HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN DE FUENTES PÚBLICAS, USADAS PARA PREVENIR ATAQUES DE INGENIERÍA SOCIAL EN PERSONAS Y ORGANIZACIONES EN EL CONTEXTO COLOMBIANO.

JOHN JAIRO ALVARADO MURCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2021

HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN DE FUENTES PÚBLICAS, USADAS PARA PREVENIR ATAQUES DE INGENIERÍA SOCIAL EN PERSONAS Y ORGANIZACIONES EN EL CONTEXTO COLOMBIANO.

JOHN JAIRO ALVARADO MURCIA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

MSC. KATERINE MÁRCELES VILLALBA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 7 de septiembre 2021

DEDICATORIA

Quiero dedicar este logró especialmente a Dios por permitirme avanzar día a día en mis metas propuestas, a mis padres, Juan, Cecilia y a mi compañera sentimental Paola por brindarme su apoyo en las metas trazadas.

AGRADECIMIENTOS

Quiero agradecer a todos los tutores, ya que todos con su conocimiento aportaron un granito de arena para la construcción de este documento que es de gran ayuda no solo para nosotros sino también para la sociedad.

Es importante nombrar y agradecer al director de proyecto de grado Joel Carroll Vargas pues fue la persona que me guio por el camino correcto para poder salir adelante con el proyecto propuesto.

A la Universidad Nacional Abierta y a Distancia por ser participe en el logro del gran sueño de ser especialista en seguridad informática.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Amenaza: Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información, las amenazas pueden proceder de ataques (fraudes, virus, robo), sucesos físicos como inundaciones, incendios, etc. o negligencia y decisiones al no implementar cifrado, contraseñas etc.

Ataques: Es un intento organizado e intencionado causado por una o más personas para causar daño o problemas a un sistema informático o red.

Caballo de Troya: Programa creado y que opera bajo un aspecto inofensivo y útil para el usuario, afecta negativamente al sistema al incluir un módulo capaz de destruir datos.

Ciberdelincuente: Persona que realiza actividades delictivas en Internet como pueden ser, ataques informáticos, publicación de sitios ilegales y fraudes o falsificaciones.

Confidencialidad: Propiedad de la información, por la que se garantiza que está accesible únicamente al personal autorizado a dicha información.

Disponibilidad: Propiedad de la información, que garantiza el acceso a los datos en el momento, formato y tiempo que se requiera.

Incidente de seguridad: Un incidente de seguridad de la información es la violación o amenaza inminente a una política de seguridad de la información implícita o

explícita. compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).

Ingeniería social: Conjunto de técnicas en donde se busca engañar a los usuarios para obtener información confidencial.

Integridad: Propiedad de la información, que garantiza que los datos generados no sufren modificaciones por personal no autorizado.

Malware: (Malicious software), Cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

OSINT: La Inteligencia de fuentes abiertas (Open Source Intelligence) OSINT, se refiere al conocimiento recopilado a partir de fuentes de acceso público, el proceso incluye la búsqueda, selección y adquisición de la información, con el fin de procesarlo y analizarlo para obtener conocimiento útil y aplicable en distintos ámbitos, las fuentes de las cuales se puede obtener información relevante son: Medios de comunicación: radio, revistas, periódicos, etc. Información pública de fuentes gubernamentales. Foros, redes sociales, blogs, wikis, etc. Conferencias, simposios, «papers», bibliotecas online, etc.

Riesgo: Es la probabilidad que se produzca un incidente de seguridad al materializarse una amenaza que puede causar daños y perdidas.

Seguridad de la información: Es la disciplina que se encarga de proteger la disponibilidad, integridad y la confidencialidad de la información almacenada en un sistema informático.

Seguridad informática: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente, la información contenida o circulante.

Vulnerabilidad: Es una debilidad, fallo o brecha en un sistema de información que pone en riesgo la seguridad de la información, puede comprometer la integridad, confidencialidad y disponibilidad sí un atacante logra irrumpir la organización.

RESUMEN

Con el avance de la tecnología y del ancho de banda de los servicios de Internet las organizaciones y personas utilizan y adquieren dispositivos para conectarse, compartir y socializar toda clase de información, conllevando a un uso mayor de recursos tecnológicos y equipos para el mejoramiento de los procesos y el flujo de información a sus colaboradores.

En este documento se dará a conocer de forma clara los conceptos básicos de ingeniería social y las herramientas y técnicas usadas por los delincuentes para la recolección de información de diferentes fuentes públicas en Internet, identificando algunos niveles de riesgo en las organizaciones relacionados a la exposición de información que puede usar un atacante para perfilar un objetivo y una guía que permita a las empresas y personas tener en cuenta al momento de exponer información en Internet.

La importancia de Internet cada día se hace muy necesario ya que las organizaciones y personas realizan transacciones, negocios y comercialización de bienes y servicios no solo a nivel nacional sino internacional, por ello se vuelve un objetivo para los ciberdelincuentes que buscan brechas de seguridad en internet para cometer sus delitos. De acuerdo con el informe “Tendencias cibercrimen Colombia 2019 - 2020” del centro cibernético policial de la policía nacional (CAI Virtual) se evidenció el incremento del cibercrimen mediante las denuncias realizadas por empresarios colombianos, en el año 2019 se registraron 30.410 denuncias correspondientes al 54%, entre ellas 17.531 fueron denunciados como infracciones a la ley 1273 del 2009 relacionados a la protección de la información y de los datos representado con un 57%, 12.879 incidentes fueron reportados sin que se llegara a instaurar una denuncia formal ante la fiscalía general de la Nación

representado con un 43%, evidenciando un incremento del 54% de incidentes cibernéticos respecto al año 2018 en donde se gestionaron 8.363 casos[1].

De acuerdo, con el informe del centro cibernético, la Ingeniería social, es uno de los métodos más usados por los ciberdelincuentes para engañar a los usuarios, orientando a realizar alguna acción que pueda producir consecuencias negativas como el robo de contraseñas o información personal al instalar o descargar un software malicioso (malware).

Se espera que esta monografía sirva de soporte a las empresas colombianas, aportando en el uso de herramientas de recolección de información de diferentes fuentes públicas que puedan generar conciencia en las organizaciones al exponer información en internet y que puede terminar siendo el objetivo de un atacante al usar ingeniería social, o que permita el fortaleciendo de los diferentes protocolos de seguridad establecidos en la organización.

[1] Tendencias_cibercrimen_colombia_2019_-_2020_0.pdf. Recuperado 14 de noviembre de 2020, de https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

ABSTRACT

With the advancement of technology and the bandwidth of Internet services, organizations and people use and acquire devices to connect, share and socialize all kinds of information, leading to a greater use of technological resources and equipment for the improvement of the processes and the flow of information to its collaborators.

This document will clearly reveal the basic concepts of social engineering and the tools and techniques used by criminals to collect information from different public sources on the Internet, identifying some levels of risk in organizations related to the exposure of information that an attacker can use to outline a target and guidance that allows businesses and individuals to take into account when exposing information on the Internet.

The importance of the Internet every day is very necessary since organizations and people carry out transactions, businesses and commercialization of goods and services not only nationally but also internationally, for this reason it becomes a target for cybercriminals who seek security breaches on the Internet to commit their crimes. According to the report "Cybercrime Trends Colombia 2019 - 2020" of the cybernetic police center of the Colombian national police (CAI Virtual), the increase in cybercrime was evidenced by complaints made by Colombian businessmen, in 2019 30,410 corresponding complaints were registered 54%, among them 17,531 were reported as infractions to law 1273 of 2009 related to the protection of information and data represented by 57%, 12,879 incidents were reported without a formal complaint being instituted before the prosecution general of the Nation represented with 43%, showing an increase of 54% in cyber incidents compared to 2018 where 8,363 cases were managed.

According to the report of the cybernetic center, Social Engineering is one of the methods most used by cybercriminals to deceive users, guiding them to carry out

any action that may produce negative consequences such as the theft of passwords or personal information when installing or download malicious software (malware).

The increase in social engineering attacks positions Colombia, as the third country in social engineering attacks with 19%, in second place, is Costa Rica with 21% and Uruguay in first place with 24% according to the study carried out by ESET Latin America and the incidents that most affected companies in Latin America.

It is expected that this monograph will serve as support to Colombian companies, contributing to the use of tools for collecting information from different public sources that can raise awareness in organizations by exposing information on the internet and that may end up being the target of an attacker to the use social engineering, or that allows the strengthening of the different security protocols established in the organization.

INTRODUCCIÓN

Es importante mencionar que las telecomunicaciones crecen a pasos agigantados y cada día se comparte mucha información tanto confidencial como personal por medios públicos y privados por ello se hace un blanco fácil y muy apetecido por los ciberdelincuentes, quienes aprovechan los descuidos o vulnerabilidades de las personas en la red para cometer sus delitos, no somos conscientes del tipo de información que terminamos compartiendo en Internet, blogs o redes sociales, pues los ciberdelincuentes usando técnicas como la ingeniería social, y diferentes métodos de suplantación buscan engañar y capturar los datos sensibles de las organizaciones y personas.

Sin lugar a duda en los últimos años se ha evidenciado este problema que ha inquietado a las autoridades a tomar medidas frente a responsabilidad de estas organizaciones que usan bases de datos relacionales o no relacionales para almacenar la información de los usuarios, para que sean datos privados y no públicos y que está en plena responsabilidad del usuario en publicar sus datos en redes sociales si así lo desea, claro está que al ser público genera una brecha de seguridad.

