Ciberseguridad y redes sociales

Lucas Giraldo Ríos
Magister en Innovación y Magister en Administración

Grupo de Investigación Masa Crítica – Escuela Superior de Guerra
Grupo de Investigación Griego – Universidad Nacional de Colombia

Administrador de Empresas. Especialista en Gestión Financiera Empresarial y Magister en Innovación y Magister en Administración (MBA), actualmente candidato a doctor en Ingeniería, Industria y Organizaciones (Universidad Nacional de Colombia). Gerente de Consultoría en la firma RSM con más de 18 años de experiencia en el sector empresarial de alimentos, tecnología, servicios, gremiales y educativos en el ámbito nacional e internacional; adicionalmente, docente en temas de Estrategia, Innovación, Prospectiva, Sistemas de Información Gerencial, Gobierno de TI, Transformación Digital y Digitalización (Universidad Nacional de Colombia, Escuela Superior de Guerra, Universidad de Asturias, Instituto Europeo de Posgrados, Universidad Espíritu Santo-Ecuador, entre otras instituciones de Educación Superior).

Foto: https://sutilweb.com/2021/04/26/tunel-informatica/

Introducción

El crecimiento en el desarrollo y el uso de las Tecnologías de la Información y la cada vez mayor dependencia de las redes sociales se ha acentuado debido a su gran valor en todos los niveles tanto de las organizaciones como de las personas, elevando factores como la productividad y en algunos casos facilitando el estilo de vida. La relación de las personas se ha vuelto cada vez más dependiente de la comunicación instantánea a través de Internet y particularmente con el uso de las redes sociales. Con el crecimiento de los dispositivos y aplicaciones móviles, combinado con las tecnologías de redes sociales, la comunicación mediante herramientas de redes sociales en línea se ha convertido en una nueva forma de vida para las personas. (Hathi, 2009)

Así, el incremento de las amenazas que dificultan el progreso e impiden el control total de los datos y la información, resulta de la creciente necesidad de gestionar a través de la tecnología de la información los programas maliciosos que se han propagado de diversas formas y evolucionan continuamente en su complejidad, lo que hace difícil y arduo detener sus efectos negativos. Lo anterior también se evidencia por el crecimiento importante del "trafico" de datos que ha aumentado en los últimos años, implicando tanto a las personas como a las organizaciones. Las personas y las empresas a través de estos, con regularidad corren riesgos con la información cuando se utilizan las redes sociales; elementos como el uso de software no aprobados, un mal uso de los equipos organizacionales, acceso a redes no certificadas o aprobadas por las empresas y el compartir datos confidenciales en redes no seguras dan cuenta de ello. (Maslennikov, Yampolskiy, 2008)

Sumado a lo anterior, en los últimos años se ha producido un aumento significativo en la tasa de uso de las redes sociales a nivel global lo que hace que el tema de la ciberseguridad en los datos de los usuarios y la privacidad de dicha información sean muy importantes.

Redes sociales

El número de redes sociales y usuarios de las mismas ha aumentado considerablemente en los últimos años, junto con la variedad de sus objetivos y usos lo que añade complejidad en su entendimiento, operaciones y control. Las redes sociales varían en características y objetivos, y se pueden dividir en varios grupos a la luz de sus objetivos, tal como en adelante se desglosa.

Sitios de redes sociales

El objetivo principal de este tipo de sitio es localizar personas y participar en sus vidas virtuales, que expresan la realidad de sus vidas personales. Los ejemplos de esta categoría incluyen lugares como *Facebook*, *WhatsApp*, *Twitter*. Aunque estos sitios se establecieron para atender a particulares, en la actualidad hay muchas instituciones que han comenzado a utilizarlos y explotarlos con fines profesionales y comerciales.

Sitios de contacto

El objetivo principal de este tipo de sitios es intercambiar datos y comunicarse entre personas, además de aumentar el número de grupos de usuarios con intereses similares. *LinkedIn* es un ejemplo de un sitio de redes sociales que conecta a colegas y compañeros de programas académicos para construir una red que pueda ayudar a avanzar en la carrera de un usuario.

"… en los últimos años se ha producido un aumento significativo en la tasa de uso de las redes sociales a nivel global lo que hace que el tema de la ciberseguridad en los datos de los usuarios y la privacidad de dicha información sean muy importantes".

Sitios de intercambio de información visual

Estos sitios permiten a los usuarios publicar videos y fotos personales. También les permite cargar películas y programas de televisión. El más importante de estos sitios es *YouTube*, pero también se pueden encontrar lugares que han crecido de manera importante como *TikTok* e *Instagram*.

Sitio Virtual Realty

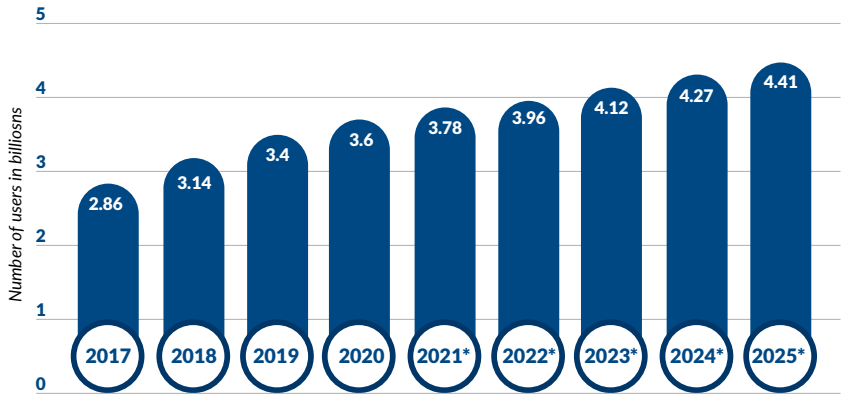
Estos son sitios que crean un entorno virtual en 3D simulando la realidad. Muchos de estos tipos de sitios, como *Second Life*, ofrecen juegos interactivos virtuales que atraen a los jóvenes.

Plataformas de redes sociales como *Facebook*, *LinkedIn*, *Instagram*, *MySpace*, *Snapchat*, *Twitter*, *YouTube* y otras que involucran tanto a usuarios individuales como a múltiples organizaciones han surgido como nuevas plataformas de comunicación en el dinámico y complicado mundo empresarial actual basado en Internet. (Kim, 2012)

La estructura de los servicios de redes sociales se divide en tres elementos. El primero de ellos contiene las aplicaciones de usuario que incluyen varios servicios como web, correo electrónico, mensajería instantánea de voz sobre IP entre otros. El segundo componente presenta los dispositivos de redes sociales, en este punto se encuentran dispositivos no portátiles como computadoras de escritorio y dispositivos portátiles como teléfonos móviles. El último componente es la infraestructura de red que incluye la red telefónica pública conmutada, cables de red, red inalámbrica (WLAN) y red celular.

El crecimiento del número de usuarios de redes sociales en los últimos años es un fenómeno ampliamente reconocido. La empresa Statista ha registrado un crecimiento constante en el número de usuarios en la mayoría de los países de 2010 a 2018 (Statista, 2021). La *Figura 1* muestra este crecimiento significativo en el número de usuarios hasta la fecha y la proyección hasta 2025.

