de manera que cuando se quiera borrar, ese contenido habrá adquirido la velocidad de la luz en el ciberespacio y ya no sea posible suprimirlo.

¿El contenido que voy a difundir contiene alguna imagen mía o de mis allegados más cercanos que, con una sencilla manipulación, podría transformarse de una imagen inocua a otra ofensiva o inapropiada? Si la respuesta a esta pregunta es afirmativa, mejor no difundirlo, puesto que puede acabar en un foro de intercambio no deseado, después de ser sometida a ligeros retoques con un programa de edición de imágenes.

Este supuesto es especialmente sensible en el caso de menores de edad, cuya distribución de imágenes en redes sociales debería ser siempre objeto de supervisión por parte de adultos con responsabilidad sobre el menor.

¿El contenido que voy a difundir contiene imágenes de otras personas que no tienen perfil en redes sociales o que tienen sus perfiles totalmente protegidos por privacidad? Entre allegados puede haber personas que por razones legítimas de modo de pensar o de entender la vida no tengan perfiles en redes sociales, pero que en cambio aparezcan

en fotografías representando momentos familiares, sociales o laborales. Puede también darse el caso de que esas personas ocupen posiciones sociales o profesionales en las que convenga un determinado control de su imagen pública.

En esos supuestos, antes de distribuir una imagen que involucre la privacidad protegida de otras personas, es recomendable consultar con ellas la difusión o no del contenido.

¿Si redifundo entre mis contactos un contenido ajeno que acabo de recibir, estaré contribuyendo a colaborar con la difusión de contenidos ofensivos, inapropiados o dañinos, o directamente ilegales? La ingeniería social es un procedimiento mediante el cual se intentan camuflar contenidos dañinos a través de contenidos aparentemente inocuos, incluso atractivos o necesarios para los usuarios (notas informativas, facturas, vídeos impactantes…).

El éxito de difusión de estos contenidos dañinos o inapropiados reside esencialmente en la **cadena de redifusión**. Es decir, que un usuario que lo recibe lo vuelva a reenviar. Por tanto, al recibir contenidos de otros contactos, ya sean conocidos o desconocidos, es recomendable pensarlo un momento y analizar mínimamente el contenido.

¿Estoy seguro/a de que puedo utilizar el contenido que voy a difundir a través de mi perfil? Algunos contenidos que se difunden contienen imágenes de marca, documentos protegidos por algún derecho. A veces la diferencia entre qué contenidos están protegidos, y qué contenidos no, es sutil.

Por ejemplo, difundir un selfi que un usuario se hace mostrando al fondo el logotipo de un edificio de una empresa no estaría, en principio y salvo que concurran otras circunstancias, limitado por derechos, o por lo menos es dudoso que la empresa reclame esos derechos. No obstante, emplear sin consentimiento de tercera parte el logotipo de una empresa o la identidad de una persona con imagen pública para difundir un producto que se desea promocionar a través de redes sociales podría conllevar reclamación de derechos de imagen por parte de la empresa o persona pública cuya imagen se está empleando.

¿Estoy seguro/a de que quiero que el contenido que voy a difundir esté para siempre en Google y cualquiera pueda encontrarlo con una búsqueda? Ante esta pregunta hay que pensar preventivamente que cualquier contenido que difundamos va a estar para siempre en el ciberespacio. Una vez que difundimos un contenido a través de una red social, ya sea en público o en privado, se ha perdido el control sobre el contenido y, por tanto, ese contenido puede acabar indexado en Google, para siempre.

3.3.2 Usos maliciosos o no deseados de los contenidos divulgados

Tanto los contenidos que se difunden y que se reciben pueden ser objeto de usos no deseado o maliciosos:

El uso **no deseado** se produce cuando otra identidad en el ciberespacio emplea contenidos para ser difundidos hacia personas a las que no les interesa, hace circular contenidos en una elevada frecuencia ("no inunda de mensajes"), remite contenidos que se consideran inapropiados, o utiliza contenidos del usuario para darles un uso que no le complace por cualquier razón.

En este supuesto el emisor de los contenidos no está incurriendo en una actividad que implique intención maliciosa o de hacer daño, pero finalmente acaba siendo molesto o inapropiado con su conducta en redes sociales.

