SEGURIDAD APLICADA EN LA UTILIZACIÓN DE REDES SOCIALES

Guzmán Sua Carlos Armando
cags84@gmail.com
Universidad Piloto de Colombia

Resumen — En el presente artículo se busca describir y realizar un análisis de todo el entorno que rodea y conforma las llamadas redes sociales las cuales actualmente mantienen un gran auge en lo que respecta a la evoluciones de las comunicaciones, en el desarrollo del artículo se analizan los riesgos y las diferentes vulnerabilidades a las que se exponen todos los usuarios que hacen uso de las mismas, también se revisara el impacto que puede causar el mal uso de las redes sociales y como este mal uso permite que a través de diferentes métodos los ciberdelincuentes se apropien de información confidencial con la cual buscan obtener alguna ganancia y lucro en la mayoría de veces de tipo monetario, al final del artículo se buscara crear un modelo donde se recopile toda una serie de recomendaciones y buenas prácticas que permitan a las empresas crear políticas adecuadas para que sus empleados hagan un buen uso de las redes sociales lo cual redundara en la mitigación de los riesgos inherentes al uso indebido de las mismas y evitar el impacto sobre los activos de las entidades.

Índice de Términos—Redes sociales, riesgos, vulnerabilidades, impacto.

Abstract— This article aims to describe and perform an analysis of the entire environment that surrounds and conform to the so-called social networks, which currently have a great boom in regards to the evolution of communications, in the development of the article will be analyzed the risks and the different vulnerabilities to which are exposed all the users who use of them , also will be reviewed the impact that may cause the misuse of the social networks and how this misuse allows through different methods cyber criminals appropiate of confidential information with which they look for obtain a gain and profit in most cases of monetary type. At the end of the article, will be sought to create a model where a series of recommendations and good practices that allow companies to create adequate policies so that their employees make good use of social networks are collected, this will result in the mitigation of the inherent risks to the improper use of them and avoid the impact on the assets of the entities.

Index Terms—Social networks, Risks, vulnerabilities, impact.

I. INTRODUCCIÓN

El tema de la seguridad informática es algo que en la actualidad tiene una gran relevancia, la exposición al robo de información y datos confidenciales que aúnan en el desarrollo de delitos informáticos, ha hecho que esto se vuelva una realidad.

Pero no solo las personas por ser las más vulnerables están expuestas a este flagelo de robo de información, las grandes empresas invierten mucha parte de sus ganancias para salvaguardar sus activos y poder así combatir este flagelo.

Muchas de las empresas centran sus esfuerzos en prevenir y combatir todos aquellos riesgos que vienen del entorno exterior, pero muchas de ellas descuidan su entorno interior y es allí donde también existe un riesgo muy latente, el cual debe ser considerado y mitigado muchas de las veces estableciendo buenas políticas de seguridad para ser cumplidas por parte de cada uno de sus empleados, ellos y dependiendo también del objetivo de la empresa, pueden llegar a ser un foco importante de riesgos y vulnerabilidades que no deben ser ajenos a los procesos de seguridad de la misma.

Es por esa razón que el presente artículo se focalizara en las llamadas redes sociales y como la importancia que día a día viene creciendo en su uso, hace que las empresas y demás instituciones deban poner foco y establecer un tratamiento adecuado ya sea con medidas de sensibilización hacia las personas, como también con el establecimiento de políticas muy fuertes de cara al uso adecuado en pro de evitar ser víctimas de ataques informáticos provenientes del uso indebido de las mismas.

¿Están preparadas las empresas y demás instituciones para prevenir los ataques provenientes del mal uso de las redes sociales por parte de sus dueños, empleados, socios, estudiantes?, la respuesta a esta pregunta se verá en el desarrollo del presente artículo.

¿Cómo deben por ejemplo controlar las empresas que sus empleados hagan uso adecuado de las redes sociales, sobre todo si cuentan con dispositivos móviles corporativos y acceso ilimitado a internet, siendo estas sus herramientas básicas de trabajo diario?, la respuesta a esta pregunta, se revisara en las recomendaciones y buenas practicas del presente artículo.

¿Cómo deben manejarse al interior de las empresas, instituciones escolares, la creación de políticas claras para el correcto uso del internet y los dispositivos móviles dentro de las mismas y en particular de cara a lo que refiere al uso de las

redes sociales?, también se verá la respuesta a esta pregunta, dentro de las recomendaciones del presente artículo.

El término de redes sociales surge por los años 70, aun cuando no fue precisamente el nombre en esa época, si claramente se daban los inicios de lo que justo tenemos en la actualidad, en el apartado de estado del arte se describirá con más detalle la evolución a través de los años del concepto y manejo de tan importante servicio de cara a la evolución de las comunicaciones.

Actualmente, las redes sociales más visitadas son Facebook, Twitter, Instagram, YouTube, Snapchat y LinkedIn entre muchas otras, la popularidad se mide con base al número de usuarios que se encuentran vinculados a las mismas, siendo en la actualidad Facebook la preferida a nivel mundial, ya que cuenta con más de 2.000 millones de usuarios matriculados.

Los objetivos o nichos más comunes que persiguen las redes sociales se conocen como las llamadas 3C de la web y son la comunicación, la comunidad y la cooperación, términos que se detallaran más adelante durante el desarrollo del presente artículo.

En la actualidad una de las redes sociales con mayor fama de utilización y popularidad es Facebook, que nació con un propósito meramente educativo en la universidad de Harvard y se utilizaba para que los estudiantes se comunicaran y sostuvieran foros acorde al desarrollo de sus estudios.

Se verá a lo largo del desarrollo del artículo cómo ha evolucionado todo lo que concierne a las redes sociales y su utilización en el mundo y en Colombia, que tratamiento se ha dado en lo que refiere a los riesgos inherentes a su uso, que políticas más comunes se establecen en las empresas para controlar su uso y también que hacen y/o que controles han desarrollado los creadores de las redes sociales para mitigar el riesgo y para poder contener los ataques de hackers que buscan aprovechar las vulnerabilidades de las mismas en pro de obtener beneficios monetarios, principalmente a través del robo de información confidencial de los usuarios y a través de la misma el robo de información de las empresas donde laboran estas personas.