Figura 1. *Número de usuarios de redes sociales alrededor del mundo de 2017 a 2025.*



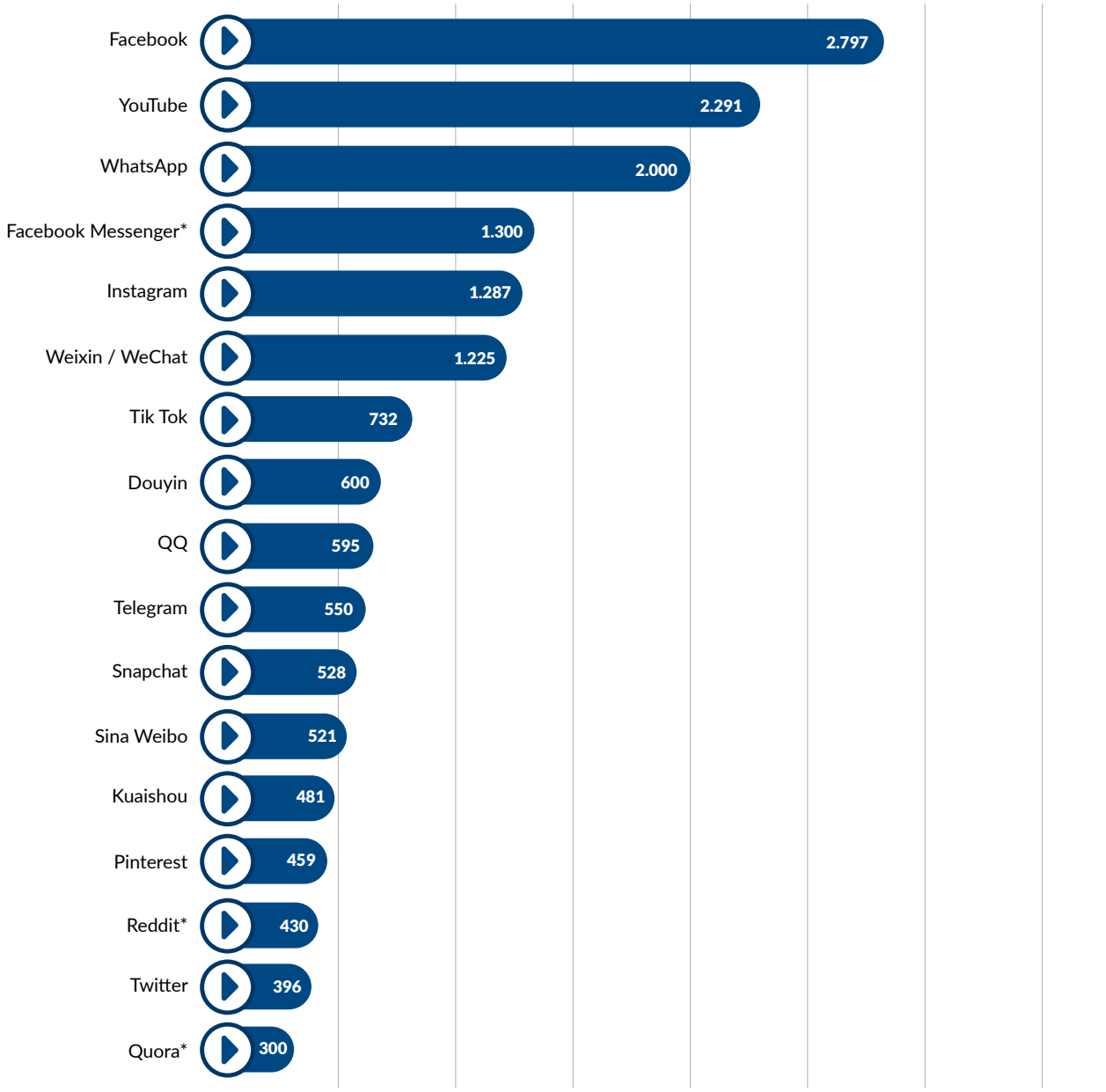
Fuente: Elaboración propia a partir de los datos registrados en Statista (2018)

Foto: https://www.wearemarketing.com/es/blog/nuevas-tendencias-redes-sociales.html

Cabe indicar igualmente, que las redes sociales están ampliamente disponibles en varios idiomas y los usuarios pueden conectarse con otros usuarios en todo el mundo. La Figura 2 muestra los sitios de redes sociales más famosos del mundo clasificados por el número de usuarios activos según lo registrado por la empresa Statista en 2018 (Statista, 2021). Concomitante con el desarrollo continuo de la Web, la tasa de participación de los usuarios ha aumentado y ha cambiado la forma en que los usuarios interactúan con las redes; desde la itinerancia y la navegación entre sitios para acceder a la información, hasta la interacción con los sitios de redes sociales, una consecuencia natural de la evolución de la propia web.

Figura 2. *Redes sociales más usadas en el mundo con corte a Abril de 2021.*

Most popular social networks worldwide as of April 2021, ranked by number of active users (in millions)



Fuente: Elaboración propia a partir de los datos registrados en Statista (2021)

Ciberamenazas y las redes sociales

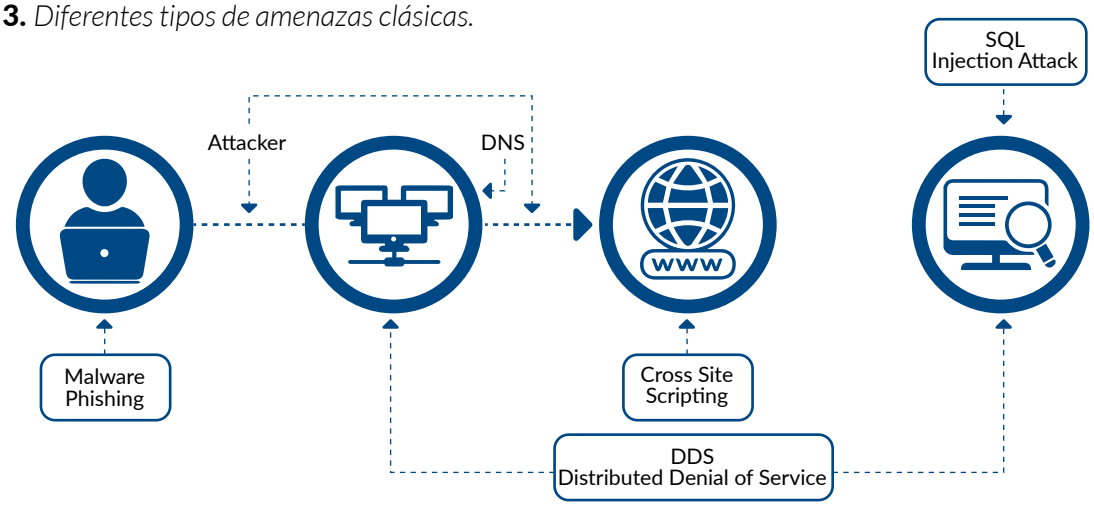
La interacción entre los usuarios en las redes sociales es el factor clave para determinar muchas tendencias en línea, sean estas comerciales, profesionales, sociales o de otro tipo. Además, muchas empresas, instituciones e individuos han aprendido a utilizar las redes sociales como *Facebook*, *Twitter* y *LinkedIn* para interactuar con colegas y clientes.

Como resultado de este rápido crecimiento en el uso de redes sociales, han aumentado las amenazas como *malware*, virus informáticos, *software* espía entre otras, dirigidas a la confidencialidad y la seguridad de los datos. Hay dos tipos de amenazas de Internet y redes sociales; amenazas clásicas y amenazas modernas. Las amenazas clásicas hacen que todos los usuarios de una red determinada sean susceptibles de sufrir ataques; las amenazas modernas están relacionadas con los usuarios de las redes sociales en línea solo debido a la infraestructura de las redes sociales en línea (OSN) que pueden comprometer la privacidad y la seguridad del usuario. (Davison, Maraist, Hamilton & Bing, 2012)

Amenazas clásicas

Desde la llegada de Internet, han surgido amenazas clásicas y sus problemas han aumentado con su desarrollo, las aplicaciones de redes sociales y su uso cada vez más amplio, tal como ya se evidenció. Las amenazas más famosas son las amenazas de *malware*, las amenazas de *phishing*, los ataques de secuencias de comandos entre sitios, los ataques de inyección SQL y los ataques distribuidos de denegación de servicio (DDoS). La *Figura 3* muestra los diferentes tipos de amenazas clásicas.