El **uso malicioso** implicaría la utilización de cualquier clase de contenido divulgado en redes sociales para obtener un beneficio ilícito y/o ilegal generalmente con perjuicio de terceras personas, o directamente para producir un daño a esas terceras personas.

Ejemplos de uso malicioso son la transmisión de virus informáticos (código dañino) a través de redes sociales o la utilización de contenidos fraudulentos con el propósito de hacer que el usuario se suscriba, mediante engaños, a servicios que conllevan una tarificación especial.

Uno de los primeros espacios de uso no deseado que terceras identidades podrían hacer de los contenidos que transmitimos a través de redes sociales viene enmarcado en la **reputación virtual**. Los contenidos que transmitimos en redes sociales, de alguna manera, definen a los usuarios, dicen algo de él, de sus gustos, pensamientos, ideologías y comportamiento.

Sin embargo, menos intuitivo de ver es el uso que terceras partes interesadas podrían dar a los contenidos que se difunden en redes sociales para **elaborar perfiles psicológicos o comportamentales** de un usuario, perfiles que posteriormente serán utilizados con fines laborales o para predecir e influir en su comportamiento.

3.3.2 Usos maliciosos o no deseados de los contenidos divulgados

Otro uso no deseado de los contenidos que se divulgan en redes sociales, que además de no deseado puede comportar una utilización maliciosa de esos contenidos por parte de otras identidades, es la **utilización de contenidos íntimos de un usuario para perjudicar su imagen o para convertirle en víctima de ciberchantaje**. El sexting es el intercambio de imágenes eróticas que un usuario realiza, inicialmente, en la intimidad de la comunicación con otro a través de redes sociales –generalmente, mediante aplicaciones tipo Messenger en Facebook, mensajes directos en Instagram o Twitter, o por medio de WhatsApp–.

El procedimiento más empleado para la difusión de contenidos maliciosos a través de redes sociales es la **ingeniería social.** Es decir, la utilización del engaño en mensajes para que el usuario se descargue un fichero con el contenido malicioso (un virus, por ejemplo) o pulse en un enlace que le llevará a una web donde va a ser expuesto a una estafa, entre otros.

Tal como su propio nombre indica, la ingeniería social trata de manejar los resortes de las relaciones sociales para obtener un propósito, o de construir un contexto específico para producir un efecto. En el ciberespacio, los procedimientos de ingeniería social se emplean habitualmente para llevar a los usuarios a uno de estos tres (3) destinos:

1. La descarga de un **virus** en su dispositivo.
2. La acción de un **fraude** mediante el cual se le va a pretender suscribir a un servicio de pago, por ejemplo, la suscripción a servicios SMS Premium.
3. La obtención de datos personales (teléfono o correo electrónico) y financieros (datos de tarjeta de crédito) del usuario para **robo** de dinero, suplantación de identidad, fraude u otros propósitos ilegales.

Figura 15.- Pestaña de configuración del cifrado en la configuración de Facebook

3.3.2 Usos maliciosos o no deseados de los contenidos divulgados

Los engaños empleados más habitualmente en ingeniería social y en redes sociales podrían clasificarse en las siguientes categorías:

Contenidos llamativos o atractivos, tales como vídeos impactantes que se recomienda ver, o vínculos a contenidos sobre curiosidades, personajes famosos, noticias alarmantes u otros del mismo tipo. La ingeniería social, en este caso, hace uso de la natural curiosidad humana por el contenido impactante o novedoso para incrementar la probabilidad de que los usuarios hagan clic en el contenido y, a partir de ahí, dirigirlos hacia el virus o el fraude.

Encuestas, que diariamente circulan por redes sociales, especialmente a través de dispositivos móviles, con el propósito aparente de solicitar la opinión del usuario sobre distintos comportamientos de compra para ocultar la finalidad real de la encuesta.

Su objetivo, generalmente, es encaminar al usuario a darse de alta en un servicio de pago por contenidos, de tarificación especial SMS o, en el menor de los casos, pedirle su correo electrónico de contacto, que inmediatamente pasará a formar parte de una base de datos que será vendida y utilizada para convertir al sujeto en receptor de ingentes cantidades de correo basura.