A la par del crecimiento de los riesgos por el uso inadecuado de las redes sociales, aumenta también el crecimiento de los hackers, spammers, desarrolladores de virus y ladrones de datos e identidades, que se dedican al rastreo del tráfico de información que circula a través de las redes sociales.

Claramente el problema no es de las redes sociales, las mismas son creadas para brindar servicios a usuarios de internet, el problema se origina es justamente por el uso inadecuado que se le da a las mismas, ese uso es justamente lo que acrecienta los riesgos y vulnerabilidades.

En la figura 1, se ilustra la diversidad de redes sociales que actualmente se encuentran disponibles para ser utilizadas por usuarios.

Fig. 1. Importancia en el uso de redes sociales
Fuente: Imágenes vulnerabilidades redes sociales

Es tanto el esplendor de las redes sociales que durante los últimos años ha crecido de manera significativa el número de usuarios que hacen uso de ellas.

En la figura 2, se podrá observar el crecimiento de uso de redes sociales durante el periodo 2018.

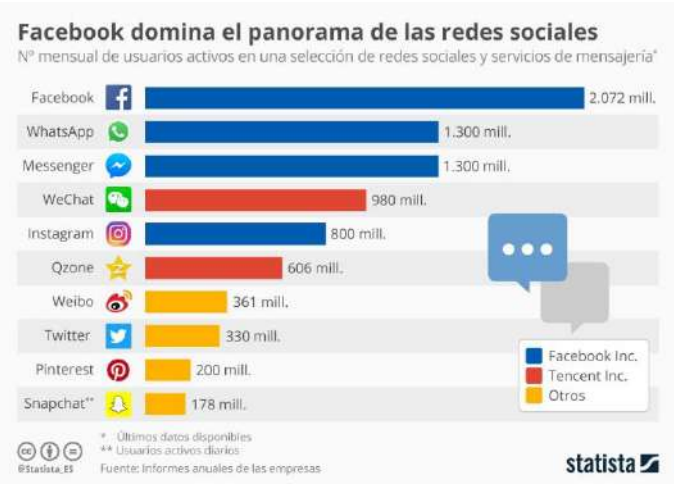

Fig. 2. Estadísticas de usuarios de redes sociales
Fuente: Graficas de internet para uso redes sociales

II. MATERIALES Y MÉTODOS

Las redes sociales son parte de los hábitos cotidianos de las personas, se estima que de casi el total de la población mundial cada persona tiene al menos y/o está vinculado a una red social y justo esta es una de las mayores preocupaciones dada la diversidad de géneros, religiones, culturas, conocimientos técnicos, entre otros, estos aspectos son muy relevantes pues precisamente de ellos se derivan la aparición de nuevas vulnerabilidades, esto es aprovechado por los ciberdelincuentes para poder realizar sus ataques y obtener información valiosa y confidencial de los usuarios.

En el desarrollo del artículo se realizara un levantamiento de información y análisis sobre las diferentes redes sociales que existen, claramente las más importantes de acuerdo a su uso, veremos cómo funcionan, se verán sus protocolos de seguridad, se conocerán sus debilidades, analizaremos los riesgos inherentes a las mismas, se identificarán y clasificarán las diferentes vulnerabilidades y amenazas que en la actualidad atacan de manera permanente a estas redes y con este análisis y clasificación, se armara un modelo con recomendaciones, buenas practicas, políticas, consejos en pro de que se proteja la triada de la información, esto es la integridad, la confidencialidad y la disponibilidad.

En conclusión, con los resultados obtenidos de acuerdo al análisis y estudio realizado, se buscará modelar un sistema que permita garantizar y mitigar los riesgos; Este modelo estará basado en recomendaciones, buenas prácticas y en lo posible herramientas informáticas.

III. ESTADO DEL ARTE

El origen de las redes sociales se remonta a los años 70, una red social se describe como una estructura social compuesta por grupos de personas o individuos, los cuales tienen un objetivo en común.

Este objetivo común varia acorde a la red social, puede ser político, religioso, de amistad, de familia, de conocimiento y muchos otros más.

En la figura 3, se ilustra cómo está conformada una estructura de red social.

Fig. 3. Estructura de red social
Fuente: PubliMarkCreative

El origen de las redes sociales se da con la aplicación de la teoría de grafos, por un lado identificando las entidades como nodos o vértices y que claramente vienen siendo las personas o empresas y por otro lado vienen las relaciones entre ellos, los cuales se identifican como enlaces y aristas.

Aun cuando el furor de las redes sociales es reciente, su origen se remonta a muchos años atrás, la masificación y el uso de la internet y la evolución acelerada de la tecnología es lo que ha permitido una gran prosperidad de las mismas y las ha convertido en un medio de comunicación fácil, rápido y muy práctico, definitivamente la tecnología ha jugado un papel crucial sobre todo en lo que respecta al avance en dispositivos móviles y equipos portátiles y la posibilidad de conectarse a las redes sociales a través de ellos desde cualquier sitio del mundo.

A continuación se mostrara una breve reseña histórica de cómo ha sido la evolución de las redes sociales a lo largo de estos años:

- En 1971, se envió el primer mail.
- En 1978, se realizó el primer intercambio BBS (Bulletin Board System) a través de líneas telefónicas.
- En 1978, se realizaron las primeras copias de navegadores de internet a través de la plataforma Usenet.
- En 1994, se funda GeoCities, una de las primeras redes sociales sobre internet.
- En 1995, Globe.com da posibilidad a sus usuarios que suban y personalicen sus contenidos e interactúen con otras personas.
- En 1997, se da el lanzamiento de AOL Instant Messenger.
- En 1997, se inaugura sixdegrees.com dentro de la cual se permite la creación de perfiles personales y además la lista de amigos.
- En 2002, el portal Friendster, es pionero en conexión online de amigos reales y alcanza un número de 3 millones en tan solo tres meses.
- En 2003, se inaugura la web MySpace.
- En 2004, se lanza nada más y nada menos que Facebook, inicialmente creada para uso estudiantil en Harvard.
- En 2006, se inaugura la red de microblogging Twitter.
- En 2008, Facebook se coloca por encima de MySpace en número de usuarios.
- En 2011, Facebook con 600 millones, MySpace con 200 millones, Twitter con 190 millones y Friendster con 190 millones son las redes sociales mejor posicionadas en cuanto a número de usuarios.
- En 2018, Facebook con 2196 millones, YouTube con 1900 millones, Instagram con 1000 millones, Twitter con 336 millones, LinkedIn con 294 millones y Skype con 300 millones son las redes sociales mejor posicionadas en cuanto a número de usuarios.