Figura 3. *Diferentes tipos de amenazas clásicas.*



Fuente: Tomada de Alghamdi, B., Watson, J., & Xu, Y. (2010, p. 7)

El *software* malintencionado o el *malware*, está diseñado para acceder a un contenido de usuarios privados a los que a menudo es relativamente fácil acceder debido a la naturaleza de la comunicación entre usuarios. Los tipos más comunes de *malware* son *adware*, *bots*, *bugs*, *ransomware*, *rootkits*, troyanos, *spyware*, virus y gusanos. Las formas más perjudiciales de *malware* son aquellas que acceden a las credenciales de un usuario y pretenden ser legítimas para los usuarios. Un ejemplo de *malware* de redes sociales en línea es *Koobface*, que se propaga a través de redes sociales como *Facebook*, *Twitter* y *Myspace*. Se utilizó para recopilar credenciales de inicio de sesión y hacer que la computadora infectada fuera parte de una *botnet* (Baltazar, Costoya & Flores, 2009). Cometer fraude y propagar *malware* son acciones delictivas en las que los usuarios están comprometidos para acceder a una URL y ejecutar un código malicioso en la computadora de un usuario de OSN (Alghamdi, Watson & Xu, 2016).

Las amenazas de *phishing* son otro tipo de ciberataque en que el intruso envía un enlace malicioso o un archivo adjunto por correo electrónico para obtener información personal, como información de inicio de sesión, información de tarjeta de crédito e información bancaria en línea. En un ataque de *phishing*, los atacantes suelen utilizar la ingeniería social y otros recursos de información pública, incluidas las redes sociales como *LinkedIn*, *Facebook* y *Twitter*, para recopilar información básica sobre el historial personal y laboral, los intereses y las actividades de la víctima. (Baykara & Ziya, 2018). Por ejemplo, durante un ataque que se atribuyó a los servicios de Inteligencia chinos, se engañó a altos funcionarios militares del Reino Unido y Estados Unidos para que se convirtieran en 'amigos' de *Facebook* con alguien que se hacía pasar por el Almirante James Stavridis de la Armada de los Estados Unidos (Protalinski, 2012). Del mismo modo, los piratas informáticos utilizaron las redes sociales en muchos lugares que se hicieron pasar por otras personas. (Vishwanath, 2017)

La secuencia de comandos entre sitios (XSS) se considera una de las formas más comunes de ataque a aplicaciones basadas en web. Los atacantes usan código malicioso y lo insertan en aplicaciones web para que se ejecuten en el navegador de un usuario. Las XSS puede afectar a una víctima robando *cookies*, modificando una página web, capturando

> "Como resultado de este rápido crecimiento en el uso de redes sociales, han aumentado las amenazas como malware, virus informáticos, software espía entre otras, dirigidas a la confidencialidad y la seguridad de los datos".

contenido del portapapeles, registro de claves, escaneo de puertos y descargas dinámicas (Raman, 2018). Además, un atacante puede utilizar XSS con una infraestructura de red social y desarrollar un gusano XSS que se pueda propagar de forma viral en las redes sociales en línea (Faghani & Nguyen, 2012). Los ataques XSS se pueden clasificar en tres partes: la primera es 'almacenamiento / persistente' en la que se guarda un código de *script* malicioso en el servidor y se ejecuta cuando el usuario visita la página web; el segundo es "reflejado / no persistente" en el que una víctima potencial proporciona información a la página web después de lo cual se ejecutan los ataques, luego los *scripts* maliciosos se guardan con enlaces y se difunden por Internet a través de correo electrónico o sitios de redes sociales; el último, 'modelo de objeto local / documento', es un *script* del lado del cliente en el que los atacantes pueden acceder a información confidencial desde la computadora de la víctima.

Los ataques de denegación de servicios distribuidos (DDoS) implican intentar comprometer los recursos de un sistema interrumpiendo el ancho de banda de la red, haciendo que dichos recursos no estén disponibles para los usuarios. Los ataques se inician desde varios puntos, como computadoras, enrutadores, dispositivos de IoT y otros puntos finales que están infectados por *software* malintencionado controlado por el atacante. Los tipos de DDoS más comunes son TCP (synchronize flood attack o sincronizar ataque de inundación), ataque de *ping* de la muerte, ataque de lágrima, desbordamiento de búfer y SMURF. Dado que los DDoS se propagan normalmente en las redes sociales, los usuarios no tienen idea de que han infectado su sistema y han propagado el *software* malicioso a otras computadoras. Los usuarios siempre serán vulnerables a la propagación de *software* malintencionado (Joshi, Tiper & Zargar, 2013). En 2000, *Yahoo*, *eBay* y *Amazon* fueron atacados por DDoS que desactivaron temporalmente sus sitios web. En 2002, los servidores del New York Times fueron pirateados, lo que le costó al

Foto: https://www.laverdad.es/tecnologia/internet/piratas-informaticos-nueva-20180713171640-ntrc.html

periódico USD $300,000 para rectificar. En octubre de 2010, se llevó a cabo un ataque a *MasterCard*, *PayPal*, *Visa* y *Post Finance*. Se lanzó otro ataque en apoyo de WikiLeaks y duró más de 16 horas. En noviembre se lanzó un ataque de la magnitud de 10 Gbps en WikiLeaks para evitar la liberación de cables secretos (Anstee, Escobar, Chui & Sockrider, 2015). Algunos de los ataques más grandes se reportaron en 2016, 2015 y 2014, donde 600, 500 y 400 Gbps respectivamente, por Redes ARBOR (Arora, Kumar & Sachdeva, 2011).

Los ataques de inyección SQL permiten a los atacantes tener sin restricciones acceso a aplicaciones de bases de datos que contienen información confidencial. Los ataques de inyección de SQL tienen varios objetivos, como extraer datos, ejecutar comandos remotos, modificar datos, realizar denegación de servicio, realizar huellas dactilares en la base de datos, evadir la detección, omitir la autenticación, determinar el esquema de la base de datos e identificar el parámetro inyectable. Además, los atacantes utilizan varios métodos según el objetivo, como inyección SQL ciega, superposición, tautologías, ataque de tiempo, inferencia, procedimiento almacenado y consultas de unión. Las aplicaciones web con una base de datos que almacena información importante son uno de los principales objetivos de SQLIA, ya que los atacantes pueden acceder fácilmente a las bases de datos que inyectan consultas SQL que son recuperadas por las aplicaciones web. Como la información del usuario se guarda con frecuencia en estas bases de datos (Zainab & Younis, 2016).

La inyección de SQL está registrada como una de las 10 principales vulnerabilidades de las aplicaciones web entre 2007 y 2019, según lo certificado por Open Web Application Security Project (Thiyah, Ali & Abdulqader, 2019). Algunos de los últimos ataques de inyección de SQL se perpetraron contra el complemento de la galería NestGEN y la empresa con sede en California Airsoft GI. En 2017, NextGEN fue atacado usando SQLI para acceder a su base de datos que almacena detalles muy confidenciales del usuario; Los investigadores dijeron que los atacantes utilizaron dos métodos para robar datos de los usuarios (Vatu, 2017). En el foro de Airsoft GI fue atacado

y los piratas informáticos robaron información sobre 65.000 cuentas que incluían datos personales de usuarios registrados. Los piratas informáticos también habían robado información relacionada con 40.000 cuentas de *Gmail*, 2.500 cuentas de *Outlook*, 3.000 cuentas de *Yahoo*, 2.500 cuentas de *Hotmail* (Amir, 2017).