Al exponer todos estos datos en Internet se está cautivando y orientando a los ciberdelincuentes a un estudio de perfiles, ya que a través de una recolección de información de un objetivo puede terminar perfeccionando un ataque a un usuario en común mediante el uso de técnicas de la ingeniería social.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Con el avance de la tecnología y el crecimiento del uso de internet se ha evidenciado que el 96% de la población tienen perfiles en diferentes redes sociales (Facebook, Twitter, Instagram, etc.), el 79% tiene y usa el correo electrónico, el 70% se conecta a sitios de entretenimiento y el 69% usa el internet como medio de consulta de noticias[2], haciendo que internet sea un espacio óptimo para compartir información, intereses, gustos, aficiones en la vida de cada persona, por ello también se incrementa el flujo de datos que es trasportado, despertando el interés de personas mal intencionadas o ciberdelincuentes.

Cabe anotar, que la información que se comparte no solo tiene afectación sobre las personas o individuos sino que también directa o indirectamente sobre las organizaciones, las personas que trabajan o son miembros de las organizaciones pueden compartir información de la compañía consciente o inconscientemente al subir información a diferentes fuentes públicas, lo cual podría representar un alto peligro al ser el objetivo principal de estudio de los delincuentes que aprovechando algún descuido pueden acceder a información confidencial o hasta la propia infraestructura al usar ingeniería social.

Según el estudio realizado por ESET Latinoamérica, el incremento de ataques de ingeniería social posiciona a Colombia, como el tercer país en ataques de ingeniería social en América Latina con un 19%, en segundo lugar, se encuentra Costa Rica con un 21% y Uruguay en el primer lugar con un 24% de los incidentes reportados y que afectaron a las empresas colombianas[3], lo que indica que la población

[2] BEST, C. (2012). OSINT, the Internet and Privacy. 2012 European Intelligence and Security Informatics Conference, 4-4. https://doi.org/10.1109/EISIC.2012.71

[3] S.A.S, E. L. R. Colombia es el tercer país con más ataques de ingeniería social en América Latina. Recuperado 14 de noviembre de 2020, de https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina-2928973

Colombiana no es consciente de la información que se publica en Internet y está siendo usada por personas malintencionadas para cometer delitos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo a través de herramientas de recolección de información de fuentes públicas se logran identificar falencias en la seguridad que pueden ser usadas para un ataque de ingeniería social?

2 JUSTIFICACIÓN

La ingeniería social se ha convertido en un problema no solo para Latinoamérica sino para todo el mundo, Colombia se ve enfrentada al uso no adecuado de las tecnologías de la información y de los datos publicados en internet, esto debido a la falta de conciencia de las personas que no cuentan con el buen habito de proteger la información personal.

De aquí la falta de conocimiento, el mal uso que se da a las tecnologías de la información y la falta de información son los puntos clave para mitigar la exposición de información confidencial en Internet y que son usados por los delincuentes para perpetuar delitos informáticos mediante el uso de ingeniería social.

Para la organizaciones o entidades este es una brecha de seguridad ya que sus colaboradores, consciente o inconscientemente pueden estar compartiendo información, que para ellos no es importante, pero si para las personas mal intencionadas que pueden sacar provecho de estas situaciones haciendo un estudio previo a toda la información contenida en fuentes públicas y que puede terminar siendo usada por los delincuentes para perfilar sus ataques de ingeniería social a una persona en particular.

En este punto, es importante comprender los riesgos asociados que traen las plataformas de redes sociales y la ingeniería social en las entidades, para ello se deben evaluar todos los blancos sensibles para evitar que personas mal intencionadas cumplan su cometido y obtengan acceso a aquella información sensible que pueda significar algún daño a las organizaciones, el atacante inicia recopilando toda la información expuesta en internet de la víctima, contactos, gustos, estados y demás información que se considere importante de la víctima, que después puede ser usada para dirigir un ataque de ingeniería social.

Por estas razones, se hace necesario brindar a las organizaciones colombianas algunas de las herramientas básicas usadas por los ingenieros sociales para la recolección de información y así contrarrestar los delitos informáticos relacionados con la ingeniería social, pues se pueden aplicar búsquedas en las herramientas que permiten visualizar los datos que son expuestos en Internet para así reforzar nuestra seguridad, adoptando medidas de seguridad internas al momento de compartir información.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Establecer herramientas de recolección de información en fuentes públicas, que puedan ser usadas en un ataque de ingeniería social para prevenir la exposición sensible de datos en personas y organizaciones en el contexto colombiano.

3.2 OBJETIVOS ESPECÍFICOS

- Seleccionar a partir de conceptos básicos de ingeniería social, ataques que se realizan a través del uso de herramientas de inteligencia de fuentes públicas.

- Compilar las diferentes herramientas usadas para la recolección de información de fuentes públicas.

- Identificar el tipo de información obtenida de fuentes públicas que puede ser usada por un atacante.

- Elaborar un documento guía de referente informativo para las empresas colombianas que permita ayudar a prevenir la exposición de información sensible en fuentes públicas.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La seguridad informática se puede definir como “la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema seguro y confiable”[4], destinados a preservar la confidencialidad, integridad y disponibilidad de la información agregando otras propiedades como la responsabilidad, la autenticidad y la fiabilidad.

Mientras la seguridad de la información se puede definir “como el conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información”[5].

4.1.1 Antecedentes. La seguridad informática y la seguridad de la información buscan proteger mediante técnicas, metodologías y buenas prácticas los activos de información de las organizaciones y personas, de individuos malintencionados que buscan sacar provecho de las vulnerabilidades o brechas de seguridad en dispositivos y aplicaciones, como es el caso del virus denominado I LOVE YOU o “virus del amor ” que fue un ejemplo bien elaborado de ingeniería social, en donde los usuarios recibían a través de un correo electrónico; un correo con el asunto I LOVE YOU acompañado de un archivo adjunto, al ejecutar el fichero, el virus modificaba los ficheros del equipo víctima y se auto enviaba por correo a todas las direcciones de correo de la víctima, este virus logró infectar a más de 50 millones

[4] LÓPEZ, Aguilera Purificación. (2010). Seguridad informática. [En Línea]: https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=seguridad+informatica&ots=PrjlUzzHW2&sig=NSJdNvBPdN5kIsurEossMI3UJ5Y#v=onepage&q=seguridad%20informatica&f=false

[5] MIFSUD, Elvira. “Introducción a la seguridad informática” [en línea]. [Madrid, España]: Observatorio Tecnológico, marzo 2012 [citado en 10 agosto de 2020]. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridadinformatica?start=1.

de computadoras en todo el mundo, generando pérdidas por más de 5500 millones de dólares.

La ingeniería social es una de las técnicas preferidas por los ciberdelincuentes, en donde buscan atacar al mayor número de víctimas con la menor inversión posible de tiempo, recursos económicos y personas, los ataques de ingeniería social generalmente usan como canal prioritario el correo electrónico para su propagación, este por su gran uso en empresas y particulares; sin embargo, el correo electrónico no es la única vía que utilizan, ya que usan otros canales para llevar a cabo el ataque como lo son las redes sociales, las aplicaciones de mensajería, llamadas telefónicas entre otras.

Tras la puesta en marcha y el nacimiento de internet en 1983 como un proyecto de redes de comunicaciones con potencial para transmitir y recibir información a través de ella, también nace la posibilidad de recopilar toda aquella información pública que por allí circula y algunos peligros que puede traer, como detectar y contrarrestar actividades maliciosas, criminales y terroristas, por ende, el extremismo de estos riesgos ha impulsado el desarrollo de herramientas y técnicas denominada OSINT. El incremento de la información se ha convertido en una amenaza creciente para la identidad personal a través de la vigilancia electrónica, las amenazas a la identidad y privacidad personal no solo provenientes del gobierno sino de delincuentes y grandes intereses comerciales[6].

El ingeniero social busca recopilar todo tipo de información de la persona o individuo que se tiene por objetivo no solo en Internet y redes sociales sino en lugares no pensados como canecas de basura, todo esto con el fin de lograr establecer y encontrar la mayor información posible de la víctima, los diferentes ataques que se presentan en Internet son los avisos instantáneos que ofrecen ganancias con el fin

[6] BEST, C. (2012). OSINT, the Internet and Privacy. 2012 European Intelligence and Security Informatics Conference, 4-4. https://doi.org/10.1109/EISIC.2012.71

de invitar al usuario incauto a registrarse, o con el simple clic que lo redirecciona a una página falsa, o de recibir mediante un correo un link de la entidad bancaria indicando que hay una falla en el sistema y debe cambiar la contraseña y datos personales y al darle clic lo redirecciona a un sitio Web suplantado o idéntico al sitio oficial del banco, es aquí en donde las personas caen en el engaño, otro método es mediante llamadas telefónicas en donde el atacante ya cuenta con un estudio previo de la víctima o de la persona, el atacante realiza la llamada imitando a un funcionario de alguna entidad solicitando información, la persona entrega la información y está puede conllevar a obtener accesos a alguna entidad, red o base de datos, en las llamadas telefónicas también se puede encontrar que se hacen pasar por algún funcionario público, el cual indica que algún familiar se encuentra en problemas y que para poder ayudarlo es necesario que pague algún dinero, él usuario desesperado por la información del problema en el cual se encuentra su familiar cae en el engaño y realiza el pago.