En la figura 4, se ilustra estadísticas de usuarios en redes sociales a julio de 2018.

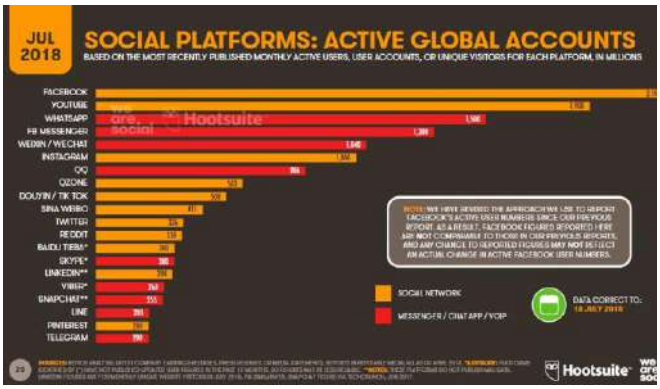

Fig. 4. Estadísticas usuarios por redes sociales en 2018
Fuente: Marketing Digital

Claramente este auge y crecimiento en el uso de redes sociales trae consigo también el crecimiento de un sin número de riesgos, cada persona vinculada a una red social se ve expuesta a un conjunto de amenazas informáticas que atentan contra su información confidencial, su privacidad, su dinero y en muchas ocasiones contra su integridad, es por eso que dados todos estos riesgos es imperativo contar con un entorno seguro al momento de estar utilizando cualquiera de las redes sociales existentes en la actualidad.

A lo largo de este artículo, el enfoque se centra en:

- Principales ataques a redes sociales.
- Mejores prácticas en el uso de redes sociales.
- Como controlar la subida desmedida de contenidos y material por parte de los usuarios.

Son tan grandes los riesgos a los que se ve expuesta la información que se comparte en las redes sociales, que se podría pensar en un futuro muy cercano que la autenticación tanto para el registro como para la conexión a una red social debería darse a través de herramientas y aplicaciones biométricas que claramente son los pilares sobre los cuales se busca garantizar el mecanismo de autenticación y comprobación de identidad.

IV. PORQUE TANTO EL INTERÉS EN LAS REDES SOCIALES

Acorde a lo que se ha venido revisando, se puede resumir que una red social no es más que una estructura social compuesta por individuos con un objetivo en común.

El florecimiento de las redes sociales corresponde al proceso de evolución en las comunicaciones, actualmente las redes sociales ocupan la mayor parte del tiempo en este proceso de evolución, una red social para ser considerada como tal, debe contemplar acorde a Boyd y Ellison las siguientes 3 características:

- La posibilidad de construir un perfil público o semipúblico delimitado dentro de un sistema.
- Poder articular una lista de otros usuarios con los que comparten una conexión.
- Ver y recorrer la propia lista de conexiones y las realizadas por otros dentro del sistema.

Aunque dependiendo de cada autor son muchas las clases de redes sociales que existen, todos convergen en dos tipos comunes que son las redes sociales **verticales** que son aquellas cuyos intereses y motivaciones de los usuarios son diversas y por otra parte están las redes sociales **horizontales** que son aquellas en las cuales los usuarios tienen intereses afines.

Igualmente y como se mencionaba anteriormente, dependiendo de cada autor existen muchas más clases de redes sociales y algunos las clasifican adicional a las anteriores como redes sociales profesionales, de ocio, verticales mixtas, universitarias, de noticias sociales, bloggings, microbloggings, contenido compartido, globales, profesionales, personales y privadas entre otras.

En la actualidad existen muchas redes sociales, pero las de mayor fama son facebook, twitter, YouTube, Instagram, google+, LinkedIn, las redes sociales son herramientas que permiten construir un perfil propio a cada persona, en ellas se muestran imágenes y personalidades propias de las personas, construidas claramente con base a información personal y confidencial.

En una red social se permite crear el llamado perfil, que básicamente está conformado por datos como el nombre, edad, sexo, foto, hobbies, gustos, formación profesional, sitio de trabajo y toda la información adicional que un usuario desee ingresar al momento de registrarse como usuario de la red, una vez ingresada, esta información queda visible para el grupo de amigos y adicional para los contactos del grupo de amigos.

Dado el crecimiento en la utilización de redes sociales, así mismo aumenta la probabilidad de número de ataques sobre las mismas, uno de los mayores riesgos en este entorno es conocido como “Suplantación de Identidad”, alguien utiliza sin permiso y de manera no autorizada los datos personales y credenciales de otro individuo, en pro de conseguir información confidencial y obtener así beneficios monetarios que es lo que busca en su mayoría los piratas informáticos.

En la figura 5, se podrá observar las estadísticas de ataques de spam y phishing a redes sociales solo durante el primer trimestre de 2018.

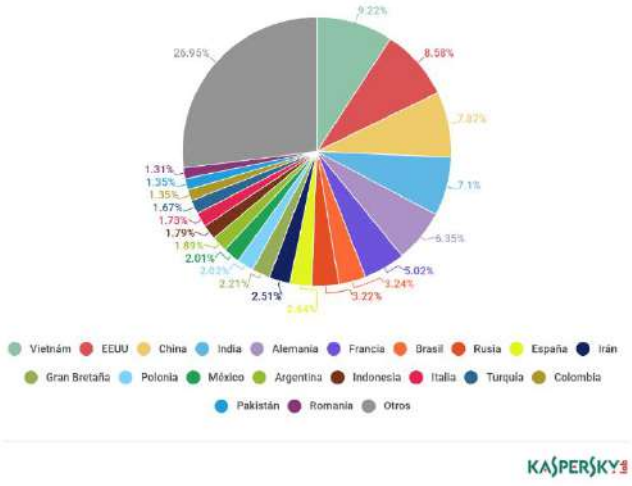

Fig. 5. Estadísticas de ataques de spam y phishing durante 2018
Fuente: Kaspersky

Colombia es uno de los países peor catalogados en cuanto al manejo y cuidados al acceder a las redes sociales.