Publicidad de *apps* novedosas o muy solicitadas, que en la mayoría de los casos son *apps* fraudulentas que el usuario descarga a través de un mensaje en redes sociales para encontrarse con que la *app* no era lo que se prometía –última versión del videojuego preferido, optimizador de espacio en el teléfono móvil, antivirus gratuito, utilidad para ver los nuevos contactos en redes sociales, dispositivo para conseguir Wi-Fi gratis–, sino que se trata de apps que contienen algún tipo de código malicioso con el propósito de tomar el control del dispositivo móvil, de robar información sensible como contraseñas o tarjetas de crédito, de secuestrar el contenido para pedir un rescate o, si se es benévolo, de mostrar publicidad no deseada.

Ofertas de vales o cupones descuento en establecimientos comerciales conocidos en los que, tras el engaño del falso cupón descuento que puede llegar por redes sociales o por correo electrónico a veces enmascarado en un sorteo, el propósito oculto es obtener datos personales del usuario para comerciar con ellos o suscribirle, mediante tretas, a servicios de pago de tarificación especial[10].

Reclamo de contactos sexuales o de pornografía gratuita, que bajo apariencia de identidades que ofrecen relaciones íntimas se sugiere al

10. Para un ejemplo de falsos cupones descuento: https://www.osi.es/es/actualidad/avisos/2016/05/de-nuevo-vales-descuento-de-lidl-que-te-vacian-la-cartera

usuario cliquear en enlaces o contenidos multimedia que le acabarán dirigiendo a sitios web donde se le pedirán datos personales para traficar con ellos, se le intentará suscribir mediante manipulación y engaño a servicios de pago, o se descargará código malicioso con diversos efectos nocivos para el dispositivo que esté utilizando el sujeto.

Solución de problemas tecnológicos o de incidencias en las cuentas de usuario, en los que se utilizan mensajes de advertencia simulando provenir de servicios técnicos de proveedores conocidos a los que el usuario puede o no estar suscrito (PayPal, Google, Facebook, Netflix u otros) para informar al sujeto de problemas en su dispositivo o en su cuenta de usuario, sugiriéndole cliquear enlaces o descargarse contenido que pretenderán conducirle hacia un fraude, un virus o robo de datos, contraseñas o dinero. Se emplea un procedimiento idéntico al *phishing* tradicional; pero, en este caso, el engaño se distribuye a través de mensajes en redes sociales en lugar de utilizar el correo electrónico.

3.4 Paso 4: Cuidar las relaciones personales

Aunque la creación de un perfil en una red social está determinada por la definición de los rasgos de identidad –quiénes somos o quiénes nos gustaría parecer–, y posteriormente los contenidos que se divulguen determinarán el modo de comportarse de las personas; los contactos y amigos son lo que proporcionan sentido al propio significado de "red social".

En efecto, una red social es un instrumento, una herramienta de socialización en el ciberespacio; socialización que se materializa a través de los contactos, amigos o seguidores, es decir, las otras identidades con las que nos relacionamos en la red a través del plano cibersocial.

El red social está determinada por la definición de los rasgos de identidad y los contenidos que se divulguen determinarán el modo de comportarse de las personas; los contactos y amigos.

3.4.1 Gestión de relaciones, contactos y amigos

En lo que respecta a la gestión de contactos, los usuarios de redes sociales tendrán que tomar principalmente dos (2) tipos de decisiones:

- **Elegir los contactos:** principalmente al crear el perfil en la red social, pero también a lo largo de toda la vida del perfil, donde se irán haciendo nuevos contactos y se irán perdiendo algunos de los existentes. En algunas redes sociales, hacer nuevos contactos implica realizar solicitudes de amistad a otras identidades y que éstas nos acepten como amigos.

- **Proteger con el velo de la privacidad,** manteniendo la lista de contactos abierta, para que todo el ciberespacio sepa con quién se relaciona (o pretendemos relacionarnos), o bien manteniendo oculta la lista de amigos y seguidores, de manera que sólo sea visible para uno mismo y para sus contactos.