Amenazas modernas

De manera típica, estas amenazas están asociadas con las redes sociales en línea. Su objetivo es adquirir la información personal de los usuarios además de la de sus contactos. En los sitios de redes sociales como *Facebook*, los intrusos se dirigen a la configuración de privacidad de un usuario. De esta manera, si la información personal se hace pública, un atacante puede ver fácilmente esta información; de lo contrario, un atacante puede enviar una solicitud de amistad a usuarios específicos que tengan una configuración personalizada. Después de eso, y tras la aceptación de una solicitud de amistad del usuario objetivo, se revela su información personal. Las amenazas modernas son la vigilancia, la creación de perfiles de usuario, los ataques de inferencia, el acoso cibernético, el secuestro de *clics*, la fuga de privacidad de la ubicación, los ataques de clonación de identidad, la fuga de privacidad de la información, los perfiles falsos y los ataques de anonimización, tal como se evidencia en la *Tabla 1* se clasifican los componentes actuales y la información que probablemente sea el objetivo de ataque.

La vigilancia de los sitios de redes sociales es un nuevo tipo de monitoreo que se utiliza para rastrear y obtener información del usuario, ya sea para individuos, grupos, organizaciones o empresas. La vigilancia de las redes sociales es una vigilancia basada en tecnología en la que las actividades humanas se controlan en las redes sociales (Brown, 2015). Por ejemplo, *Facebook* permitió a la empresa Cambridge Analytics acceder a millones de perfiles sin el consentimiento informado de los usuarios para utilizar la información recopilada para campañas políticas. Se afirma que la compañía ha analizado publicaciones en redes sociales que pertenecen a millones de usuarios para crear sus perfiles psicológicos que luego se utilizaron para mensajes dirigidos a fin de tener un efecto en los patrones de votación en las elecciones de los Estados Unidos (BBC, 2018). El monitoreo más deliberado de los individuos a menudo tiene lugar en un contexto de confrontación, utilizando cada vez más medios técnicos para recopilar y analizar datos, y

Tabla 1. *Información y subprocesos en los que están los objetivos de ataque especializados modernos*

Vigilancia	Social, ambiental, eCommerce, y política de gobierno
Perfil de usuario	Actividades y características ambientales
Ataque de inferencia	Predicción sensible, religión, política e información de educación.
Cyberstalking	Acoso e intimidación
Clickjacking	Presione el enlace o el botón Me gusta, el cursor en movimiento, el micrófono y la cámara
Locación de privacidad	Geo-etiquetado
Clonación de perfiles	Crear un perfil falso
Fuga de información	Salud, infraestructura operacional y propiedad intelectual
Ataques de perfiles falsos	Información de usuario
Anonimización	Servicios de salud, redes sociales, eCommerce

Fuente: Elaboración propia a partir de los datos registrados en universo editorial consultado

se utiliza para la gobernanza social, ambiental, económica o política. (Brown, 2015)

La elaboración de perfiles de usuario implicó el registro y análisis de unas actividades del usuario con relación a las características psicológicas y de comportamiento mediante el uso de varios métodos, como redes neuronales, algoritmos genéticos y reglas de asociación. Los perfiles de usuario contienen diversos contenidos, como intereses, habilidades, conocimientos, objetivos y comportamientos de los usuarios. La elaboración de perfiles de usuarios mediante la inferencia de la edad, el género y los rasgos de personalidad de los usuarios juega un papel importante en la prestación de servicios personalizados, *marketing* viral, sistemas de recomendación y anuncios personalizados (Nowson & Oberlander, 2006). Los proveedores de servicios en línea realizan perfiles de usuarios con fines comerciales; sin embargo, puede abrir el camino a la filtración de privacidad (Ali, Rauf, Islam, Farman & Khan, 2017).

El ataque de inferencia se utiliza para predecir la información personal de los usuarios. En este tipo de ataque, los atacantes acceden ilegalmente a la información del usuario mediante el uso de diferentes técnicas de minería de datos para predecir información útil. Es posible que los usuarios de las redes sociales en línea no deseen

> "El acoso cibernético se entiende como el evento de acechar electrónicamente a una persona, es un delito en el que los atacantes acosan o amenazan a otros usuarios a través de sitios de redes sociales, mensajería instantánea, correo electrónico o cualquier otro".

Foto: https://www.kaspersky.es/resource-center/threats/ddos-attacks

> "Los piratas informáticos descargan programas maliciosos o cualquier otra amenaza en el sitio de redes sociales, el correo electrónico y otros, que monitorean y penetran la información de los usuarios"

revelar su información personal y sensible, como religión, afiliaciones políticas, domicilio, educación, preferencias, edad y género. Específicamente, el atacante podría ubicarse en cualquier parte (por ejemplo, un ciberdelincuente, un proveedor de redes sociales en línea, un anunciante, un intermediario de datos y una agencia de vigilancia) que tenga interés en los atributos privados de los usuarios.

Para realizar tales ataques a la privacidad, el atacante solo necesita recopilar datos disponibles públicamente de las redes sociales que estén en línea (Gong & Liu, 2018). La información en las redes sociales que se detecte debe tener privacidad. Sin embargo, el atacante puede utilizar técnicas de minería de datos para predecir la información privada. Se puede emplear un ataque basado en amigos mutuos para encontrar el vecino común de dos usuarios cualquiera (Heatherly, Kantarcioglu & Thuraisingham, 2013). Se utiliza una técnica de análisis de componentes principales (PCA) para predecir los atributos de un usuario en función de sus otros atributos públicos que estaban disponibles en línea (Viswanath, Bashir, Crovella, Guha, Gummadi, Krishnamurthy & Mislove, 2014). *Facebook* se utilizó para probar las técnicas de PCA a fin de deducir diferentes atributos del usuario, como la ubicación y los antecedentes educativos.

El acoso cibernético se entiende como el evento de acechar electrónicamente a una persona, es un delito en el que los atacantes acosan o amenazan a otros usuarios a través de sitios de redes sociales, mensajería instantánea, correo electrónico o cualquier otro. Este comportamiento implica acoso e intimidación y puede incluir hacer un seguimiento o monitorear a la víctima personalmente. Los tipos comunes de ciber acoso son: el acosador cibernético compuesto, los acosadores cibernéticos colectivos, el acosador cibernético íntimo y los acosadores cibernéticos vengativos. Los atacantes del ciber acoso confían en el anonimato para hacer un seguimiento de su víctima sin que se lo revelen a ellos

Foto: https://www.bloglenovo.es/actualiza-tus-aplicaciones-si-no-quieres-ddos/

ni a otros (Winkelman, Early, Walker, Chu & Yick-Flanagan, 2015).

Clickjacking también conocido como ataque de reparación de la interfaz de usuario, es un ataque que engaña al usuario para que haga *clic* en un elemento oculto, como un botón o un enlace, en el que no tuvo la intención de hacerlo. Esto puede lograr que los usuarios visiten una página web maliciosa o descarguen *malware*. Por ejemplo, los atacantes pueden engañar a los usuarios de las redes sociales en línea para que hagan clic en un botón "Me gusta" en un *Facebook* a enlaces sin saberlo. Algunas variaciones de ataque de *clickjacking* son *likejacking*, *cursorjacking*, *drag-and-drop*, *strokjacking* y otros. Los atacantes pueden incluso utilizar el *hardware* de las computadoras de los usuarios, por ejemplo, un micrófono y una cámara, para registrar sus actividades (Lundeen, Ou & Rhodes, 2011). En 2016, según el Informe de estadísticas de vulnerabilidad de Edgescan, (61%) de las vulnerabilidades de aplicaciones web conducen a ataques al navegador y en 2017, (27%) de todas las vulnerabilidades estaban asociadas con aplicaciones web y (73%) eran vulnerabilidades de red (BBC, 2016).