V. PRINCIPALES VECTORES DE ATAQUE SOBRE REDES SOCIALES

Las redes sociales contribuyen de manera significativa a la evolución y avance de todo el proceso de las comunicaciones a nivel mundial, es por esto que se habla que las redes sociales se apoyan en las llamadas 3C de la web y son las siguientes:

- **Comunicación**: Que sirve para apoyar el conocimiento común de todos los usuarios.
- **Comunidad**: hace referencia a la integración de personas y grupos de personas alrededor de objetivos afines.
- **Cooperación**: Para realización de actividades conjuntas y afines, así como apoyarse mutuamente para la consecución de objetivos comunes.

Pero como no todo es tan bueno y maravilloso, existen infinidad de riesgos a los que se exponen los usuarios que se registran en las diferentes redes sociales.

Siempre se ha hablado que uno de los activos más valiosos es la información y es justo es lo que más se comparte a través de las redes sociales, la información personal de cada uno de los usuarios que se registran y que comparten con los demás miembros de la red queda expuesta y comprometida a poder ser utilizada de manera fraudulenta, es por eso que en el presente artículo se realiza un compendio de las principales vulnerabilidades a las que se ve expuesto este activo y son entre otras las siguientes:

- Suplantación de identidad.
- Uso indebido de la información.
- Phishing.
- Ingeniería social.
- Publicidad.
- Aprovechamiento de los recursos.
- Suplantación de la imagen de personajes famosos para recabar datos de otros usuarios.
- Rumorología.
- Malware.

En otros escenarios se habla de las 10 peores amenazas que han sido detectadas y que generan impacto sobre el uso de las redes sociales, en cada una de ellas se dará un poco más de detalle por ser consideradas de gran relevancia para este estudio, a continuación:

- **Virus de redes sociales**: a través de botnets o robots informáticos, los hackers toman el control de los PCs enviando correos no deseados y que promueve hacer clic en los enlaces para de esta forma instalar software malicioso.
- **Phishing Bait**: un mail que lleva al usuario a entrar a su cuenta de Facebook, esperando que no se identifique la página de su buscador y de esta manera robar sus contraseñas.
- **Trojans**: La zona URL es similar a un banco trojan pero más astuto, puede calcular el valor en La cuenta de su víctima y ayudar a decidir la prioridad.
- **Infiltración de Información:** Los usuarios comparten demasiada información acerca de la organización, proyectos, productos, finanzas, cambios organizacionales, escándalos y otra información sensible en las redes.
- **Abreviación de enlaces:** Los servicios que ayudan a abreviar enlaces para que quepan en lugares más pequeños, también hacen un buen trabajo escondiendo en los enlaces malware permitiendo que las víctimas no se den cuenta que están haciendo clic para instalarlo.
- **Botnets**: Las cuentas de twitter han sido usadas para dirigir y controlar los canales de algunos botnets.
- **Amenazas avanzadas persistentes: (ATP),** Esta es la inteligencia que recopila los datos de personas de alto nivel (ejecutivos, políticos, individuos de alto poder adquisitivo), para quienes las redes sociales pueden ser una fuente importante de información.
- **Cruce de páginas web para falsificación de solicitudes (CSRF):** este tipo de ataques aprovechan a la confianza que brindan las aplicaciones de las redes sociales al ingresar en el buscador de los usuarios. Siempre y cuando la aplicación de las redes sociales no refleje el encabezado del sitio referido será más fácil iniciar un ataque, en el momento en que un usuario comparte una imagen en una secuencia de eventos, otros usuarios podrán hacer click para difundirlos.

- **Impostores:** Muchos impostores han colectado cientos y miles de seguidores en Twitter y los personificados han sido avergonzados cuando los impostores se han hecho pasar por ellos.
- **Confianza**: Cuando un correo electrónico se vuelve popular o un mensaje instantáneo de convierte ubicuo, las personas confían en los enlaces, las fotos, los videos y ejecutables cuando vienen de parte de amigos.

El robo de datos es uno de los riesgos que más proliferan a través de las redes sociales, los datos son robados por los ciberdelincuentes con el fin de utilizar la información para cometer delitos a través de la red y en otros muchos casos son robados y son puestos en venta como ocurrió con datos de usuarios de Facebook procedentes principalmente de Rusia y de Ucrania hace apenas unos meses, de acuerdo con la investigación realizada por la compañía de ciberseguridad Digital Shadow, los hackers se valieron de entradas maliciosas sobre los navegadores Chrome, opera y Firefox para cometer este ciberdelito.

Y, ¿qué piensan las empresas dueñas de las grandes redes sociales con respecto a los riesgos y vulnerabilidades a las que se ven expuestos sus usuarios?, se resolverá esta pregunta en el apartado de recomendaciones.

Las redes sociales como por ejemplo Facebook, se desligan del manejo y cuidado de la información que los usuarios comparten, para ellos, los usuarios al dar aceptar, están de acuerdo con todas las condiciones de manejo de la red social y por ende dan su permiso para que la información sea accesible una vez ellos mismos la suban a la red.

La propagación del malware sobre redes sociales es bastante común, el foco de los ciberdelincuentes se centra en la obtención de credenciales, en muchos casos no para la obtención del control de los dispositivos desde donde está conectado el usuario afectado, los ataques se centran en la búsqueda y obtención de información personal y de otra índole, la cual será utilizada en su mayoría para obtención de beneficios monetarios, pero también en muchos casos para realizar sabotajes contra la integridad de las personas.