Antes de decidir si se quiere hacer no visible la lista de seguidores, contactos o amigos mediante las opciones de privacidad que tienen establecidas las distintas redes sociales, el primer paso es elegirlos, es decir, comenzar a cliquear "seguir" o a realizar solicitudes de amistad a otras identidades.

Algunas redes sociales solicitan al usuario acceder a su libreta de contactos ya existente para desde ella confeccionar una lista inicial de amigos con la que comenzar a construir el perfil que se acaba de crear. Esta solicitud de acceso es común en las apps de las redes sociales para dispositivos móviles donde los usuarios suelen tener grabados sus contactos de agenda telefónica. En la solicitud de una app a la libreta de contactos de un usuario, hay que distinguir dos (2) conceptos:

- **Solicitud de permisos de la *app*.** Algunas redes sociales, de modo obligatorio para que sus *apps* sean instaladas por el usuario, solicitan permiso para realizar algunas acciones en la libreta de contactos (leerla y modificarla, principalmente). Este permiso **no implica** que los contactos del usuario en su listín telefónico vayan a incorporarse como amigos o seguidores al perfil de la red social que se haya constituido.

3.4.1 Gestión de relaciones, contactos y amigos

Solicitud de importación de contactos. Algunas redes sociales, cuando un usuario está en el proceso de crear un nuevo perfil, le solicitan permiso para importar contactos de otras redes sociales en las que el sujeto ya tenga amigos, o bien de su libreta de contactos. Con la importación de contactos, lo que intenta la red social es absorber toda la lista de amigos de un perfil que el sujeto ya tenga en otra red social o en su teléfono.

Las solicitudes iniciales de acceso a la libreta de direcciones o de importación de contactos no presentan en sí mismas amenazas de seguridad (salvo que concurran otras circunstancias de riesgo, por ejemplo, infección del dispositivo por malware), pero sí **instancias relevantes de la privacidad del sujeto en el ciberespacio.**

En ambos casos, se está cediendo a la empresa operadora de la red social información enriquecida sobre los contactos del usuario en varias redes sociales. Esta realidad no representa un problema a priori, pero sí es una buena práctica tomar consciencia de la implicación de ceder información a varias redes sociales, que están gestionadas por el mismo grupo empresarial, como por ejemplo Facebook, Instagram y WhatsApp, todas bajo el grupo Facebook; o Skype, LinkedIn o Yammer, propiedad de Microsoft.

Por otro lado, en la mayoría de las redes sociales, la estructura de contactos de un usuario se compone de aquellas otras identidades a la que el sujeto sigue en redes sociales, sumadas a los usuarios que realizan seguimiento al perfil del sujeto. En algunas redes, como en Facebook, la adición de nuevos contactos implica "solicitar amistad" a ese contacto para ser aceptado en su red de relaciones.

En cualquiera de los supuestos, ya sea por adición directa de un contacto o por solicitud de amistad, ese contacto pasa a formar parte de la información a la que otras identidades acceden en redes sociales. Si el perfil está difundiendo información en abierto sin protección de privacidad, a través de él otras personas conocerán no sólo quiénes somos (las declaraciones biográficas consignadas), cuáles son nuestros intereses, gustos y en cierta medida nuestros comportamientos (los contenidos que publicamos), sino también con qué otras personas nos relacionamos o nos gustaría relacionarnos.

La estructura de relaciones de un sujeto es una fuente primaria de información para deducir su ideología, sus estudios, su área de desempeño laboral, su probable lugar de residencia y otros factores que, a pesar de que el usuario no los haya declarado expresamente, puede dar lugar a que sean inferidos. Esta información que sería

deducible sobre un sujeto a partir de sus contactos en redes sociales puede ocultarse restringiendo, mediante controles de privacidad, la visibilidad de la lista de contactos, amigos o seguidores del perfil del usuario.

La configuración de la privacidad de los contactos de un perfil está disponible en el menú de configuración de todas las redes sociales, del mismo modo que se activa y desactiva la privacidad para los contenidos. A este respecto, Facebook permite ocultar la lista de amigos manteniendo abiertos los contenidos del perfil, mientras Twitter o Instagram requieren que el sujeto proteja por privacidad todo el perfil (contenidos y amigos) para no hacer visible la lista de contactos del sujeto ante otras identidades que no sean amigos o seguidores del usuario.