Otro método es registrar la basura de las personas en las oficinas y casas, este método consiste en obtener toda la información relevante que la víctima haya depositado en la caneca de basura logrando encontrar documentos con números de cedulas, NIT, números de cuentas, contactos, números de teléfonos, direcciones, fotos, manuales de empresas, planos, USB, discos duros, agendas personales, etc. El atacante o ingeniero social recopila toda esta información la analiza y sigue ampliando la información de la víctima con los datos encontrados en la basura.

Otro método usado son las redes sociales pues con el auge de internet nace la web 2.0 que representaba una nueva etapa en el surgimiento de nuevas aplicaciones que permiten la participación directa de internet de la gente común, generando múltiples plataformas para compartir contenidos en blogs, wikis, redes sociales, programas p2p, etc. Hacen que el uso de estas aplicaciones sea interactivo y hasta se puedan crear sus propios contenidos, de aquí la red comienza a volverse más

social y aparece lo que hoy en día se llama redes sociales o "social media"[7], toda esta información contenida en las redes sociales hace que sea el bocadillo predilecto para los ciberdelincuentes, al indagar sobre las denominadas redes sociales se pueden encontrar Facebook, Twitter, etc. La Figura 1, muestra las redes sociales más usadas en los últimos 15 años, haciendo que las herramientas tecnológicas evolucionen con dispositivos móviles, mayores anchos de banda, para mantener la necesidad de conexión humana, en la imagen se detalla el Rankin global de las plataformas de redes sociales y el número de usuarios activos de cada una.

Figura 1. El auge y la caída de las plataformas de redes sociales

Global Rank	Social Platform	Parent Company	Monthly Active Users
1	Facebook	Facebook	2.2 billion
2	Instagram	Facebook	1.1 billion
3	Qzone	Tencent	528 million
4	Weibo	Sina Corp	528 million
5	TikTok	ByteDance	524 million
6	Twitter	Twitter	340 million
7	Pinterest	Pinterest	329 million
8	Snapchat	Snap Inc	302 million
9	LinkedIn	Microsoft	260 million

Fuente: Routley, N. (2019, octubre 9). The Rise and Fall of Social Media Platforms. Visual Capitalist. https://www.visualcapitalist.com/rise-and-fall-of-social-media-platforms/

De acuerdo con la Figura 1. se evidencia la cantidad de plataformas de redes sociales que pueden ser usadas por los usuarios, pero si detallamos el número de usuarios activos de cada plataforma se puede afirmar que el tráfico de información que manejan las redes sociales es alto, sin tener en cuenta otros medios abiertos como los son los blogs, noticias y demás fuentes abiertas que pueden ser objeto de recopilación y análisis que basados en OSINT por los ingenieros sociales pueden obtener mucha información para orientar su ataque, según el significado del

[7] MOYA. Analista de Inteligencia en Comunicación Online.pdf. Recuperado de https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/5149.pdf

acrónimo OSINT (OPEN SOURCE INTELLIGENCE), Inteligencia de fuente abierta hace referencia a toda la información recopilada de fuentes públicas disponibles en internet para ser usadas en el contexto de inteligencia.

Como se puede observar el número de usuarios y la cantidad de información que se genera hace que las redes sociales sea un centro de datos para el ingeniero social, en la Tabla 1, se detalla la información que puede ser recopilada por los atacantes en los diferentes sistemas de información.

Tabla 1. Información obtenida de redes sociales

RED SOCIAL O PLATAFORMA	USO	INFORMACIÓN OBTENIDA
Facebook/G+/Hi5/Badoo	Estas redes proporcionan mucha información en general de la persona y sus contactos.	Estados de ánimo, lugares visitados, fotografías, intereses, familiares, relaciones, entre otros.
Twitter/Tuenti/BBM	Establece un listado de actividades, lugares visitados, perfil psicológico, información consultada y gustos de la persona.	Estados de ánimo, fotografías, intereses, lugares visitados.
Linkedin	Identifica el perfil laboral de la persona, conocimientos, trabajo actual, pasados, intereses de trabajo, estudios, etc.	Conocimientos, estado laboral, estudios en proceso, asignación Salarial.
MySpace/Grooveshark/ LastFM	Establece un perfil de preferencias y gustos musicales.	Gustos musicales, música escuchada.
Flickr/Picasa	Establece un listado de actividades, lugares visitados, perfil psicológico, y gustos de la persona.	Gustos particulares, lugares visitados, entorno en que se desarrolla el individuo.

RED SOCIAL O PLATAFORMA	USO	INFORMACIÓN OBTENIDA
Foursquare	Permite geolocalización a las personas e identificar qué lugares suelen frecuentar o sus posibles movilizaciones a través de viajes.	Gustos gastronómicos, lugares visitados.

Fuente: Redes sociales, entre la ingeniería social y los riesgos a la privacidad | Revista .Seguridad. Recuperado 15 de noviembre de 2020, de https://revista.seguridad.unam.mx/numero-12/redes-sociales-entre-la-ingenier%C3%AD-social-y-los-riesgos-la-privacidad

Como se mencionó los atacantes, usando engaños y un poco de psicología pueden encontrar vulnerabilidades en las personas, aprovechando las situaciones de estado de estas, las actividades que realiza, lugares que frecuenta entre otros, logrando formar un perfil de la víctima para después crear perfiles falsos y seguir obteniendo toda clase de información.

La clasificación de la información obtenida por los ingenieros sociales tras el uso de diferentes herramientas es clasificada de acuerdo con su disponibilidad, estas son:

- Información pública: Es toda aquella información que sube el usuario a la red, generalmente se puede encontrar en listas de correo, redes sociales, en foros, blocks, entre otros. El problema que se presenta es que esta información puede estar presente por muchos años en Internet, dejando una huella del usuario casi imborrable. A través de herramientas de OSINT, o solo consultando los repositorios de caches se puede acceder a versiones antiguas de sitios especializados de rastreo o páginas como Shodan.io o Google, con solo aplicar las técnicas de Google Hacking, que tan solo son consultas bien definidas y concretas con palabras clave que permiten obtener información sensible de organizaciones o personas.

- Información oculta: Es aquella información que guardan las aplicaciones en sus ficheros, pero generalmente no conocemos de su existencia se les conoce como metadatos y suelen encontrarse en ficheros como imágenes, documentos de texto, e incluso en la comunicación de algún protocolo.

- Información privada: Es toda aquella información que el usuario introduce en una aplicación o página Web, pero no quiere compartirla con nadie, los datos pueden ser fotografías, cuentas de bancos e información personal, la perdida de esta información suele ser por la mala configuración en las opciones de seguridad o por imprudencia, estas pueden ser indexadas por un atacante o por algún buscador.

Existen varios tipos de ataques que son usados por los ingenieros sociales, en ellos se busca obtener acceso a cualquier sistema sin importar la plataforma, el hardware o software involucrado, las técnicas más usadas y populares son:

- Shoulder Surfing: Es una técnica en la cual el atacante usa técnicas de observación, como ver las notas en las pantallas de los equipos de los empleados, observar por encima del hombro mientras la victima manipula un dispositivo móvil, entre otras, con el fin de obtener información valiosa como correo electrónico, la contraseña de desbloqueo del equipo móvil, contraseñas y demás datos sensibles.

- Dumpster Diving: Esta técnica consiste en la búsqueda de cualquier tipo de información depositada en los contenedores de basura de la empresa, en ellos se puede encontrar agendas telefónicas, manuales, contactos, discos, manuales de políticas de la compañía, planos de red y mucho más, en donde el atacante puede obtener información de la empresa y de su estructura organizacional.

- Caballo de Troya: Es una de las técnicas más usadas en la que a través de engaños se busca que el usuario descargue un archivo malicioso al sistema, al ejecutarlo se crea una puerta trasera en el sistema con la cual el atacante puede acceder en cualquier momento, logrando obtener acceso completo a la máquina de la víctima.

- Juego de roles: Es una técnica en la cual se busca persuadir o reunir información del usuario mediante el uso de sesiones de chats en línea, teléfono, correos electrónicos o cualquier medio que use la empresa para interactuar con el público, en el cual pretender ser un servicio de ayuda, técnico, empleado, o usuario importante para divulgar información confidencial.

- Phising: Esta técnica consiste en crear, usar sitios Web y correos electrónicos elaborados y diseñados para parecerse a los sitios oficiales de reconocidos negocios, agencias gubernamentales e instituciones financieras para engañar a los usuarios de Internet con el fin de entregar la información confidencial y personal. Los sitios falsos persiguen ser una empresa legitima estableciendo en un intento estafar al usuario que entrega la información personal, que después será usada por el atacante para el robo de identidad.

- Ingeniería Social Inversa: Es un método más avanzado de la ingeniería social en esta se busca engañar a los empleados, generalmente suplantan un perfil de alto mando en la organización que informa que tiene algún daño en el acceso al sistema, que las contraseñas no le funcionan, el empleado incauto puede entregar los accesos y contraseñas de acuerdo con lo que le indico el atacante, pues al ser un alto mando en la organización el empleado hace lo posible por solucionar el supuesto inconveniente. En la ingeniería social inversa se presentan tres etapas de ataque que son: Sabotaje, es en donde se realiza al daño inicial, Publicidad, el atacante gana la confianza de la

víctima y lo persigue indicando que él es que puede resolver el problema, Asistencia, es en donde el atacante recibe y obtiene la información que necesita.