En 2018, es uno de los años de más ataques, así mismo como avanzan los desarrollos en materia de ciberseguridad, los delincuentes no se quedan atrás, un año complicado en materia de ciberseguridad dado que por el momento los dispositivos móviles son unos de los más vulnerables por ser la principal vía de acceso a internet y como se mencionaba al inicio del artículo, el uso de dispositivos móviles ha disparado de manera desenfrenada el uso de las redes sociales.

Antes de la revisión de los tipos de malware que buscan infectar a los dispositivos de los usuarios de uso de las redes sociales, se ahondara un poco sobre el mismo, cuando se habla de este concepto se hace referencia a todo tipo de amenaza informática o programas de software malicioso y/o dañino cuyo objetivo es infiltrar en busca de información y causar daño, sus principales formas son las siguientes entre otras:

- Virus.
- Troyanos.
- Keyloggers.
- Spyware.
- Ramsomware.
- Scareware.
- Gusanos.
- Botnets.
- Adware.

En la figura 6, uno de los riesgos más importantes a los que se enfrentan los usuarios de redes sociales y es conocido como phishing.

Fig. 6. Phishing, uno de los riesgos más críticos en redes sociales
Fuente: Redeszone.net

De las anteriores clases de malware las que más proliferan buscando atacar redes sociales son principalmente:

- **Smishing**: Delito o actividad criminal que valiéndose de ingeniería social y empleando mensajes de texto dirigidos a usuarios de telefonía móvil e induciéndolos a visitar páginas fraudulentas buscan infiltrar en este dispositivo en busca de información personal, robar datos bancarios, y/o infectar el dispositivo, esto se da, dado el auge de la utilización de dispositivos para el ingreso a internet y el uso proliferado de las redes sociales a través de estos dispositivos en la actualidad.
- **Spyware:** Software que convierte tu Smartphone en un espía a través de la instalación de programas como flexispy y mobilespy.
- **DroidKungFu**: Virus cuyo principal foco es Android, muy peligroso, roba datos personales y los envía de manera inmediata a los creadores del virus.

Señales muy comunes que pueden dar indicios que un dispositivo móvil pudiera estar siendo atacado por algún virus y se encuentra infectado por el mismo:

- Consumo de batería excesivo.
- Ralentización del móvil.
- Consumo excesivo de datos.
- Pop up en la navegación.
- Publicidad en la barra de notificaciones.
- Redirecciones en tu navegación.
- Aplicaciones no instaladas por el usuario.

Si se presenta en un dispositivo móvil alguna de estas señales, es importante que se revise y se utilice una herramienta de software para detectar posibles virus o malware y conseguir contrarrestarlos.

VI. RIESGOS Y VULNERABILIDADES FOCALIZADOS EN REDES SOCIALES

Es importante tener claro el concepto de lo que es y no es una red social, cuales son los objetivos de la misma, cuales son los beneficios, que esperan los usuarios y muchas cosas más, pero el punto más importante es tener claro los riesgos a los que se exponen los usuarios que las utilizan y sobre todo aquellos que por desconocimiento y exceso de confianza hacen un uso inadecuado de las mismas.

Las redes sociales no son más que servicios a través de los cuales, usuarios y/o individuos quienes como prerrequisito deben crear un perfil personal con sus datos básicos, interaccionan con los demás usuarios ya creados en esta red social, a través de estos servicios, los usuarios se comunican a través de mensajes, comparten información muchas veces confidencial, comparten fotos, comparten videos, y muchas más cosas que pueden ser vistas por todos aquellos que conforman el grupo de contactos.

Los siguientes son los principales riesgos a los que se ven expuestos los usuarios que hacen uso de las redes sociales y sobre todo de aquellos que no hacen un manejo adecuado de las mismas, casi siempre por desconocimiento:

- La publicación, principalmente de fotografías y videos de la vida personal de los usuarios en las redes sociales, los lleva inmediatamente a perder el control sobre su privacidad.
- Uno de los mayores riesgos es poder tener la certeza de realmente estar en contacto a través de la red social con las personas cuyo perfil es verdadero.
- La suplantación de identidad está a la orden del día en las redes sociales.
- En las redes sociales, la vulnerabilidad más grande está dada sobre los menores de edad, esto dado en muchas ocasiones por la mala influencia de amigos y una no correcta asesoría de padres y maestros.
- Principalmente en jóvenes y niños, se da, que no tienen en cuenta todas las indicaciones de los formularios para el registro en las redes sociales y tampoco al momento de la creación de perfil y de la información que se comparte.
- El robo de credenciales y contraseñas es quizás uno de los mayores peligros a través de redes sociales, con solo la obtención del usuario y contraseña los hackers ya tienen acceso a toda la información y aprovechan esto para cometer toda clase de delitos.
- Los usuarios no tienen claro que todo lo que se sube a internet, aunque se borre, siempre quedara allí flotando y podría ser localizado en cualquier momento, este es un riesgo muy latente y peligroso del cual los usuarios muchas veces no tienen el conocimiento.
- La ingeniería social llamada así por cuanto lo definen como el arte de los ciberdelincuentes para disuadir y/o persuadir a los usuarios para que entreguen y compartan información personal valiosa que será utilizada para perpetrar ataques y cometer delitos informáticos.
- Perdida de privacidad, acceso a sitios con contenidos inadecuados, acoso por parte de compañeros y personas desconocidas, incumplimiento de normas legales son otros de los riesgos a los que se ven expuestos en su mayoría los usuarios de las redes sociales.
- El afán de las redes sociales por ser las de mayor auge y participación de usuarios, hacen en muchas ocasiones descuiden el concepto de seguridad que deben mantener sobre este tipo de servicios y no mantienen visión sobre los tres pilares de la seguridad como lo son la integridad, la disponibilidad y la confidencialidad.