Una derivada de la protección de privacidad de la lista de contactos está relacionada con las solicitudes de amistad. Esta intención de nuevas amistades forma parte de la propia naturaleza de las redes sociales, conocer a personas nuevas para entablar nuevas relaciones. Por tanto, es un aporte positivo de las redes sociales como herramientas de comunicación.

Sin embargo, entraña riesgos que un usuario debe conocer y gestionar. El riesgo más evidente de dar entrada (aceptar una solicitud de amistad) a una nueva identidad a la lista de contactos, si está protegida por privacidad, es que el recién llegado tendrá acceso a la información sobre los contactos y la estructura de la malla de relaciones del usuario en esa red social.

3.4.2 Ingeniería social y riesgos de las relaciones en red

La visibilidad de la estructura de amigos y contactos en una red social entraña riesgos potenciales. El más evidente de ellos está asociado a dar entrada en el círculo de contactos a identidades desconocidas, lo que constituye una oportunidad para ampliar y enriquecer el universo de relaciones personales, sociales y laborales, pero que implica una fase de riesgo inicial en la que una persona puede acercarse a otra con intenciones ocultas.

El personaje que se construye como un "yo virtual" para que represente a una persona en redes sociales puede hacer creer que son "amigos".

Un concepto preliminar a tener en cuenta respecto de los contactos que se van adquiriendo en una red social es el **enmarcado de la relación de amistad**. Puesto que las personas se relacionan virtualmente, la inexistencia de la proximidad física es compensada por una tendencia a sobrevalorar el vínculo virtual, dándole más peso sentimental del que se le daría en un proceso habitual de conocimiento mutuo entre personas en el mundo analógico.

Otro elemento que contribuye a que en redes sociales se sobredimensione la naturaleza de las relaciones interpersonales, **considerando amigos a quienes no son más que contactos**, es la propia máscara o personaje que el perfil en una red social representa para cada usuario. En redes sociales se pueden exagerar las virtudes o incluso representar un papel con cualidades que al usuario le gustaría poseer, además de que se tiene más facilidad para ocultar lo que se consideran defectos; de este modo, al conocer a alguien nuevo, al hacer un nuevo contacto e interactuar con él o ella, se intenta autoafirmar lo máximo posible al personaje que se ha construido en la red social.

La particular estructura psicológica y perceptiva que se genera cuando un usuario tiene muchos contactos en una red social le puede llevar a albergar la falsa sensación de que esos contactos son amigos, en el mismo sentido que los amigos en el mundo analógico. Este fenómeno puede originar que se baje la guardia, que **disminuya la percepción del**

riesgo en las relaciones interpersonales con desconocidos y que, por tanto, se otorgue más confianza de la debida en tiempos más cortos de los debidos.

Con acceso a la red de amigos, una identidad maliciosa no sólo puede inferir información sobre una persona que en principio no se desea declarar explícitamente, sino que podría emplear esa información para llevar adelante conductas de ciberacoso de distinto tipo.

Entre el abanico de conductas de ciberacoso, ya ha sido mencionado el sexting sobre contenidos íntimos. La distorsión perceptiva de la amistad virtual es más incidente en niños y jóvenes, ante los cuales personas con intenciones maliciosas e ilegales pueden desarrollar conductas de acoso sexual, que en internet y redes sociales se denominan *grooming*. El *grooming* es el "conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor a través de internet con el fin de obtener concesiones de índole sexual[11]".

Otra modalidad de acoso a través de redes sociales, que afecta particularmente a niños y menores de edad, es el ciberbullying, mediante el cual un agresor trata de socavar la estabilidad emocional de una víctima utilizando los canales en redes sociales, pero también SMS, correos electrónicos o mensajes en WhatsApp, haciendo a la víctima objeto de amenazas, insultos o mensajes intimidatorios (que pueden incluir el chantaje).

En lo que respecta al control del riesgo con relación a mantener "sana" una lista de contactos en redes sociales, un elemento adicional de prevención es efectuar un control de seguidores y solicitudes de amistad para eliminar, en el momento en que se presenten, tanto a seguidores como a solicitudes de las que se tenga la sospecha de que son **bots**.