- Crawling Sitios Web de organizaciones y foros online: Es toda aquella información que se encuentra en fuentes abiertas sitios Web de la compañía foros y demás, puede contener números de teléfono, correos electrónicos, estructura de la organización y demás información que un atacante puede usar para enfocar y crear un plan para orientar o dirigir su objetivo.

Cabe anotar, que el uso de inteligencia de fuentes abierta OSINT no es reciente, ya que en la antigua Roma existían documentos públicos y pregones donde cualquiera podía enterarse de los rumores que circulaban, y es posible que los generales de la antigüedad consultaran con los comerciantes las condiciones políticas y rumores de los mercaderes se dieran por enterado de las expediciones comerciales[8], de aquí parte la idea de inteligencia de fuentes abierta y se siguió extendiendo en los ámbitos militares, políticos y delictivos.

OSINT generalmente es usado por entidades estatales de orden nacional, agencias de seguridad nacional, compañías con activos de alto valor e incluso por ciberatacantes, en donde las agencias de aplicación de la ley pueden usar OSINT para investigar o establecer un delito alrededor del triángulo de tres aspectos (Motivo, Oportunidad, Medios), de esta forma, podría ser posible conocer los motivos (la razón para desarrollar un ataque) detrás de un atacante, las oportunidades (cuánto puede estar expuesto o vulnerable el activo) que ofrece la

[8] Inteligencia de fuentes abiertas (OSINT): Características, debilidades y engaño | GESI. Recuperado 28 de noviembre de 2019, de http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

víctima y los medios (capacidades requeridas para realizar dicho ataque) que tiene el adversario[9].

4.2 MARCO CONCEPTUAL

OSINT: Es definido como la investigación de información en fuentes abiertas de datos, en idioma ingles es conocido como Open Source Intelligence bajo las siglas OSINT, en la práctica consiste en el uso de un conjunto de técnicas y tecnologías que hacen fácil la recopilación de información que se encuentra disponible públicamente implica que puede ser accesible para cualquier persona sin necesidad de contar con contraseñas de acceso de algún tipo, la información puede ser obtenida de textos, videos, audios, redes sociales, blogs, datos geoespaciales, imágenes entre otros[10].

Los primeros hechos de Inteligencia de fuentes abiertas u OSINT abarcaron la creatividad y la búsqueda de información gratuita disponible de diversas fuentes en forma procesable, remontándose a la segunda guerra mundial, en donde la resolución de problemas no era precisamente la disponibilidad de la información, sino en la capacidad que tenía el recolector de la información para hallar la información relevante y moldearla de tal manera que fuese útil o para beneficio propio[11].

Cabe resaltar que el OSINT la inteligencia de fuentes abiertas fue impulsado por los avances tecnológicos que se fundamentó principalmente en formas novedosas de capturar, recopilar e interconectar la información para llevarlo al contexto de

[9] R. A. Pinto, M. J. Hernández, C. C. Pinzón, D. O. Díaz y J. C. C. García, “Inteligencia de fuentes abiertas (OSINT) para operaciones de ciberseguridad. “Aplicación de OSINT en un contexto colombiano y análisis de sentimientos””. Revista Vínculos: Ciencia, Tecnología y Sociedad, vol 15, n° 2, julio-diciembre 2018,195-214. DOI: https://doi.org/10.14483/2322939X.13504.

[10] L. Ucciferri, 045-seguidores-que-no-vemos-10-2018.pdf. Recuperado 19 de noviembre de 2020, de https://adc.org.ar/wp-content/uploads/2019/06/045-seguidores-que-no-vemos-10-2018.pdf

[11] M. Glassman, Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Recuperado 15 de junio de 2021, de https://www.sciencedirect.com/science/article/pii/S0747563211002585

inteligencia, de aquí, el gran mérito de internet en convertir a cada usuario en la red en una fuente accesible de información, conllevando no solo a un sinfín de información sino del procesamiento adecuado de esta y para lo cual se puede inferir en una serie de características de OSINT como lo son[12]:

- Eficiente, poca inversión de recursos frente al tiempo y los beneficios generados.

- Rápido, el acceso a la información abierta permite de forma ágil ejecutar el ciclo de inteligencia.

- Intermediado, cuando se hace OSINT se pesca en un mar de información y datos que otros ya han generado, por lo que las fuentes ya han pasado por un intermediario o por varios.

- Dependiente, con la presencia de los intermediarios también se refleja la presencia de una fuente y un receptor que generan y sufren dependencia, asimismo tienen a existir varios intermediarios de la forma de periodistas, editores, medios, usuarios etc.

- Accesible, con el bajo costo económico de los medios, permite a los usuarios alimentar el mar de información y con el mismo costo les permite a los buscadores de información hacer OSINT, así cualquier organización o individuo puede hacer uso de esta forma de inteligencia.

- Voluminoso, con el gran mar de información cualquier individuo es una fuente de información.

[12] GESI, Grupo de estudios en seguridad internacional. inteligencia de fuentes abiertas (osint): características, debilidades y engaño. Recuperado 15 de junio de 2021 de https://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

Definición de Ingeniería Social: “La ingeniería social es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso u objetos de valor. En la ciberdelincuencia, estas estafas de "piratería humana" tienden a atraer a los usuarios desprevenidos para que expongan datos, propaguen infecciones de malware o den acceso a sistemas restringidos. Los ataques pueden ocurrir en línea, en persona y a través de otras interacciones”[13]. Los atacantes realizan estafas basados en el comportamiento y los sentimientos de las personas, de esta forma pueden engañar y manipular los usuarios de manera eficaz, la ingeniería social presenta dos vectores importantes de ataque[14]:

- Basados en el uso de tecnología, en donde se hace creer a las personas que se encuentran interactuando verdaderamente con un sistema de información o un programa, con el propósito de obtener información sensible o privada.

- Basados en el engaño humano, usando la naturaleza humana como son congraciar, el ser útil, eficiente o simplemente caer muy bien para obtener información valiosa.

Riesgo: Se puede definir como una eventualidad que impide o imposibilita el cumplimiento de un objetivo, la Organización Internacional de normalización ISO define el riesgo como “la probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existente de un activo o un grupo de activos, generando perdidas o daños”[15].

---

[13] Social Engineering (2020, agosto 26). Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

[14] CARVAJAL, M. (12. 2018.). Estudio de metodologías de ingeniería social. 56.

[15] Admcion_de_Riesgos.pdf. Recuperado 26 de noviembre de 2020, de https://d1wqtxts1xzle7.cloudfront.net/33216454/Admcion_de_Riesgos.pdf?1394789954=&response-content-disposition=inline%3B+filename%3DFCEA_Catedra_Introduccion_a_la_Computaci.pdf&Expires=1606425086&Signature=TqGarUkn6jl3jpmgot49jwCEo6n1GBCsOeBaT74gmVWHfn4tByY4Y-pIFeqe7gBQA9xgYOXogrjWHGKFIt6Bo29TQyDtRs7LVL9Jp2QSYGnP6u~4mzxLmq3FxlzkrWsbO0dk9~nIZbyRxZT2RCrf-bdwS6AZirNZqp55hxkdW4Wn~OM~mZ9NGRnnMOaYSM4qqhVPk~q2Haojq3yCyZSqJiXH0ktKF3i

4.3 MARCO HISTÓRICO

El OSINT actual nació en 1942, bajo la rama Research and Analysis del Office of Strategic Services (OSS), entidad encargada de recopilar toda la información abierta, pedían traer los periódicos de las embajadas y consulados, escuchaban las emisiones de radio públicas extranjeras y en generar accedían a librerías y fuentes oficiales de información[16], observando como los países tenían la necesidad de espiar y tomar medidas de las interceptaciones realizadas.

El ministerio de defensa de España en el estudio de ciberseguridad. Retos y amenazas a la seguridad nacional analizó un caso de OSINT bajo una investigación forense, desarrollado en un proyecto denominado Grey Goose 2 cuya misión era examinar cómo se desarrollaron las operaciones cibernéticas Rusas contra Georgia, en él se identificaron dos sitios Web rusos desde donde se organizaron ciberataques vinculados con el conflicto armado, en los sitios se detallaba los pasos a seguir para atacar sitios georgianos, detalles de listas de objetivos, se ofrecían descarga de programas para participar en los ataques de DDOS, los investigadores deducen que el 90% de los ataques fueron generados por voluntarios y hacktivistas y los sitios Web oficiales y bancarios de Georgia estuvieron fuera de servicio durante varios días[17].