VII. PELIGROS, RIESGOS, VULNERABILIDADES EN REDES SOCIALES Y RECOMENDACIONES DE COMO EVITARLOS

Las redes sociales son un foco gigante de peligros, riesgos y vulnerabilidades a las que se ven expuestos los usuarios día a día, aunque atacan a todos, los ciberdelincuentes ponen especial foco en adultos mayores que van desde los 50 a los 65 años y en los niños menores cuyas edades oscilan entre los 8 y los 16 años, esto por cuanto son los más vulnerables por dos razones fundamentales como lo son el conocimiento en la mayor parte de los adultos mayores y la falta de guía y concientización de padres y maestros de cara a los niños y adolescentes, la siguiente es la lista de lo que se considera son los mayores peligros al navegar por redes sociales y algunas recomendaciones de como minimizar y mitigar el riesgo en caso de materializarse el mismo:

- **Suplantación de identidad:** Significa que alguien se hace pasar por quien no es, casi siempre con objetivos maliciosos y en busca de un beneficio lucrativo, el

mayor peligro se da con los llamados pederastas que se hacen pasar por niños justamente para atacar a niños.
Acá la recomendación es denunciar por cuanto esto es un delito, pero también la guía, la educación y la concientización juegan un papel importante para no caer en este flagelo.

- **Malware:** Las redes sociales son un foco de vulnerabilidades que cualquier ciberdelincuente está dispuesto a explotar y para esto se vale de muchas tretas para conseguir instalar programas que roben datos en los dispositivos de los usuarios, programas camuflados en falsos links, falsos correos, falsos anuncios y falsas publicaciones entre otros.
  Acá la recomendación es la utilización de programas antivirus, su continua actualización, pero también es importante desconfiar de invitaciones publicaciones y correos que lleguen de origines desconocidos.
- **Ciberbullyng**: Es uno de los grandes flagelos de la era digital, hace referencia a cuando un niño o un adolescente valiéndose de la internet o cualquier otro dispositivo electrónico, acosa, amenaza, humilla, hostiga, avergüenza o abusa de otro menor o adolescente.
  Acá la recomendación es denunciar y buscar ayuda de padres, profesores y autoridades competentes.
- **Uso indebido de fotos y otros contenidos**: En muchas ocasiones los derechos de imágenes y contenidos pasan a ser propiedad de la plataforma de la red social y esto hace que se pierda el control de los mismos por parte del usuario.
  Acá la recomendación es que se debe documentar claramente en cuanto a las políticas de uso de la red social, revisar políticas de seguridad en cuanto a la privacidad, pero también es importante ser cuidadosos con lo que sube a la red.
- **Problemas legales**: Hay que tener mucho cuidado con lo que se dice y publica en redes sociales, todo tiene repercusión legal.
  Acá la recomendación es justo evitar insultar, difamar, crear falsos rumores contra los demás usuarios de la red y demás personas.
- **Fake News**: Corresponde este peligro a noticias falsas que se difunden por la red social y por su impacto se esparcen como pólvora a una gran velocidad, buscando crear temor, caos, y confusión hacia la opinión pública.
  Acá la recomendación es no creer en todo lo que se divulga y publica, ante la duda se deben consultar fuentes confiables de información.
- **Desprotección de menores**: Uno de los mayores riesgos en menores de cara al uso de redes sociales, justo de acá se desprenden otras grandes amenazas y se da por descuido, falta de orientación por parte de padres y maestros de cara al buen uso de las redes sociales que se debe dar por parte de niños y adolescentes.
  Acá la recomendación es orientar, asesorar y concientizar a menores y adolescentes sobre el buen uso de las redes sociales.

Todos estos peligros y riesgos en las redes sociales listados anteriormente, claramente pueden ser evitados y/o mitigados si se aplican de manera correcta los controles y las recomendaciones mencionadas, aunque muchas veces son obviadas por temas de tiempo y otros factores, con el paso de tiempo pueden llegar a salir más costosas por no haber seguido estas sencillas pero muy practicas recomendaciones.

VIII. MODELO DE SEGURIDAD RECOMENDADO PARA EL USO DE REDES SOCIALES

La tasa de delitos cibernéticos sobre redes sociales crece año tras año, delitos como la suplantación de identidad, robo de datos, son de los más comunes para estas aplicaciones.

En cuanto a concepto de seguridad, es muy importante que las diferentes redes sociales las cuales manejan grandes cantidades de datos personales y otros cuenten con estándares de seguridad muy altos para que así los usuarios se sientan tranquilos y utilicen con toda confianza estos servicios.

Proponer un modelo de cara a mitigar riesgos y evitar al máximo la propagación de ataques informáticos sobre las diferentes redes sociales será el propósito del presente artículo, este modelo se basa en tres pilares:

- Recomendaciones y buenas prácticas.
- Conocimiento de políticas.
- Configuración adecuada de perfiles y uso de privacidad.

A continuación una lista con la recopilación de una serie de recomendaciones, buenas prácticas, creación de políticas, en muchas ocasiones esto sirve más que cualquier aplicativo informático de seguridad y van en pro de minimizar los riesgos inherentes al uso de redes sociales en la actualidad:

- Conocer las reglas, políticas, condiciones de uso y manejo de las diferentes redes sociales.
- Conocer las políticas de la red social en cuando al uso de contenidos, imágenes e información subidos a la plataforma por parte de los usuarios.
- Para el caso de las empresas, se deben crear políticas claras en cuanto al uso de redes sociales en dispositivos corporativos entregados a sus empleados de cara a blindar de manera segura la información de la entidad y salvaguardar su activo más importante.
- Configurar de manera correcta perfiles y usuarios dentro de los parámetros existentes en las redes sociales.