Los *bots*, cuya denominación responde a la abreviatura de robots, son perfiles automatizados constituidos en redes sociales para desarrollar comportamientos repetitivos que no necesitan la intervención de un humano para ser llevados a cabo. Por ejemplo, un *bot* en Twitter o en Instagram puede estar programado para emitir *likes* o realizar comentarios (siempre iguales, como "bravo", "genial" o "es mejorable") ante contenidos específicos; por ejemplo, cuando se hable de una película, de un libro, de una exposición o de un Gobierno o líder político.

Hay otros *bots* programados para seguir automáticamente a perfiles que hablen sobre determinados temas. Los bots son herramientas útiles en el ciberespacio cuando se trata de automatizar tareas y son cada vez más empleados en campañas de marketing online, en sondeos de

11. http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/grooming-acoso-a-menores-en-la-red.shtm

opinión, en testeo del comportamiento de nuevas soluciones software o para dinamizar el tráfico en las propias redes sociales o en sitios web.

Sin embargo, los bots en redes sociales también pueden ser empleados para generar tráfico no deseado, molesto o directamente malicioso. A continuación, se relacionan ejemplos de escenarios a evitar en los que *bots* pueden estar involucrados:

- **Crear una imagen negativa de una persona o una marca.** Estos bots están programados para emitir mensajes negativos y para ello emiten contenido prediseñado, buscando lograr seguidores que reproduzcan y redifundan esos contenidos.
- **Acosar o presionar a determinadas personas o colectivos,** lo que se denomina en el argot de las redes sociales **trolear** (*trolls* son los *bots* que trolean), conducta que puede llevarse a cabo con *bots* preprogramados para insultar, descalificar o reprochar determinados contenidos o a personas que cumplan ciertas características (por ejemplo, una determinada ideología, orientación personal o afición).
- **Difundir spam, publicidad o servicios no deseados.** Este es el ecosistema más habitual de actuación de los *bots*, que son capaces de transmitir un conjunto programado de mensajes publicitarios y difundirlos sin descanso. En ocasiones, se diseñan bots que contienen publicidad engañosa, cuyo objetivo es captar los clics de los usuarios para redirigirlos a webs de descarga de software dañino. Es decir, distintos tipos de virus que infectarán el dispositivo del usuario con intenciones cibercriminales.
- **Aumentar artificialmente el volumen de seguidores de los usuarios.** Este tipo de bots son creados en masa, del orden de varios cientos de miles, para acumularse en la lista de seguidores o amigos de determinados usuarios para generar una falsa sensación de popularidad en el perfil de ese usuario –usualmente relacionado con la venta de seguidores en redes sociales, cuando un usuario acaba de constituirse un perfil en redes sociales y necesita "tener amigos y seguidores" –. Es habitual la venta de paquetes de seguidores (5 mil, 10 mil, 100 mil).

En estos casos, las **buenas prácticas recomendadas** son:

- **Mantener protegida por privacidad** la información que se considera más personal en los perfiles y que podría exponer a una persona si se conociera públicamente. En general, sería una práctica inteligente no insertar en un

perfil en redes sociales ningún tipo de información personal que se pueda considerar sensible.

Aumentar la prevención en solicitudes de amistad de identidades desconocidas. Antes de aceptarlas, es preferible revisar el perfil de esa persona en esa red social, para cerciorar que se tienen intereses comunes, o que al menos lo que cuenta de sí mismo no hace saltar ninguna alarma. Si el perfil está oculto o restringido o si tiene algún rasgo que a priori "no nos cuadre", la recomendación es no aceptar la solicitud de amistad.

Bloquear a las identidades con intenciones maliciosas o molestas. Situaciones de bloqueo son aquellas en las que otra identidad insulta o comparte con el usuario contenidos inapropiados o que hacen sentir incómodos, como identidades con propósitos de administrar continuamente publicidad o servicios no deseados, perfiles que siguen al usuario o solicitan su amistad para "conseguir más seguidores" o aumentar artificialmente los suyos.