En los últimos años se han publicado algunos ataques, entre los que más se destacan y que han causado más daño se encuentran en, 1999 un pirata informático

2pEt5cLRaE3CZJfkUbLYfLrDBfT7RQOSIt39WzxZhR2tew5AjYtYSLYF4xfnGKgRQGNEHn4NJ6vs0ZCq-HL-QFgFpiDAsFOP7o4x-PkOW6TzhPwVhwY-bTA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[16] Inteligencia de fuentes abiertas (OSINT): Características, debilidades y engaño | GESI. Recuperado 28 de noviembre de 2019, de http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

[17] CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO. Castellano. Recuperado 28 de noviembre de 2020, de https://publicaciones.defensa.gob.es/ciberseguridad-retos-y-amenazas-a-la-seguridad-nacional-en-el-ciberespacio.html

ataca la NASA y el departamento de defensa de Estados Unidos robando nombres de usuario y contraseñas de más de 3.000 cuentas de correos electrónicos, en 2014 se presentó un ataque de Corea del Norte a Sony, la empresa Sony Pictures sufrió un ataque por un grupo de hackers denominados los guardianes de la paz, aunque Corea del Norte negó su participación el FBI acusó al norcoreano Park Jin-hyok por estar detrás del ataque, según el FBI Park trabajó con una empresa que operaba como fachada para el gobierno de Corea del Norte, en el 2015 se presenta un ataque a la red eléctrica de Ucrania, los piratas informáticos cerraron durante 6 horas los generadores de energía eléctrica en tres regiones de Ucrania afectando a más de 230.000 personas, según la investigación realizada por Estados Unidos el ataque se originó en Rusia indicando que es el primer ataque con éxito que realizan los piratas informáticos a una red de distribución de electricidad, en 2016 se presenta el ataque a las elecciones presidenciales en Estados Unidos, los piratas informáticos filtraron miles de correos electrónicos del Comité Nacional Demócrata (DNC), años más tarde el departamento de justicia de los Estados unidos atribuye el ataque a 12 rusos en donde se cree son agentes de la agencia de inteligencia de Rusia, en la investigación se cree que el gobierno Ruso intervino en la votación presidencial ayudando a elegir para ese entonces al candidato del partido republicano Donald Trump, en 2017 se presenta el ataque por WannaCry, un ataque de ransomware conocido como WannaCry afectó a bancos, hospitales incluidos los pertenecientes al Servicio Nacional de Salud (NHS) y otras empresas del reino unido infectando a más de 300.000 computadoras en 150 países, el software cifró los archivos y exigía a los usuarios el pago de cientos de dólares a cambio de la contraseña para descifrar los archivos, Estados Unidos y el Reino Unido culparon a Corea del Norte que negaron la participación y la denominaron como una acusación de “grave provocación política”, en 2019 se presenta el ataque del Bundestag alemán, el ataque se dirigió a todos los partidos políticos del parlamento alemán a excepción del partido de extrema derecha alternativa para Alemania, en el ataque obtuvieron chats privados, tarjetas de identificación e información financiera que fue

publicada por los hacker posterior al ataque, el Gobierno en su investigación no ha nombrado sospechosos, o los posibles motivos del ataque[18].

4.4 ANTECEDENTES O ESTADO ACTUAL

En una encuesta realizada por la casa de investigación del Reino Unido, Vanson Bourne entre diciembre del 2018 y enero del 2019 a los responsables en la toma de decisiones de los departamentos de TI encargada por SophosCybersecurity se indicó que dos de cada tres negocios son víctimas de ataques cibernéticos, Colombia, Brasil y México participaron en la encuesta en donde se les preguntó cómo llego el ataque más significativo a su entorno, los resultados se inclinaron por el correo electrónico con un 33% de los ataques, el 33% ocurrió a través de sitios Web maliciosos en donde es usado en tres de cada 10 ataques, el 23% de los ataques se produjo a través de una vulnerabilidad de software y el 14% a través de una memoria USB o dispositivo externo, del total de los encuestados el 20% de los administradores de TI desconocen cómo se produjo el ataque más importante y las puertas de seguridad que se han dejado abiertas[19].

El panorama para América Latina cada vez es más preocupante, de acuerdo a un estudio realizado por la compañía Rusa Kaspersky detalla que de Julio de 2018 a Julio de 2019 fueron bloqueados 45 intentos de infección cada segundo, entre los que se destacan piratería de Windows de 64 bits y el adware que mediante anuncios masivos durante la navegación invade la privacidad del usuario, pero no son la única amenaza ya que de acuerdo con el informe fueron bloqueados 92 millones de accesos a sitios falsos de phishing en donde Brasil encabezo la lista seguido de Venezuela, según el informe un tercio de los ataques de malware aprovechan vulnerabilidades en América Latina usando las brechas en el protocolo de

[18] WELLE, D. Seis ataques cibernéticos que sacudieron el mundo | DW | 05.01.2019. DW.COM. Recuperado 29 de noviembre de 2020, de https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

[19] SOPHOS, Sophos-impossible-puzzle-of-cybersecurity-wp.pdf. [Consulta: 29 de noviembre de 2020], Disponible en: https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

comunicación SMB que es usado para la comunicación de computadoras servidores, impresoras de red entre otros[20].

De acuerdo al balance realizado por el Centro Cibernético Policial de la policía nacional de Colombia en lo corrido del año 2020 se atendieron a través del CAI Virtual 11.950 incidentes reportados, entre las principales modalidades se encontraron estafa por compra y/o venta de productos 2.391, phishing 1.753, suplantación de identidad 1.776, vishing (voice phishing) 1.087, malware 1.045, amenazas a través de redes sociales 972 e injuria y/o calumnia a través de redes sociales 676, entre los resultados operacionales de la Policía se encuentran 5.165 páginas bloqueadas con material de abuso sexual infantil, 482 portales suspendidos con contenido malicioso (Spam, Malware y Phishing), 541 alertas generadas en redes sociales, medios de prensa y canales de cooperación internacional, 151 noticias falsas identificadas y desvirtuadas con las fuentes oficiales y validadores autorizados y 155 capturas de las cuales 27 fueron por delito de pornografía infantil con menores de 18 años. La ciberdelincuencia se encuentra en crecimiento y cada vez perfeccionan sus ataques aprovechando las vulnerabilidades que dejan los usuarios y empresas en la red, pues el incremento del uso de Internet y las tecnologías de la información y las telecomunicaciones abren una gigantesca oportunidad para que los ciberdelincuentes ataquen[21].

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

De acuerdo con el reporte de Ciberseguridad 2020, Colombia cuenta con un ente máximo para el tratamiento de temas intersectoriales de seguridad digital, en donde se crea el comité de seguridad digital y dentro de sus políticas se incluyó la política

[20] FORBES, En América Latina se registran 45 ataques cibernéticos por segundo Forbes México. Recuperado 28 de noviembre de 2020, de https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/

[21] CENTRO CIBERNÉTICO POLICIAL DE COLOMBIA. Balance_cibercrimen_2020_-_semana_45.pdf. [Consulta: 20 de febrero 2020], Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

de seguridad digital como parte integral de la operación estratégica de entidades públicas y privadas, adicionalmente el Ministerio de Tecnología y las Comunicaciones (MinTIC) tiene desplegado a nivel nacional el modelo de seguridad y privacidad de la información para el apoyo de la gestión e implementación de las buenas prácticas y estándares para la protección de activos críticos de información, infraestructuras tecnológicas y sistemas de información y comunicaciones, adicional cuenta con un equipo nacional de respuestas a incidentes de seguridad digital (colCERT), tiene como objetivo la coordinación de la Ciberseguridad y Ciberdefensa nacional depende del Ministerio de Defensa Nacional[22].

El 24 de julio de 2018 se aprueba el "convenio sobre la ciberdelincuencia" adoptado en noviembre del 2001 en Budapest bajo la ley 1928 y el 16 de marzo de 2020 depositó su instrumento de adhesión, para hacerle frente a los delitos informáticos a través de la cooperación internacional[23].

Colombia ha puesto a disposición de los colombianos diferentes canales para el aprendizaje de seguridad cibernética tanto a nivel de grado y de posgrado, el MinTIC ha otorgado becas a los servidores públicos en las áreas de seguridad digital y ciberdefensa, brindando y patrocinando cursos en las ramas de las TIC, adicionalmente cuenta con un programa denominado "en TIC Confió" que busca crear y promover conciencia sobre el uso apropiado y responsable de Internet y las TIC[24].

El gobierno nacional ha tomado medidas significativas que buscan asegurar el ciberespacio del país con las políticas de seguridad sin embargo el sector privado

[22] BANCO INTERAMERICANO DE DESARROLLO. (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe (2020.a ed.). Disponible en: https://doi.org/10.18235/0002513

[23] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus. MinTIC Colombia. [Consulta: 29 de noviembre 2019]. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-126496.html

[24] Banco Interamericano de Desarrollo. (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe (2020.a ed.). Banco interamericano de Desarrollo. https://doi.org/10.18235/0002513

(en especial las pymes) tienen un largo camino por recorrer ya que deben estar preparadas para las actuales amenazas que se presentan.

4.6 MARCO LEGAL

Ley 1273 del 2009 Ley de delitos informáticos en Colombia "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[25].

Ley 1581 de 2012 Ley de protección de datos personales en Colombia “Tiene por objeto, desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales"[26].

Ley 1928 de 2018 Por medio de la cual se aprueba el “Convenio sobre la ciberdelincuencia” adoptado el 23 de noviembre de 2001, en Budapest, en él se pretende buscar un número común entre las diferentes legislaciones para la lucha de los delitos cibernéticos con cooperación internacional[27].

[25] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273 de 2009. [Consulta: 11 de diciembre 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[26] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. [Consulta: 29 de noviembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

[27] DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA. LEY 1928 DEL 24 DE JULIO DE 2018.pdf. [Consulta: 29 de noviembre de 2020] Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

Ley 1341 de 2009 Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones[28].

Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones[29].

[28] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1341 de 2009. [Consulta: 29 de noviembre 2020], Disponible en: https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009

[29] DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA. Ley 1266 de 31 de diciembre 2008.pdf. Recuperado 30 de noviembre de 2020, de http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

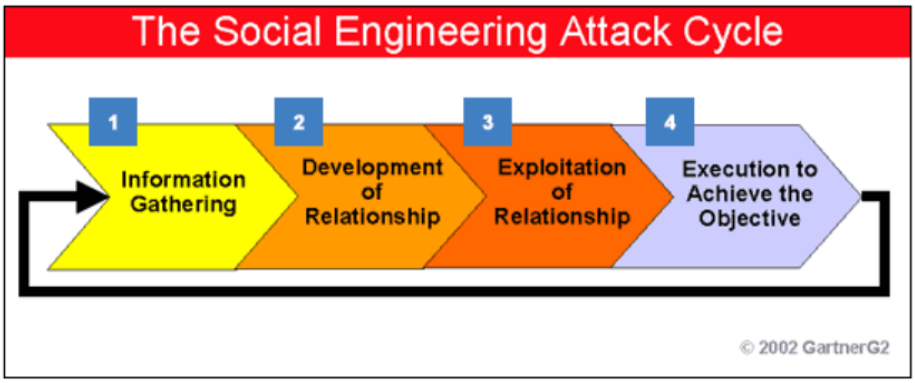
5 DESARROLLO DE LOS OBJETIVOS

5.1 OBJETIVO 1: SELECCIONAR A PARTIR DE CONCEPTOS BÁSICOS DE INGENIERÍA SOCIAL, ATAQUES QUE SE REALIZAN A TRAVÉS DEL USO DE HERRAMIENTAS DE INTELIGENCIA DE FUENTES PÚBLICAS

5.1.1 La ingeniería social. La ingeniería social es el acto de engañar a las personas con el fin de conseguir un beneficio, es considerado como el ataque más peligroso en donde se basa principalmente en la manipulación psicológica de las vulnerabilidades humanas, en donde se considera a la persona como el eslabón más débil de la cadena. Con esta técnica se busca que las personas entreguen información confidencial o de encontrarla sin que el usuario se dé cuenta de ello.

5.1.2 Etapas de un ataque de ingeniería social. Cualquier tipo de ataque informático está basado en una metodología básica, que permite cumplir los objetivos con un mayor porcentaje de éxito; sin embargo, depende del tipo de seguridad que cuente la víctima, para ello se enuncian las principales etapas: Footprinting o reconocimiento, relación de confianza, manipulación psicológica y salida como se ilustra en la Figura 2.

Figura 2. Ciclo de ataque de ingeniería social



Fuente: Ingeniería Social Jose André Morales, Ph.D. 56.

- Footprinting o reconocimiento: Es la técnica de recolección de información sobre el objetivo u objetivos de forma pasiva, consiste en reunir toda la cantidad posible de información, analizarla en busca de vulnerabilidades o brechas potenciales, pero no es una técnica exclusiva que usan los delincuentes, también es usada por periodistas, investigadores, académicos, estudiantes, entre otros. En esta fase se puede encontrar, números de teléfonos y listas de nombres de empleados, direcciones IP, organigramas, Información de las instalaciones y demás información que sea importante para el accionar del ataque o el investigador. En esta fase es necesario indicar que las herramientas OSINT son usadas para la adquisición, procesamiento, recopilación y análisis de la información son Maltego, The harvester entre otras y pueden ser usadas para cualquier técnica de ingeniería social.

- Relación de confianza: Una vez el atacante ha enumerado los posibles objetivos entra a desarrollar una relación con el objetivo que puede ser un empleado o una persona que trabaja en el negocio creando una buena relación con ellos, la confianza que gana y genera el ingeniero social será usada después para ventilar información confidencial que podría causar graves daños a la empresa.

- Manipulación psicológica: En esta etapa, el ingeniero social ya ha ganado la confianza de la víctima y manipula dicha confianza para extraer toda la información confidencial posible y así conocer las operaciones relacionadas al sistema o negocio al que pertenece el empleado, una vez conseguido el objetivo el ingeniero social puede avanzar hacia la explotación del sistema o pasar al siguiente objetivo bajo su consideración.

- Salida: Una vez el ingeniero social ha conseguido toda la información real, realiza una salida desviando o eliminando cualquier tipo de sospecha sobre

él, se debe asegurar de no dejar algún tipo de prueba de su visita que lo involucre con el rastro de su identidad real, tampoco lo puedan vincular a las entradas no autorizadas en el sistema en el futuro.

5.1.3 Tipos de ataque de ingeniería social. Los ataques de ingeniería social se pueden dividir en dos tipos Hunting y Farming que se enunciaran a continuación.

5.1.3.1 ***Hunting.*** Este tipo de ataque busca obtener datos e información específica del objetivo con la menor exposición directa posible, generalmente se busca obtener X dato, puede ser contraseñas o credenciales de acceso a algún servicio o cuenta, el atacante se pone en contacto con la victima de alguna forma y la incita a entregar sus datos personales, el mejor ejemplo son las campañas de phishing por correo, en donde el atacante tiene contacto directo con la victima a través del correo solo una vez, en donde usualmente se hace pasar por una entidad o conocido suplantando sitios Web legítimos.

5.1.3.2 ***Farming.*** En este tipo de ataque se busca obtener algo y desaparecer con una exposición mínima, el objetivo del ataque es mantener el engaño en el mayor tiempo posible, exprimiendo al máximo el conocimiento y recursos de la víctima.

5.1.4 Técnicas de ingeniería social

5.1.4.1 ***Tailgating***. También conocido como piggybacking, esta técnica busca aprovechar la solidaridad o inconciencia de un empleado autorizado al abrir una puerta a un desconocido para ingresar a un área restringida, un atacante puede saltarse la seguridad de los controles de acceso solicitando la ayuda de un empleado.

5.1.4.2 ***Phishing.*** Técnica que consiste en engañar a un grupo masivo de usuarios a través de correos electrónicos, mensajes de texto falsos, páginas Web, perfiles sociales con el fin de obtener o robar la información confidencial.

5.1.4.3 ***Spear Phishing.*** Esta técnica es considerada más avanzada que el Phishing, pues requiere de más esfuerzo por el atacante, conlleva en analizar el objetivo, conocer de sus actividades diarias, sus gustos y demás información relevante, con esta información se enfoca en un solo objetivo y elabora el Phishing dirigido a la víctima, con nombre propio, haciendo que la víctima pueda creer con mayor facilidad.

5.1.4.4 ***Whalling.*** Es un ataque de tipo Phishing que busca suplantar u ocupar altos cargos en la compañía con el objetivo de atacar directamente a los altos ejecutivos u otros cargos importantes dentro de la organización.

5.1.4.5 ***Pretexting.*** Esta técnica consiste en intentar convencer a la víctima para que entregue información valiosa, generalmente viene apoyada con una historia o pretexto, en el cual el atacante toma un cargo de alto nivel o autoridad que tiene derecho a acceder a la información que busca.

5.1.4.6 ***Baiting.*** El baiting (cebo o poner carnada) consiste en dejar dispositivos de almacenamiento como memorias USB, discos ópticos infectados con algún tipo de malware en lugares públicos con el fin de que algún empleado la recoja por curiosidad y la inserte en los dispositivos de la empresa u hogar.

5.1.4.7 ***Vishing.*** Esta técnica consiste en realizar fraude a través de una llamada telefónica, ofrecen a la víctima un número de teléfono falso para comunicarse, suplantando el verdadero para después obtener los datos personales.

5.1.4.8 ***Ingeniería social inversa.*** Esta técnica consiste en realizar un estudio sobre un objetivo en concreto, observar su comportamiento para después crear un problema e involucrarse para solucionarlo.

5.1.4.9 ***Shoulder surfing.*** Consiste en observar o mirar por encima del hombro a un usuario al momento de ingresar a un portal o al propio equipo de la oficina con su contraseña.

5.1.4.10 ***Dumpster diving.*** Consiste en el acto de husmear o buscar entre la basura, con el fin de encontrar u obtener información personal.

5.1.4.11 ***Cartas Nigerianas.*** Esta técnica consiste en ilusionar a un usuario con una fortuna que no existe y persuadirla para que pague una mínima cantidad de dinero para ganar una mayor cantidad.

5.1.4.12 ***Quid pro quo.*** Esta técnica busca seleccionar a personas desprendidas de la organización con promesas de entregar algo a cambio con el fin de obtener información confidencial, las promesas generalmente vienen acompañadas de compensaciones monetarias, vacaciones y demás.

5.1.4.13 ***Sextortion.*** La sextorsión o extorsión sexual consiste en chantajear a una persona con revelar por medio de un video o fotos información intima con el fin de que la víctima pague al extorsionista.

5.1.4.14 ***Sexting.*** Consiste en el envío y recepción de contenido sexual por medios electrónicos, mensajes de texto, videos o fotos de contenido erótico usando aplicaciones de mensajería instantánea, correo electrónico, redes sociales u otros tipos de herramientas de comunicación.

5.1.4.15 ***Ciberacoso o Ciberbullyng.*** Consiste en avergonzar u humillar por medio de las diferentes tecnologías de la información a una persona, causando daño de manera repetida, deliberada y hostil.