La filtración de la privacidad de la ubicación es otro tipo de amenaza a la privacidad. Debido a la popularidad en el uso de dispositivos de teléfonos inteligentes y gracias a que es fácil de usar, anima a los usuarios de las redes sociales en línea a compartir su ubicación en estas redes. Por lo tanto, el riesgo de infracción de la privacidad del usuario aumenta para detectar la ubicación de los usuarios de redes sociales en línea por parte de otros o atacantes. Además, los usuarios de las redes sociales en línea comparten su ubicación sin saberlo subiendo imágenes y videos, y esto lleva a conocer sus ubicaciones geográficas. Murphy (2010) documento que incrustado en la imagen había una etiqueta geográfica, un dato que proporciona la longitud y latitud del lugar donde se tomó la foto. Por lo tanto, reveló exactamente dónde vivía. Un estudio titulado ¿How much is too much?, presentado en la Conferencia de Comunicación Internacional en 2010 encontró que (12,1%) de los *tweets* de *Twitter* examinados (n = 253) mencionaban la ubicación de una persona. Además, Mao, Shuai, Kapadia (2011) utilizaron una técnica de clasificación para identificar la ubicación del usuario en tiempo real.

La clonación del perfil de identidad es una técnica en la que los atacantes crean un perfil falso utilizando imágenes, videos y otra información privada robada del perfil real de un usuario objetivo. Los atacantes pueden duplicar el perfil de un usuario que se parece mucho al perfil del objetivo. Especialmente si la mayor parte del perfil de usuario se establece como público. La clonación de perfiles se puede realizar de dos formas, en el sitio cruzado y en la clonación del mismo sitio. En la clonación entre sitios, la información privada del usuario se roba de los diferentes sitios de redes sociales en línea. Pero, en la clonación del mismo sitio, el usuario privado ubica la información y se toma del mismo sitio de redes sociales en línea. Además, la clonación de perfiles se puede realizar de forma automática y manual. Requiere automáticamente un código de secuencia de comandos escrito y tener la autorización para ejecutar el código de secuencia de comandos en redes sociales en línea como *LinkedIn* y *Facebook* (Bolton & Hand, 2002). En el método manual, el atacante copia toda la información privada del usuario y crea un nuevo perfil.

La filtración de la privacidad de la información sensible es cuando se filtra información privada

> "El crecimiento en el uso de sitios de redes sociales en la 'La estructura WEB 2.0' da como resultado un aumento de los riesgos de seguridad de los datos que dificulta el progreso y el crecimiento tecnológico en la dirección deseada".

Foto: https://www.bbc.com/mundo/noticias-43472797

a usuarios no autorizados. En las redes sociales en línea, los usuarios siempre comparten e intercambian su información con amigos y otros usuarios de estas. La infiltración de información a través de las redes sociales en línea se clasifica en cuatro formas: información de infraestructura como decisiones técnicas, datos de clientes como información de salud, datos operativos como adquisiciones y propiedad intelectual como documentos. Un estudio presentado en *Conference on Safety, Security, Privacy and Interoperability of Health Information Technology* por *Torabi* y *Beznosov* (2013) demostró que 95,8% (n = 166) de los participantes de las redes sociales en línea compartieron alguna información relacionada con la salud. La filtración de información tan sensible y privada puede tener consecuencias negativas para los usuarios de las redes sociales en línea. Por ejemplo, las compañías de seguros utilizan los datos de las redes sociales en línea para distinguir a los clientes riesgosos de los demás (Scism & Maremont, 2010). La filtración de información personal puede dañar la reputación de las organizaciones, por lo tanto, los futuros clientes estarán preocupados por tener negocios con estas empresas o revelar información privada de la empresa. Existen razones importantes para la fuga de información, como las estafas de *phishing*, el uso de herramientas no seguras, el robo de información y el envío de información a usuarios incorrectos.

Por su parte, el ataque de anonimización es una técnica de minería de datos en cuyos datos no identificados se cotejan con otras fuentes públicas para volver a identificar la fuente de datos anónimos con el fin de identificar a una persona

o grupo. La anonimización cubre toda la información de identificación personal de los usuarios que operan en diferentes áreas, como comercio electrónico, servicios de salud, redes sociales y otros. Debido a que los datos compartidos a través de las redes sociales en línea están configurados como públicos de forma predeterminada, son un objetivo fácil para los ataques de anonimización (Ding, Zhang, Wan & Gu, 2010) para volver a identificar a una persona a partir de dichos datos. Por ejemplo, en *An Efficient and Robust Social Network De-anonymization Attack* presentado por Gulyás, Simon y Imre (2016) diseñaron y evaluaron un Bumblebee que es un novedoso ataque de anonimización social y los resultados demostraron tasas de reidentificación con alta precisión, robustez frente al ruido y también un mejor control de errores, sumado a lo anterior Lee, Liu & Ji (2017) proponen un nuevo ataque de anonimización basado en estructuras que no requiere que el atacante tenga información previa. La técnica de ataque propuesta se basa en información de vecindad de varios saltos y optimiza el proceso de anonimización mediante la explotación de técnicas mejoradas de aprendizaje automático. Los resultados demostraron importantes ventajas que mejoran hasta 10 veces la precisión de la desanonimización y superan a los ataques de desanonimización de última generación.

Asegurar sitios de redes sociales en línea

En los últimos tiempos, la propagación de la piratería en los sitios de redes sociales ha aumentado significativamente con el aumento del número de sitios y usuarios de redes sociales. La *Tabla 2* muestra las diez peores contraseñas de 2015 a 2020. Según SplashData (2020), estas contraseñas se utilizan principalmente en América del Norte y Europa Occidental y después de evaluar más de cinco millones de contraseñas filtradas en Internet, la firma descubrió que los usuarios de computadoras continúan usando las mismas contraseñas predecibles y fáciles de adivinar.

Tabla 2. *Las 10 contraseñas más comunes*

2015	2016	2017	2018	2019	2020
123456	123456	123456	123456	123123	123456
clave	clave	clave	clave	111111	123456789
12345678	12345	12345678	123456789	iloveyou	picture1
QWERTY	12345678	QWERTY	12345678	12345	password
12345	football	12345	12345	12345678	12345678
123456789	QWERTY	123456789	111111	1234567	111111
football	1234567890	letmein	1234567	password	123123
1234	1234567	1234567	sunshine	qwerty	12345
1234567	princes	football	QWERTY	123456789	1234567890
baseball	baseball	1234	iloveyou	123456	senha

Fuente: Elaboración propia a partir de los datos registrados en Splashdata (2020)

Al estudiar las contraseñas que se muestran en la *Tabla 2*, es posible deducir la similitud entre los usuarios de redes sociales en la selección de contraseñas que conducen a facilitar la tarea de los atacantes. Los intrusos suelen utilizar estos datos con énfasis en una alta tasa de éxito y penetración. La similitud de estas contraseñas conduce a los siguientes hechos:

- Los usuarios eligen una contraseña simple que sea fácil de guardar y recuperar.
- Los usuarios seleccionan solo una contraseña para todos los sitios de redes sin volver a cambiarla y esto facilita el proceso de penetración.
- Los usuarios utilizan con frecuencia los componentes de contraseña asociados entre sí para que se puedan recuperar fácilmente.
- Tratar con sitios de redes sociales no requiere el uso de contraseñas complejas. Por lo tanto, los usuarios eligen las contraseñas más simples. Además, los sitios de redes no requieren un cambio continuo de contraseñas.
- Los usuarios generalmente eligen la contraseña de información privada que se puede recordar fácilmente. Por lo tanto, cualquier persona familiarizada con los datos puede piratearlo.