Informar al proveedor de servicios sobre identidades no deseadas. Si se está recibiendo contenido inapropiado, se está siendo víctima de algún tipo de acoso o se considera que una identidad se está comportando inadecuadamente, por principio es recomendable informar sobre esa identidad al proveedor de servicios de la red social. Todas las redes sociales tienen establecido un procedimiento para "denunciar incumplimientos"[12].

Guardar y comunicar los contenidos que se consideren inapropiados o acosadores. Si se comienzan a recibir contenidos específicamente dirigidos a la persona, considerados sospechosos porque parecen insultos, proposiciones inapropiadas, amenazas u otro tipo de expresiones que causan molestia, se debe guardar una copia de esos contenidos, ya que podrían ser de utilidad si hay que presentar una denuncia sobre la identidad molesta o maliciosa.

Activar sistemáticamente la protección por privacidad en los perfiles de menores de edad. Es recomendable cerciorarse de que los menores de edad que crean un perfil en redes sociales activan los controles de privacidad, tanto para contenidos como para listas de amigos, manteniendo en mínimos y sin aportar datos personales, como información visible para el público general en el ciberespacio.

Si a los controles de privacidad se unen la supervisión del perfil por parte de los adultos a cargo del menor y una mínima educación sobre el uso de redes sociales, se estará manteniendo un aceptable estándar de buenas prácticas en la gestión de las redes sociales del menor de edad.

12. https://support.twitter.com/articles/108038

3.5 Paso 5: Adoptar una cultura personal de ciberprotección

La prevención y gestión de riesgos en redes sociales no se logra aisladamente, intensificando y robusteciendo la seguridad de las webs o de las apps desde donde se proporciona el servicio en cada red social; tampoco solo disminuyendo cada vez más las vulnerabilidades de los dispositivos que se emplean para conectarse al ciberespacio, como teléfonos, ordenadores, relojes y poco a poco cualquier objeto de uso cotidiano como el coche o el televisor.

La mejor prevención de riesgos se logra cuando, en un ecosistema donde confluyen varios factores como es el caso del ciberespacio con webs, dispositivos, objetos y personas, **se incrementa sustancialmente la seguridad del eslabón más débil;** y, en el ciberespacio, el eslabón más débil en términos de seguridad es el ser humano, quien al contrario que las máquinas no se puede programar.

La ciberseguridad del ser humano en el ciberespacio puede lograrse parcialmente "obligándole" a realizar determinadas tareas que implican conductas de seguridad. Por ejemplo, impidiendo que elija contraseñas que no sean alfanuméricas de más de ocho caracteres o limitando en los navegadores web la utilización de ciertos tipos de ficheros que se consideran potencialmente vulnerables. Sin embargo, tanto el propio libre albedrío del comportamiento humano como las técnicas maliciosas que utiliza la ingeniería social demuestran una y otra vez que **la ciberseguridad más efectiva es la que comienza por la propia autoprotección del internauta en el ciberespacio.**

El ser humano tiene que protegerse de las amenazas del ciberespacio. Por ejemplo: contraseñas alfa numéricas de más de ocho caracteres o disminuyendo las vulnerabilidades de los dispositivos.

3.5.1 Definiendo al cibernauta inteligente

Dotarse de autoprotección en el ciberespacio requiere del internauta, del usuario de las redes sociales, adoptar un comportamiento de ciberseguridad personal:

- **Tomar consciencia situacional del riesgo.** La autoprotección en el ciberespacio requiere entender que, al igual que sucede en el mundo analógico, también en las redes sociales existen espacios donde identidades maliciosas tratarán de obtener un beneficio ilícito ocasionando un perjuicio a otras personas.

- **Estar informado sobre amenazas y vulnerabilidades.** Conocer de modo general los peligros potenciales que pueden acechar en las redes sociales. La mejor manera de estar informado es suscribirse, en las propias redes sociales, a algún canal de noticias con actualizaciones diarias con consejos y advertencias sobre la seguridad del internauta. En España, el Instituto Nacional de Ciberseguridad tiene habilitada la Oficina de Seguridad del Internauta precisamente con ese propósito, con canales informativos en web y redes sociales[13].

- **Interiorizar y aplicar buenas prácticas de ciberprotección,** estando al tanto de qué conductas ponen en riesgo al usuario en redes sociales y cuáles otras previenen de quedar expuesto a las ciberamenazas. Se han de poner esas conductas preventivas en práctica e interiorizarlas paulatinamente como parte de una **manera segura de navegar** en el ciberespacio.