5.1.4.16 ***Redes sociales.*** Esta técnica tiene dos objetivos, el primero es obtener toda la información posible y el segundo es la de generar algún tipo de relación con la víctima. Existen personas que publican el minuto a minuto de su vida en redes sociales lo que hace para los atacantes “oro puro”, pues entregan información por ellos mismos que puede terminar en un delito.

5.1.4.17 ***Grooming.*** Esta técnica es realizada por un adulto que a través de engaños busca ponerse en contacto con adolescentes, niñas o niños por medio del uso de las tecnologías de la comunicación y telecomunicaciones, con el fin de obtener concesiones de carácter sexual.

Una vez estudiadas las técnicas y el modo de operación de los ingenieros sociales se puede contar con cierto conocimiento para no caer en las manos de los delincuentes, claro está, que depende del tipo de información que se comparte en internet; de nada sirve estar atento de los posibles ataques de ingeniería social si las personas no son conscientes de la información que se pública.

5.2 OBJETIVO 2: COMPILAR LAS DIFERENTES HERRAMIENTAS USADAS PARA LA RECOLECCIÓN DE LA INFORMACIÓN DE FUENTES PÚBLICAS

Como se mencionó anteriormente todo ataque de Ingeniería social inicia con una actividad de reconocimiento de aquí la importancia de OSINT para cualquier tipo de investigación basada en la obtención de información a través de fuentes abiertas, social networks o redes sociales en mensajes, conversaciones, publicaciones, videos e imágenes para analizarla y llevarla al campo de la inteligencia[30], el proceso de OSINT consta de 6 fases como se detallan en la Figura 3.

Figura 3. Fases de OSINT

[30] ¿Qué es SOCMINT? Para qué sirve + Aplicaciones + Fases. (2019, agosto 27). Recuperado 11 de diciembre de 2019, de CiberPatrulla website: https://ciberpatrulla.com/socmint-social-media-intelligence/

Fuente: OSINT - La información es poder. (2014, mayo 28). INCIBE-CERT. https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

A continuación, se describe cada una de las fases de OSINT.

- Fase de requisitos: Se establecen todos los requerimientos a cumplir, identificando las condiciones para dar cumplimiento al objetivo a resolver.

- Fase de identificación de fuentes de información relevantes: Se debe especificar las fuentes de interés que serán recolectadas.

- Fase de adquisición: Fase en donde se obtiene la información de las fuentes mencionadas.

- Fase de procesamiento: En esta fase se da formato a la información recolectada.

- Fase de análisis: En esta fase se genera inteligencia partiendo de los datos recolectados y procesados. El objetivo es relacionar la información recopilada con distintos orígenes encontrando patrones que permitan dar una conclusión significativa.

- Fase de presentación de inteligencia: En esta fase se presenta la información obtenida.

5.2.1 Herramientas OSINT. A continuación, se presentan diferentes herramientas que permiten recolectar información a partir de fuentes abiertas.

5.2.1.1 ***Portales Web***. En la tabla 2, se lista una serie de portales Web para la recopilación de información.

Tabla 2. Portales Web

PORTAL WEB	CARACTERÍSTICAS
Navegadores Web	Google, Microsoft Edge, Mozilla, Tor, etc. Permiten la búsqueda de información de empresas, empleados etc. Caso es el de Google que proporciona comandos de operador avanzado para la búsqueda de información. https://support.google.com/websearch/answer/2466433?hl=es Además de la geolocalización de una dirección objetivo y búsqueda de imágenes.
Whois	Permite obtener el propietario de un nombre de dominio o una dirección IP en Internet.
Shodan	Permite encontrar tipos específicos de dispositivos (servidores, routers, Firewall) en Internet.
Archive.org	Permite ver las versiones anteriores de una página Web (Cache), puede proporcionar nombres de exempleados.
beenverified.com	Es un servicio Web que puede proporcionar antecedentes penales de un objetivo.
haveibeenpwned.com	Permite buscar múltiples violaciones sí una cuenta de correo se ha visto comprometida.
TinEye	Es un motor de búsqueda inversa de imágenes basado en los metadatos.
mxtoolbox	Permite saber la integridad de la dirección IP.
Facebook, Twitter, FrendFinder, Linkedin, entre otros.	Pueden revelar gran cantidad de información, como son experiencias, gustos, estados, estructura de las empresas entre otras.
webmii.com	Es un servicio Web que permite ubicar personas y encontrar toda la información que se encuentre pública en Internet.

Fuente: El autor

5.2.1.2 ***Herramientas diseñadas para OSINT.*** En la tabla 3, se listan una serie de herramientas diseñadas para la recopilación de Información.

Tabla 3. Herramientas diseñadas para OSINT

HERRAMIENTA	CARACTERÍSTICA
Maltego	Es una herramienta interactiva de minería de datos que presenta gráficos dirigidos para el análisis de enlaces. La herramienta puede ser usada en investigaciones en línea para encontrar relaciones entre piezas de información de varias fuentes ubicadas en Internet. Entre ellas se encuentran: Personas (Alias, Correos electrónicos y Nombres), Grupos de personas (en redes sociales), Empresas u Organizaciones, Sitios Web, Infraestructura en internet (Nombres, Dominios, DNS, Direcciones IP, Bloques de red, Afiliaciones Documentos y archivos).
Tinfoleak	Es una herramienta SOCMINT (Social Media Intelligence) que permite automatizar la extracción de información detallada de una cuenta en Twitter. Entre sus características se encuentran para Buscar fugas de usuarios de Twitter se encuentran: Información básica de un usuario en Twitter (ubicación, imagen, nombre, seguidores, etc.), Equipos y sistemas operativos usados por el usuario en la red social Twitter, Aplicaciones y redes sociales usadas por el usuario de Twitter, Lugar y coordenadas de geolocalización con el fin de generar un mapa de seguimiento de las ubicaciones que visito. Mostrar tweets del usuario en la plataforma de Google Earth, Descargar las fotos encontradas de un usuario en Twitter, Hashtags usados por el usuario de Twitter y resultados de cuándo se usó (fecha y hora), Menciones del usuario por parte del usuario de la red social Twitter y cuándo se produjeron (fecha y hora).
The Harvester	El objetivo de esta herramienta es reunir correos electrónicos, subdominios, hosts, nombres de empleados, puertos abiertos y pancartas de diferentes fuentes públicas como bases de datos informáticas SHODAN, servidores de claves PGP y motores de búsqueda. Entre sus características se encuentran:

	Retrasos entre solicitudes, Buscar todas las fuentes, Verificador de host virtual, Enumeración activa (enumeración DNS, búsquedas inversas, expansión de TLD), Integración con la base de datos de la computadora SHODAN, para obtener los puertos y banners abiertos, Guardar en XML y HTML, Gráfico básico con estadísticas.
Recon-ng	Es un framework de reconocimiento Web escrito en python, entre sus características principales se encuentran, módulos independientes, interacción con base de datos, ayuda interactiva, y completado de comandos. Recon-ng ha sido diseñado exclusivamente para reconocimiento basado en Web open source, permite identificar y buscar de una manera más o menos automatizada información sobre: Hostnames, IP´s, localizaciones y emails.
Intel Techniques	Es una máquina virtual Linux que viene preconfigurada para investigadores en línea, fue desarrollada por Michael Bazzel y David Westcott, proporciona un conjunto de servicios orientados a OSINT. Entre los módulos se encuentran: Facebook, este módulo permite la búsqueda de perfiles usando Facebook, Documents, este módulo permite la búsqueda de documentos a través del buscador de Google, Image reserval, este módulo se usa para reconocimiento facial usando algoritmos de inteligencia artificial de Google, UserSherlock, este módulo permite la búsqueda de cuentas a través de internet que usen usuario con nombre similar al del objetivo.
Datasploit	Es una herramienta de investigación automatizada para la recopilación de dominios, persona, correos electrónicos, teléfonos y demás información relevante acerca de su objetivo.

Fuente: El autor

Las herramientas mencionadas como portales Web y las herramientas diseñadas para OSINT permiten recopilar todo tipo de información que se encuentre pública

en internet, con el fin de que pueda ser analizada para convertirla en información útil para el atacante o el ingeniero de seguridad de la entidad.

5.3 OBJETIVO 3: IDENTIFICAR EL TIPO DE INFORMACIÓN OBTENIDA DE FUENTES PÚBLICAS QUE PUEDE SER USADA POR UN ATACANTE

Una vez identificado el alcance, el potencial de los portales Web y de las herramientas OSINT, se logró encontrar un listado de información de las organizaciones que puede ir desde la exposición de datos en Internet hasta indicios de entrega de información importante basado en el comportamiento de los empleados activos en redes sociales, sitios de una organización en donde se describen detalles como eventos, avances y demás, sitios Web en donde los empleados opinan y son de acceso público, servicios en la Web para empleados que pueden contener alguna vulnerabilidad a ser explotada, las organizaciones mencionan o describen personas o integrantes para la colaboración con otras entidades, etc. Los niveles de riesgo a que las organizaciones están expuesta dependen de su actividad económica, por ende, el objetivo de los ciberdelincuentes en la búsqueda de información puede conllevar a:

- Información y estado de la red.
- Información de sistemas operativos.
- Información de la entidad, como puede ser información del CEO y de empleados, números de contacto, direcciones de correos electrónicos, etc.
- Diagramas de red.
- Nombres de empleados.
- Experiencia de los colaboradores.
- Servicios de red.
- Información y datos de aplicaciones Web y de su configuración.
- Arquitectura del sistema.