Los piratas informáticos descargan programas maliciosos o cualquier otra amenaza en el sitio de redes sociales, el correo electrónico y otros, que monitorean y penetran la información de los usuarios. Además, los piratas se comunican con los usuarios y proponen proporcionar algunos servicios especiales, como iniciar sesión en el sitio web y pedir a los usuarios que ingresen su contraseña. Por lo tanto, los usuarios deben evitar ingresar la contraseña cuando trabajen con aplicaciones de servicio o sitios web que no sean de confianza.

Las amenazas más importantes para penetrar en los sitios de redes sociales son el método de preparación y uso de diferentes contraseñas. Así, una serie de recomendaciones que inciden positivamente en estos riesgos se pueden mencionar y resumir de la siguiente manera:

- No usar una contraseña simple porque es fácil de penetrar.
- No repetir el uso de la contraseña para diferentes sitios porque penetrar en un sitio puede provocar la penetración en todos los sitios.
- Utilice una contraseña compleja que no sea fácil de penetrar.
- Utilice programas de gestión de contraseñas como ZOHO, Keeper y Dashlane para almacenar y administrar contraseñas.

Foto: https://www.elsaber21.com/los-peligros-de-los-piratas-informaticos-en-la-actualidad-y-en-el-futuro

Prevención de riesgos y amenazas vulnerabilidades

El riesgo se define como la posibilidad de dañar, filtrar o destruir la información o los dispositivos de los usuarios como resultado de una amenaza que explota una vulnerabilidad. La vulnerabilidad es una debilidad en la protección de la información del usuario que puede ser aprovechada por una o más amenazas (NIST - National Institute of Standards and Technology 2013). La *Tabla 3* muestra los riesgos, amenazas y vulnerabilidades de seguridad de la información. Por ejemplo, en el sistema de redes sociales cuando los usuarios tienen contraseñas débiles o no tienen un sistema seguro. En este caso, la contraseña de un usuario es vulnerable a un atacante o el sistema seguro puede ser fácilmente penetrado.

Tabla 3. *Riesgos, amenazas y vulnerabilidades*

Riesgos	Amenazas	Vulnerabilidades
Pérdida de privacidad	Hackers (Piratas)	Procesos vulnerados
Pérdida de confidencialidad	Terroristas	Bugs en software
Pérdidas financieras	Empleados no éticos	Inefectividad en controles
Pérdidas de vida	Criminales	Defectos en hardware
Disrupción de negocios	Competidores	Sistemas legados
Daño de reputación	Empleados enojados o insatisfechos	Errores humanos
Penalidades legales	Gobiernos	Cambios en los negocios
Crecimiento desigual	Prensa	Inadecuada planeación en la continuidad de negocio

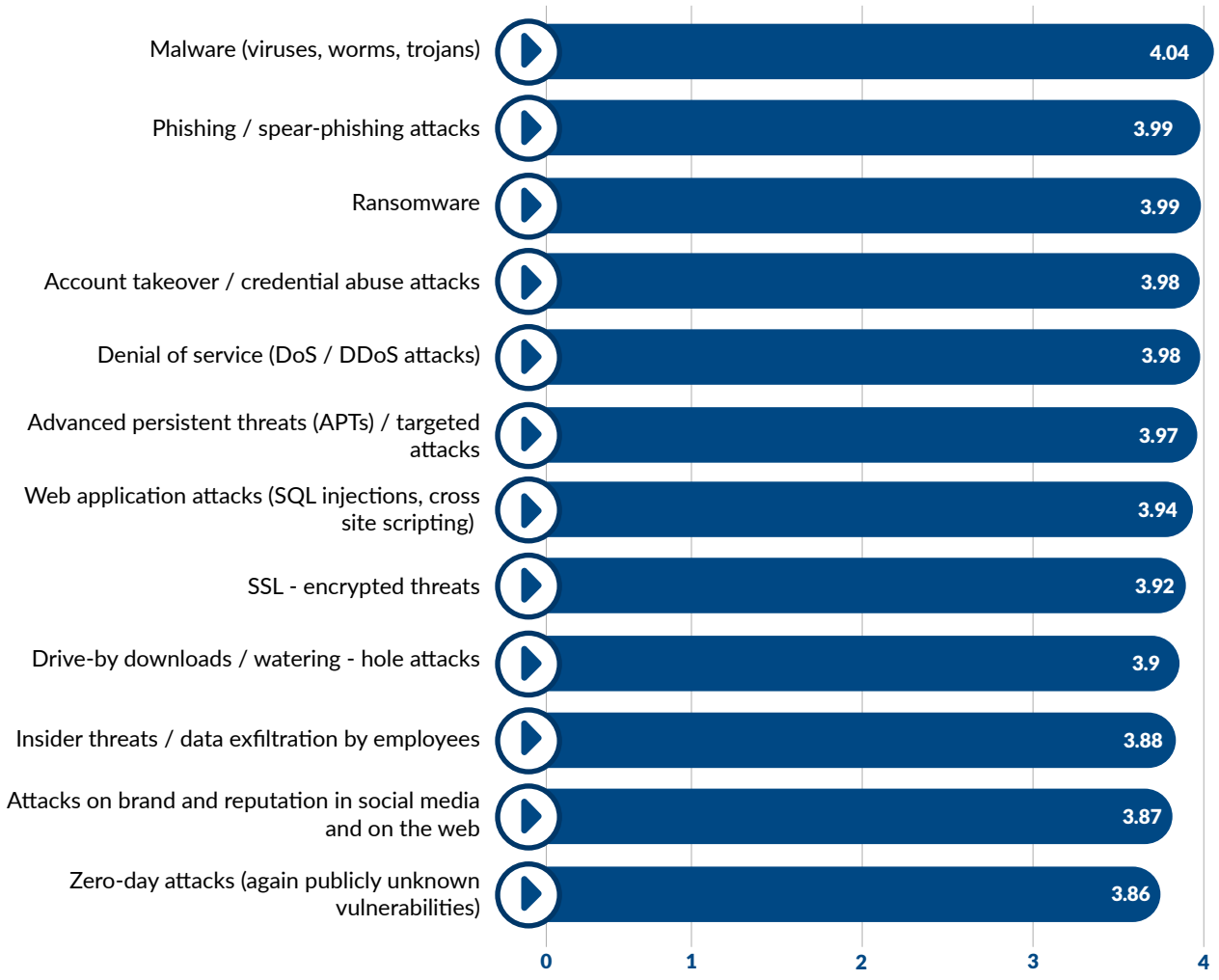
Fuente: Elaboración propia a partir de los datos registrados en universo editorial consultado

A medida que las amenazas se propagan en los sitios de redes sociales de todo el mundo con diferentes actividades, y debido a la gran disminución en el nivel de privacidad de la información del usuario, los siguientes pasos son necesarios para las anti-amenazas que enfrentan los usuarios en los sitios de redes sociales.