13. www.osi.es, www.facebook.com/osiseguridad, www.twitter.com/osiseguridad, www.youtube.com/user/OSIseguridad.

3.5.1 Definiendo al cibernauta inteligente

Por tanto, el **cibernauta inteligente** es una persona concienciada e informada, que aprovecha los contenidos que diariamente circulan por sus redes sociales para incluir entre ellos alertas o notificaciones sobre nuevos riesgos y mejores prácticas; que está al tanto de las últimas modalidades de *phishing*, del último contenido dañino o de publicidad no deseada que puede afectarle, de los últimos esquemas de fraude o de los últimos códigos dañinos que se están transmitiendo por redes sociales con la intención de robarle datos personales o dinero.

Es decir, el cibernauta inteligente aprovecha lo que representan las redes sociales como canales de información inmediata y continuada para dotarse a sí mismo de una **cultura personal de ciberprotección y ciberseguridad;** cultura que le convierta en un habitante menos vulnerable del ciberespacio, reduciendo la superficie de exposición y permitiéndole extraer todo el valor personal, social y laboral que podrían proporcionarle las redes sociales. Así, incorporando a sus rutinas diarias de navegación en internet unas sencillas pautas de protección y buenas prácticas, se dejan de lado los riesgos que pueden ser prevenidos.

4. Decálogo de recomendaciones

A continuación, se indican diez (10) recomendaciones de seguridad en el uso de las Redes Sociales

Decálogo de seguridad en Redes Sociales

1. Un sitio permanente encabezado por fotografías, datos personales e información sobre estudios, profesión, gustos, intereses, amigos y familia proporciona mucha más información de la persona que su DNI o Pasaporte. Además, quedaría a la vista de todo el mundo. Es clave, prestar atención a cómo uno define su perfil en redes sociales, ya que será la carta de presentación de su identidad en el ciberespacio.

2. Reflexionar sobre los contenidos que se comparten en redes sociales. Cada vez más personas y empresas observan y analizan las redes sociales para adoptar un juicio sobre otras personas. Si se quiere un juicio justo, se han de controlar los propios contenidos.

3. No compartir contenidos sensibles sobre la vida personal o la de otros en redes sociales: documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos, etc. Cuanto más contenidos de este tipo se compartan, más probabilidades hay de ser víctima de un robo de identidad, de ciberacoso u otra conducta ilícita que utilice esa propia información para perjudicar al usuario.

4. En el ciberespacio aplica el principio de "prevención ante lo desconocido". No hacer clic en contenidos sobre los que no se tenga claro su origen o propósito y aumentar la cautela ante mensajes de identidades desconocidas. En definitiva, huir de la tentación de todo aquello que cuanto más desconocido, más atractivo parece.

5. Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes utilizando dos factores de autenticación donde sea viable.

6. Controlar la geolocalización de perfiles y contenidos en redes sociales. Desactivar la geolocalización por defecto en el menú de configuración de los perfiles y hacer un uso inteligente de la misma, pensando en cada caso si interesa que los demás tengan un mapa de tu vida o de parte de ella.

7. Comprobar la configuración de privacidad tanto en el perfil como en los contenidos que se comparten. Tomar consciencia de que el ciberespacio está lleno de ojos digitales y que se debe mostrar únicamente lo que se está seguro que cualquiera pueda ver. Ante la duda, mantener la información privada para amigos y contactos.

8. No difundir información privada sobre otras personas sin su consentimiento y no etiquetar por su nombre a otras personas que no tienen perfil en redes sociales sin solicitar previamente su permiso para hacerlo.

9. Cuidar y proteger las relaciones en el ciberespacio. Mantener en privado la lista de contactos y analizar en detenimiento las solicitudes de amistad de desconocidos.

10. Adoptar la consciencia de que la primera línea de defensa para la protección en el ciberespacio es uno mismo. De esta manera, la ayuda que instituciones y organizaciones de ciberseguridad presten será mucho más eficiente y uno mismo será de ayuda inapreciable para mantener unas redes sociales seguras.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es