- Dar un adecuado uso al manejo de usuarios y contraseñas.
- Utilizar en lo posible y si la red social lo permite, un segundo factor de autenticación al igual que el protocolo https para navegación.
- Por parte de las empresas utilizar herramientas anti spam y firewall de cara a optimizar la seguridad del sistema ante eventuales riesgos.
- No se debe permitir el uso de usuarios administradores al momento de navegar por redes sociales.
- En las empresas, cada empleado debe tener su propio equipo y su propio perfil para navegar en las redes sociales.
- Utilizar herramientas que permitan monitorear el uso de redes sociales por parte de los empleados.
- Utilizar herramientas que permitan el bloqueo para uso de redes sociales en horarios y para empleados que de acuerdo a su trabajo diario no las requieran.
- Se recomienda no tomar la configuración que viene por default en la red social, es importante tomar un tiempo prudencial para su revisión y configuración propia en pro de mantener el concepto de privacidad y proteger la información y contenidos subidos a la plataforma.
- Se recomienda no utilizar la misma contraseña de la red social en otros sitios de internet.
- Utilizar contraseñas difíciles de adivinar y encontrar, no utilizar nombres y palabras comunes.
- En lo posible evitar el uso de computadores públicos para acceder a redes sociales.
- Evitar dar clic y descargar contenidos que no se tenga certeza provengan de fuentes confiables, esta es la manera que los ciberdelincuentes utilizan para la instalación de malware.
- Configurar un segundo factor de autenticación en la red social es muy importante, siempre que esta lo permita, facebook por ejemplo basa su privacidad en tres pilares, quien puede ver los contenidos es uno, quien puede ponerse en contacto es el segundo y quien puede buscar es el tercero.
- Buscar mantener la información privada fuera del alcance de personas desconocidas.
- Tener mucho cuidado con las cuentas bots, si no tenemos certeza lo mejor es bloquearlas; normalmente las podemos detectar por cuanto contienen letras y números aleatorios y sin mucho sentido.
- Tener especial cuidado con las fake news o noticias falsas, tienen como objetivo crear pánico pero a la vez al ingresar a la misma podemos estar instalando en nuestro dispositivo algún tipo de malware.
- Evitar en lo posible el ingreso a sitios de anuncios, en muchas de las ocasiones son falsos y lo que buscan es instalar malware en nuestros dispositivos.
- Mantener siempre actualizadas las aplicaciones con la última versión existente y contar con claves fuertes y complejas.
- Utilizar programas y herramientas de seguridad para estar libres de malware, evitando así los Keyloggers por ejemplo.
- Utilizar contraseñas de desbloqueo, para nada es recomendable que con solo deslizar los dedos sobre la pantalla del dispositivo, este quede desbloqueado, cualquiera que lo haga quedará inmediatamente con acceso al mismo.
- En caso de no contar con huella dactilar, es importante al menos utilizar el llamado patrón de desbloqueo, aunque al igual es recomendable cambiarlo de manera frecuente, sobre todo por las huellas dactilares que quedan en el mismo de tanto utilizarlo.
- Instalar una app antirrobo, este tipo de aplicaciones lo que permite es ubicar el dispositivo en caso de extravío y en caso de robo permite de manera remota bloquearlo, borrar datos de la tarjeta de memoria, hacerlo sonar en caso que solo este refundido, permite grabar y sacar fotos entre otras funciones.
- Redes WiFi, mucho cuidado con las redes públicas, es como tener un hacker en potencia y aun cuando ayudan en esos momentos en los cuales se carece de datos, se debe ser muy precavidos a la hora de exponer al riesgo cualquier tipo de información confidencial y sensible.
- Buscar la forma de cifrar la información delicada.
- Monitorizar el uso de recursos de los dispositivos móviles.
- Actualizar las versiones del sistema operativo.
- Instalar parches.
- Utilizar directamente el navegador cuando se tengan dudas del enlace al que se va a ingresar, este debe aparecer con las letras HTTPS, lo cual indica que se está utilizando un protocolo de seguridad valido, adicional el color verde en la barra de direcciones y un icono con forma de candado son indicios que la página es legítima.
- Utilizar contraseñas seguras combinando letras mayúsculas, minúsculas y números.
- No compartir demasiada información en las redes sociales.
- Utilizar un bloqueo añadido para apps delicadas haciendo uso de las aplicaciones que se encuentran en el mercado y que se utilizan para imponer contraseñas o patrones de desbloqueo a ciertas apps que se tienen instaladas en los dispositivos y que se consideran como de mayor riesgo, en caso de pérdida, robo y/o hackeo del dispositivo, se pueden utilizar para las redes sociales, apps bancarias, o las que se consideren necesarias.

- Al momento de ingresar a las redes sociales, es importante comprobar que efectivamente se está ingresando a la página correcta, esto aplica al igual para el ingreso a cualquier sitio en internet.
- Tener el control de quien o quienes tienen acceso a la información personal, muy importante sobre todo porque existen personas que valiéndose de algunos de los contactos buscan conseguir información confidencial del grupo.
- Utilizar las bondades de algunas de las redes sociales que permiten organizar las listas de acuerdo a alguna afinidad como por ejemplo grupo de familia, trabajo, estudio y otros.
- Validar que quienes están con aprobación de amistad sean quienes dicen ser y no hay riesgo de suplantación de identidad.
- Mantener bien configurada la privacidad del perfil para que solo las personas del grupo de amigos puedan ingresar a las diferentes opciones del mismo.
- Si no se va a utilizar de manera temporal o definitiva una red social, lo más recomendable es deshabilitar o eliminar de manera definitiva ese perfil.

IX. CONCLUSIONES

El crecimiento en el uso de las redes sociales es hoy por hoy uno de los aspectos más relevantes en cuanto a avances en tecnología, sus grandes ventajas y beneficios de cara a lo que tiene que ver con el mundo de las comunicaciones hacen que utilizarlas aumente de manera significativa.

Este florecimiento implica aparte de los grandes beneficios, infinidad de riesgos que deben ser tratados con la importancia que revisten.

Las pequeñas, medianas y grandes empresas deben preocuparse por el uso adecuado de las redes sociales por parte de cada uno de sus empleados.

Los padres, maestros y demás adultos deben estar muy atentos y ofrecer una orientación adecuada a niños y adolescentes para el uso correcto de las redes sociales.

Las empresas dueñas de las plataformas de redes sociales deben preocuparse mucho más por lo que respecta a la seguridad de la información de sus usuarios y buscar mecanismos como por ejemplo el uso de biometría para garantizar dicha seguridad.

La importancia de las redes sociales en las comunicaciones, el aprendizaje mutuo, la colaboración y el progreso que se puede obtener a través de las mismas es en la actualidad muy relevante.

El uso adecuado o inadecuado de las redes sociales depende de cada usuario y el manejo de la información al igual es responsabilidad de cada usuario.

Los riesgos por el uso inadecuado de las redes sociales afectan de manera más notoria a niños, adolescentes y adultos mayores.