- Determine el nivel de privacidad requerido del sitio a la luz del nivel de uso y el grado de interacción del usuario en las redes sociales.
- Aprovechar las ventajas de todas las actualizaciones en el sitio, que se desarrollan continuamente para elevar el nivel de seguridad de los datos.
- Seleccione y revise cuidadosamente a los usuarios antes de aceptarlos o tratar con ellos.
- Las funciones utilizadas para el sitio deben detenerse periódicamente y ejecutarse nuevamente una tras otra.
- Antes de actualizar los sitios de redes sociales y otro software, lea atentamente todas las funciones nuevas.

El crecimiento en el uso de sitios de redes sociales en "La estructura WEB 2.0" da como resultado un aumento de los riesgos de seguridad de los datos que dificulta el progreso y el crecimiento tecnológico en la dirección deseada. La *Figura 4* resume las principales amenazas a nivel mundial en 2020, según los responsables de la toma de decisiones de seguridad de TI en todo el mundo. (Statista, 2020)

Figura 4. *Ciberamenazas más preocupantes.*



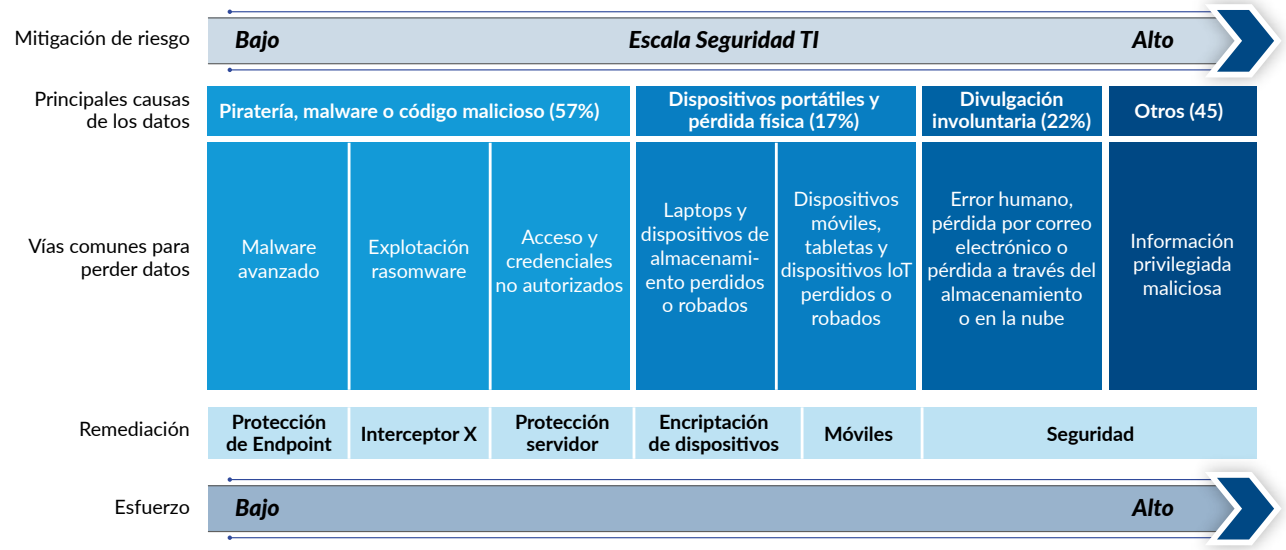
Fuente: Tomada de Statista (2020)

Varios estudios han señalado que existe una gran importancia para el impacto de las amenazas, especialmente a nivel de las instituciones que se ocupan de los sitios de redes sociales y dependen en gran medida de estos sitios para tratar con clientes, proveedores y empleados en muchas actividades vitales relacionadas con la operación, economía y producción. (Hunt 2012; IT Trends 2019; Polvereda 2017)

De acuerdo con el estudio de SOPHOS (2018) para gestionar el riesgo de los datos y los activos de TI, la figura 9 demuestra la cantidad de esfuerzos necesarios para lograr la mitigación de riesgo más baja para proteger los datos.

Las sugerencias esenciales anteriores tienen un impacto positivo significativo en los usuarios de las redes sociales en línea para hacer frente a las innovaciones interactivas de las aplicaciones de redes en línea y permitir mantener la seguridad y la confidencialidad de los datos

Figura 5. *Protección de los datos.*



Fuente: Tomada de SOPHOS (2018)

Foto: https://cadenapolitica.com/2021/02/08/la-proteccion-de-datos-personales-debe-tener-un-alcance-general-y-no-solo-a-algunas-plataformas/

a nivel institucional así como a nivel individual.

Como parte de los esfuerzos para abordar estos riesgos, se pueden habilitar una serie de sugerencias esenciales en el sistema de redes sociales y que respaldan el uso de la tecnología "Web 2.0", que funciona para proteger los datos y superar diversas amenazas.

- Control por parte de las empresas a las aplicaciones que se utilizan en Internet para limitar los programas maliciosos que no emplean los protocolos estándar.
- Revisión continua de los sitios utilizados, identificación de periodos de uso y desarrollo de diferentes mecanismos para corregir los negativos. La información recopilada y revisada en el uso real tiene un gran valor para identificar los riesgos y resolver cualquier problema.
- Determinación de los navegadores utilizados y determinación de sus técnicas para proteger los datos mediante el uso de propiedades avanzadas.
- Empleo del software antiamenazas para combatir programas maliciosos, spyware y otras amenazas con un estado de actualización continua para permitir que este software haga frente al rápido desarrollo de las amenazas.
- Utilización de una contraseña sofisticada que sea difícil de penetrar y actualización constante de estas contraseñas en todas las aplicaciones en línea, para garantizar la preservación de los datos y evitar la piratería.

Foto: https://cip-formacion.com/cursos-de-formacion/formacion-subvencionada/cursos-formacion-subvencionada-plan-estatal/gestion-de-recursos-web-2-0/

- Verificación de las políticas de piratería y conocimiento de los mensajes y enlaces desconocidos enviados por usuarios no conocidos.
- Empleo de diferentes mecanismos para proteger los datos y restaurarlos en caso de que se contaminen o se pierdan como resultado de una piratería.

Conclusiones

A principios del siglo XXI, el crecimiento y el desarrollo de las aplicaciones de Internet y las redes sociales aumentan significativamente. Por lo tanto, se incrementa la interacción entre los usuarios en las redes sociales mediante el uso de diferentes aplicaciones en línea. Con este crecimiento, se han desarrollado una serie de amenazas para penetrar la protección de datos del usuario y la confidencialidad. Esta infiltración se considera como la mayoría de los problemas al utilizar las redes sociales en línea. La penetración de datos podría provenir de usuarios no autorizados, proveedores de servicios y otros que utilizan datos de redes sociales en línea para sus negocios. Este documento explica varios problemas de protección y privacidad relacionados con los usuarios de redes sociales en línea y los datos de amenazas en línea como piratas informáticos y proveedores de servicios. Además, demuestra los esfuerzos necesarios para abordar y gestionar los riesgos en las redes sociales.

REFERENCIAS

Alghamdi, B., Watson, J., Xu, Y. (2010). "Toward detecting malicious links in online social networks through user behavior". In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence Workshops, Omaha, NE, USA, 13-16 pp. 5-8.

Ali, S., Rauf, A., Islam, N., Farman, H. & Khan, S. (2017). User Profiling: "A Privacy Issue in Online Public Network.", Sindh Univ. Res. J. (Sci. Seri.) 49, 125–128.

Amir, W. (2017). Gun retailer Airsoft GI's Forum hacked; 65,000 user accounts leaked https://www.hackread.com/gun-retailer-airsoft-gi-forums- hacked/

Anstee, D., Escobar, J., Chui, C.F. & Sockrider, G. (2015), Jan 27. 10th Annual Worldwide Infrastructure Security Report. Arbor Networks Inc.