Se estima que una persona en su vida utiliza 5 años y 4 meses conectado a redes sociales.

El uso de redes sociales afecta la productividad de los empleados de las empresas.

En cuanto a la seguridad en las redes sociales no basta solamente con tener las mejores herramientas de seguridad del mercado, el mejor software de encripcion, los mejores certificados digitales, es de vital importancia la sensibilización de los usuarios para que hagan de manera responsable el mejor uso de las mismas.

El concepto de seguridad de cara a las redes sociales va muy de la mano de la edad de las personas; los llamados millenials son menos tolerantes a barreras de seguridad, los jóvenes son propensos a utilizar las redes sociales de manera indiscriminada.

En la actualidad se pone en contexto el concepto de “fraude sintético”, esto es combinar por parte de los cibercriminales información real más información falsa y crear de esta manera una identidad totalmente nueva, esto se da mucho en redes sociales.

A medida que aumenta la utilización de las redes sociales, aumenta también el peligro de vulnerabilidades y riesgos inherentes a ellas y por ende la seguridad siempre debe ir de la mano de este progreso.

Las contraseñas continúan siendo una de las principales herramientas de autenticación, aun por encima de otras herramientas más sofisticadas.

Los usuarios de las redes sociales deben ser muy precavidos en el uso de las redes sociales, es muy importante tener claro que para este uso existen tanto derechos como deberes por parte de cada uno.

El problema no es la existencia de las redes sociales, no son más que una herramienta tecnológica de avanzada, los riesgos y las vulnerabilidades se generan a partir del buen o mal uso que se le dé a las mismas por parte de los usuarios de internet.

Precisamente por lo anterior hay 3 casos de tutela ya interpuestos y el pasado 28 de Febrero de 2019, la corte constitucional en Colombia convoco en una audiencia pública a representantes de Google y Facebook para evaluar entre otros el alcance de la libertad de expresión pero sin

menoscabar los derechos al buen nombre y la intimidad a través de las redes sociales.

REFERENCIAS

[1] Riesgo y vulnerabilidad en las redes sociales. https://www.forbes.com.mx/riesgo-y-vulnerabilidad-en-las-redes-sociales/.

.[2] La vulnerabilidad de tu información en redes. https://mx.blastingnews.com/tecnologia/2018/04/la-vulnerabilidad-de-tu-informacion-en-redes-002498885.html.

[3] Las 10 peores amenazas para la seguridad en redes sociales. https://mundocontact.com/las-10-peores-amenazas-para-la-seguridad-en-redes-sociales/.

[4] Cibercriminales venden datos de cuentas de Facebook. https://mundocontact.com/cibercriminales-ponen-a-la-venta-datos-de-cuentas-de-facebook/.

[5] Las vulnerabilidades, las redes sociales y los dispositivos móviles, grandes objetivos de los ciberdelincuentes. https://www.revistabyte.es/actualidad-byte/456las-vulnerabilidades-las-redes-sociales-y-los-dispositivos-moviles-grandes-objetivos-de-los-ciberdelincuentes/.

[6] Seguridad de la información y redes sociales. http://www.idinteligencia.com/wp-content/uploads/2012/01/seguridad_de_la_informacion_y_redes_sociales.pdf.

[7] Vulnerabilidad en redes sociales. https://sites.google.com/site/vulnerabilidadenredessociales/bienvenidos/.

[8] Redes sociales. https://histinf.blogs.upv.es/2011/12/20/redes-sociales/.

[9] Estadísticas en redes sociales en 2019. https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/.

[10] Los 10 tipos de rede4s sociales y sus características. https://psicologiaymente.com/social/tipos-de-redes-sociales

[11] Red social, que es, tipos de redes sociales y para qué sirven. https://www.mabelcajal.com/2017/06/que-es-una-red-social-tipos-redes-sociales-para-que-sirven.html/.

[12] Tipos de redes sociales que existen en la actualidad. https://www.redes-sociales.com/%C2%BFque-tipos-de-redes-sociales-existen/.

[13] El spam y el phishing en el primer trimestre de 2018. https://securelist.lat/spam-and-phishing-in-q1-2018/86992/.

[14] Las redes sociales, el hogar de los malware y las estafas. https://www.redeszone.net/2016/11/27/las-redes-sociales-el-hogar-de-los-malware/.

[15] Las 5 claves esenciales para evitar los engaños a través de las redes sociales. https://www.redeszone.net/2018/12/10/claves-evitar-enganos-redes-sociales/?utm_source=related_posts&utm_medium=widget.

[16] Malware, principal amenaza para redes sociales y dispositivos móviles. http://www.proteccionononline.com/malware-principal-amenaza-para-redes-sociales-y-dispositivos-moviles/.

[17] Virus, malware y peligros de las redes sociales. http://virusmalwareyredessociales.blogspot.com/.

[18] Los 10 peligros de las redes sociales y como evitarlos. https://www.yoseomarketing.com/blog/peligros-redes-sociales-riesgos/.

[19] Las mejores slidesshares de hoy. https://es.slideshare.net/.

[20] Imágenes de redes sociales. https://es.slideshare.net/search/slideshow?searchfrom=header&q=%22REDES+SOCIALES%22.

[21] Imágenes de redes sociales. https://www.publimarkcreative.com/wp-content/uploads/2017/08/Comunicacion-no-verbal-online.-La-primera-impresion-cuenta.png.

[22] Peligros en redes sociales. https://www.academia.edu/.

[23] Corte cita a google y Facebook por uso de redes sociales. https://www.eltiempo.com/justicia/cortes/corte-hara-audiencia-por-insultos-y-calumnias-en-las-redes-sociales-325418

AUTOR

Carlos Armando Guzmán Sua, se graduó como Ingeniero de Telecomunicaciones en la Universidad Piloto de Colombia, actualmente se encuentra finalizando una especialización en Seguridad Informática en la Universidad Piloto de Colombia.

En la actualidad se desempeña como Gerente General en una empresa de comunicaciones en el departamento de Arauca y desea aplicar todo lo que aprendido en dicha entidad.