Arora, K., Kumar, K., & Sachdeva, M. (2011). Impact analysis of recent DDoS attacks. International Journal on Computer Science and Engineering, 3(2), 877-883.

BBC Mundo. Disponible en https://www.bbc.com/mundo/noticias-43472797

BCC Risk Advisory Ltd. (2016). Vulnerability Statistics© 2015-19, IJARCS All Rights Reserved 8 Report Edgescan, 2016. http://www.edgescan.com.

Baltazar, J., Costoya, J. & Flores, R. (2009). "The Real Face of Koobface": The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research

Baykara, M. & Ziya, Z.G. (2018). "Detection of phishing attacks", IEEE, 978-1-5386-3449-3/18.

Bolton, R.J. and Hand, D.J. (2002). Statistical Fraud Detection: A Review. Statistical Science. 17, 3, 235–249.

Brown, I. (2015). "Social Media Surveillance". The International Encyclopedia of Digital Communication and Society, First Edition". John Wiley & Sons, Inc. Published by John Wiley & Sons, Inc., DOI: 10.1002/9781118290743.wbiedcs122.

Davison, H.K., Maraist, C.C., Hamilton, R. & Bing, M.N. (2012). ¿To Screen or Not to Screen? Using the Internet for Selection Decisions. Empl. Responsib. Rights J., 24, 1–21.

Ding, X., Zhang, L., Wan, Z. & Gu, M. (2010). "A brief survey on de-anonymization attacks in online social networks". In Proceedings of the IEEE International Conference on Computational Aspects of Social Networks (CASoN 2010), Taiyuan, China, 26–28; pp. 611– 615.

Experience Group. https://www.experience-group.com/wp-content/uploads/2018/10/Cybersecurity-Presentation-October-2018.pdf.

Faghani, M.R. & Nguyen, U.T. (2013). "A study of XSS worm propagation and detection mechanisms in online social networks". IEEE Trans. Inf. Forensics Secur. 8, 1815–1826.

Gong, N.Z. & Liu, B. (2018). "Attribute Inference Attacks in Online Social Networks", ACM Transactions on Privacy and Security, Vol. 21, No. 1, Article 3. Publication date: January

Gulyás, G.G., Simon, B., Imre, S. (2016). An Efficient and Robust Social Network De-anonymization Attack. In Proceedings of the Workshop on Privacy in the Electronic Society, Vienna, Austria, 24 October; pp. 1–11.

Hak J. Kim."Online Social Media Networking and Assessing Its Security Risks: International Journal of Security and Its Applications, Vol. 6, No. 3, July, 2012.

https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Hathi, S. (2009). "Cómo aumentan las Redes Sociales. Colaboración en IBM", Gestión de la comunicación estratégica, vol. 14, no. 1, pp. 32-35.

Heatherly, R., Kantarcioglu, M., Thuraisingham, B. (2013). "Preventing private information inference attacks on social networks." IEEE Trans. Knowl. Data Eng. 25, 1849–1862.

Humphreys, L., Gill, P. & B. Krishnamurthy. (2010). "How much is too much? Privacy issues on Twitters". In Conference of International Communication, Pages 1-29. ACM Press

Hunt, E. (2012). "US Government Computer Penetration Programs and the Implications for Cyberwar". IEEE Annals of the History of Computing 34(3):4–21.

IT Trends. (2019). "Crecen Los Ataques Ciberneticos Especialmente Los Destinados A- Ot." IT Trends. Retrieved (https://www.ittrends.es/seguridad/2019/03/crecen-los-ataques-ciberneticos-especialmente-los-destinados-a-iot).

Lundeen, R., Ou, J., Rhodes, T. (2011). "New Ways Im Going to Hack Your Web APP". Black Hat Abu Dhabi. Available Online: https://www.blackhat.com/html/bh-ad 11/bh-ad-11-archives.html#Lundeen.

Mao, H. X., Shuai, Kapadia, A. (2011). "Loose Tweets: An Analysis of Privacy Leaks on Twitter", In proceeding of the 10th annual ACM workshop on privacy in the electronic scoiety, pages 1-12. ACM.

Murphy, K. (2010). "Web Photos That Reveal Secrets, Like Where You Live", The New York Times, https://www.nytimes.com/2010/08/12/technology/persona ltech/12basics.html.

NIST - National Institute of Standards and Technology. (2013). "Security and Privacy Controls for Federal Information Systems and Organizations." NIST Special Publication 800:53.

Nowson, S., Oberlander, J. (2006). "The identity of bloggers: Openness and gender in personal weblogs In Proc. of AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs", pages 163–167.

Polvereda, J. (2017). "Sistema De Monitorización Del Ids Snort"

Protalinski, E. Chinese Spies Used Fake Facebook Profile to Friend Nato Officials. Available online: https://www.zdnet.com/article/chinese-spies-used-fake- facebook-profile-to-friend-nato-officials.

Raman, P. (2008). "aSPIn: JavaScript based anomaly detection of cross-site scripting attacks", Ph.D. thesis, Carleton University, Ottawa.

Rua Mohamed Thiyah, Iyab Musab A. M. Ali, Farooq Basil Abdulqader. (2019). "The impact of SQL injection attacks on the security of databases", Proceedings of the 6th International Conference on Computing and Informatics, ICOCI 2017 25-27 April, Kuala Lumpur. Universiti Utara Malaysia

S. T., Joshi, J., Tipper, D. & Zargar. (2013). "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks". IEEE communications surveys & tutorials.

Scism, L., Maremont, M. (2010). Insurers Test Data Profiles to Identify Risky Clients. The Wall Street Journal, 19 November

Sloane Burke Winkelman, Jody Oomen Early, Ashley D. Walker, Lawrence Chu, Alice Yick-Flanagan". (2015). Exploring Cyber Harrassment among Women Who Use Social Media", Universal Journal of Public Health 3(5): 194-201, DOI: 10.13189/ujph.2015.030504

Social Networks. (2014). "In Proceedings of the USENIX Security Symposium", San Diego, CA, USA, 20–22 August; pp. 223–238.

Splashdata. Disponible en https://www.teamsid.com/splashdatas-top-100-worst- passwords-of-2020/.

Statista. Disponible en https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

_____. https://www.statista.com/statistics/500946/worldwide-leading-it-security-threats/

Torabi, S., Beznosov, K. (2013). Privacy Aspects of Health Related Information Sharing in Online Social Networks. In Proceedings of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, Washington, DC, USA, 12 August 2013; p. 3.

Vatu, G., (2017). Critical SQL Injection Vulnerability Found in NextGEN Gallery WorldPress Plugin http://news.softpedia.com/news/critical-sql-injection- vulnerability-found-in-nextgengallery-wordpress-plugin-513375.shtml.

Viswanath, B., Bashir, M.A., Crovella, M., Guha, S., Gummadi, K.P., Krishnamurthy, B. & Mislove, A., "Towards Detecting Anomalous User Behavior in Online

Vishwanath, A. (2017). "Getting phished on social media". "Decisios Support Systems", ELSEVIER., Vol. 103, November, pp. 70-81.

Wei-Han Lee, Changchang Liu, Shouling Ji (2017). "Blind De- anonymization Attacks using Social Networks", Proceedings of the 2017 on Workshop on privacy in the Electronic Society. Dallas, Texas, USA, October.

Zainab S. Alwan, Manal F. Younis. (2017). "Detection and Prevention of SQL Injection Attack: A Survey", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.8, August, pp. 5-17.

www.securelist.com, «"Instant" threats», Denis Maslennikov, Boris Yampolskiy, 27.05.2008.