- Información de los sistemas de detección y prevención de intrusiones implementado, etc.

En la tabla 4, se detalla la información que puede ser obtenida por un atacante.

Tabla 4. Información y datos obtenidos

INFORMACIÓN	DATOS OBTENIDOS
Información y estado de la red	• Información de nombres de dominios interno. • Nombres de dominio que la empresa usa para llevar a cabo las funciones de negocio en donde se puede incluir relaciones con los clientes. • Direcciones IP de los sistemas y recursos disponibles. • Sitios Web no monitoreados o que son usados para pruebas. • Sitios Web privados. • Tipo de servicios usados (TCP/UDP) o que se ejecutan. • Autenticación de equipos y sistemas. • Información de VPN red privada virtual. • Mecanismos de control de acceso incluyendo Firewall y ACL. • Información de IDS e IPS y datos de configuración. • Números de teléfono incluyendo VoIP o análoga.
Información de sistemas operativos	• Arquitectura del sistema. • Versión del sistema operativo. • Usuario y grupo de información. • Tablas de enrutamiento (ARP). • SNMP • Datos de sistemas remotos. • Contraseñas.
Información de la entidad	• Información del sector ya sea público o privado. • Detalles de los empleados. • Sitio Web de la entidad.

	• Detalles de su ubicación. • Números de teléfono y direcciones de correo. • Enlaces de servidores Web importantes de la organización. • Antecedentes de la entidad. • Políticas de seguridad implementadas en la organización. • Comunicados de prensa, artículos de noticias, blocks.
Diagramas de red	• Proporciona información de interconexión entre dispositivos, Firewall, router, switches, computadores y demás. • Información de direccionamiento de subredes (direcciones IP, máscaras de ID, VLAN).
Nombres de empleados	• Información importante como números de identificación, teléfonos de contacto, correos electrónicos, dependencia o cargo actual en la organización. • Vínculos familiares, datos de residencia etc.
Experiencia de los colaboradores	• Información de estudios actuales y ejercidos. • Certificaciones realizadas. • Empresas en las que ha laborado.
Servicios de red	• Voz y datos • Radiodifusión TV y radio. • Internet. • Correo electrónico. • Listas de distribución. • Transferencia de archivos FTP.
Información y datos de aplicaciones Web	• Aplicaciones Web estática (desarrollado bajo HTML y CSS). • Aplicaciones Web dinámicas (desarrollado bajo PHP y JavaScript). • Tiendas virtuales o de comercio electrónico (e-commerce). • Portal Web de App.

	• Aplicaciones Web animada (está relacionada con tecnología Flash, CSS y SVG). • Aplicaciones Web con gestor de contenido (Drupal, WordPress y Joomla).
Arquitectura del sistema	• Estructura del sistema, elementos componentes y partes. • Información entre los elementos. • Características y propiedades lógicas y físicas del sistema.
Sistemas de detección y prevención de intrusiones	• Información del fabricante. • Información del modelo, versionamiento y referencia.

Fuente: El autor

La información recopilada u obtenida por las diferentes herramientas es usada generalmente para perfilar un ataque de ingeniería social basado en la información recolectada, explotando las vulnerabilidades que le permitan al atacante perfilar un objetivo con mucha precisión, pero también puede ser de gran utilidad para las empresas y personas, puesto que con ello pueden fortalecer la seguridad personal, o de una entidad en particular.

5.4 OBJETIVO 4: ELABORAR UN DOCUMENTO GUÍA DE REFERENTE INFORMATIVO PARA LAS EMPRESAS COLOMBIANAS QUE PERMITA AYUDAR A PREVENIR LA EXPOSICIÓN DE INFORMACIÓN SENSIBLE EN FUENTES PÚBLICAS

Es importante tener en cuenta que las técnicas de ingeniería social y las herramientas para la recolección de información son cambiantes y cada vez son más estructuradas y eficientes, lo que conlleva a tomar medidas de seguridad que permitan minimizar el impacto de las empresas colombianas a través de la implementación de políticas de seguridad, la concientización, sensibilización y capacitación constante de los usuarios en materia de ataques de ingeniería social.

A continuación, se describen algunas sugerencias para evitar que la información sensible sea usada para un ataque de ingeniería social tanto para personas y empresas.

5.4.1 Para empresas

- Firewall o cortafuego perimetral, para que bloquee el acceso y la salida de comunicaciones no autorizadas, este debe contar con buenas políticas de seguridad y una adecuada configuración, evitando las configuraciones por default.

- Web Application Firewall WAF o cortafuego de aplicación Web, permite la protección de los servidores de aplicaciones Web de determinados ataques en Internet.

- Sistema de detección y prevención de intrusos IDS/IPS, se encargan de vigilar el tráfico para detectar patrones sospechosos en la compañía.

- Antivirus, anti-phishing, antispyware, antispam, permiten detectar amenazas que pueden llegar a los usuarios.

- Web Gateway o puerta de enlace, permite filtrar la navegación de los usuarios en la compañía.

- Email Gateway o puerta de enlace de correo electrónico, permite el filtrado de los correos electrónicos evitando correos no deseados, suplantación de identidad, virus y amenazas avanzadas.

- Actualizaciones y parches de seguridad, permiten mitigar las vulnerabilidades en los sistemas operativos, equipos de comunicaciones, bases de datos y servicios Web.

- Autenticación, permite controlar el acceso y saber que usuarios son, en los casos de acceder a información sensible es necesario implementar una autenticación en dos pasos o un doble factor de autenticación, usar contraseñas con un mínimo de 12 caracteres alfanuméricos en donde se incluya mayúsculas, minúsculas, caracteres especiales y números, evita establecer contraseñas con fechas, nombres, direcciones de domicilio y números de teléfono de familiares.

- Roles y perfiles, permite establecer los permisos y restricciones que tiene cada usuario basado siempre en el principio del mínimo privilegio.

- Cifrado de discos duros, permite a los usuarios proteger la información allí depositada evitando que personas sin autorización accedan a ella, y así prevenir la fuga de información.

- Red privada virtual o VPN, permite la comunicación externa de forma segura a los sistemas de información corporativa.

- Controles de acceso, permiten identificar a los usuarios frecuentes y no frecuentes en las instalaciones, implementar requisitos de ingreso, carnet visible y acompañamiento en los casos de los visitantes.

- Información con sentido de urgencia, tómese el tiempo y analice que tipo de información le están solicitando, identifique y confirme la persona, la mayoría de los ataques se producen transmitiendo un sentido de urgencia, con ello evitara entregar información sensible.

- En casos en donde se presente duda con órdenes de compra, pagos, transferencias bancarias consulta con tu jefe inmediato o superior a cargo.

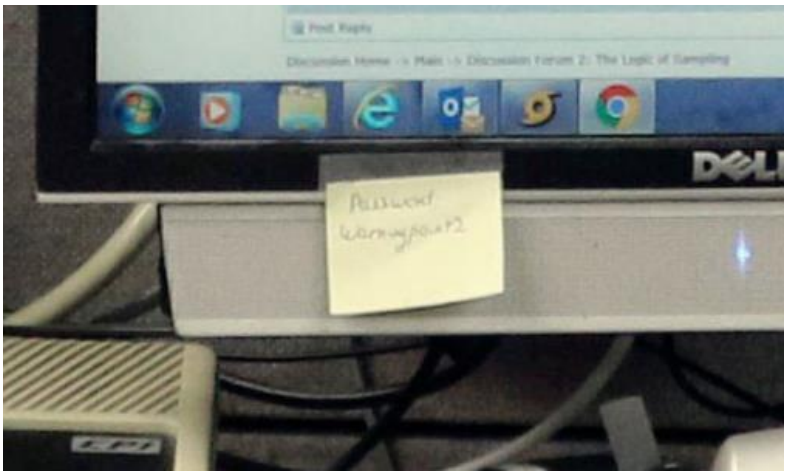
- Equipos de cómputo, los equipos que asigna la compañía son para el uso de las actividades diarias, no abrir enlaces, archivos adjuntos sospechosos que se reciban por correo, tener cuidado al momento de abrir correos personales.

- No divulgar o compartir información sobre proveedores, cronogramas, organigramas, seguridad o procedimientos internos de la empresa.

- Asegura el equipo portátil, en caso de salir o cada vez que se retire de la oficina, verificar que la guaya de seguridad quede conectado al equipo, bloquear la sesión o apagar el computador.

- Dejar solo lo necesario en el escritorio, no utilizar post-it o papelitos para apuntar contraseñas, usuarios o información confidencial, no dejar documentos impresos con información sensible en la figura 4, se muestra información confidencial escrita y adherida a un equipo de cómputo en donde alguna persona puede tomar los datos y usarlos para beneficio propio.

Figura 4. Post-it con contraseña



Fuente: https://www.microsiervos.com/archivo/seguridad/agencia-gestion-emergencias-hawaii-post-it-contrasena.html

- Retirar unidades externas de los equipos, no dejar USB, CD o DVD en los equipos de cómputo o en lugares visibles, no insertar memorias de dudosa procedencia, en la figura 5, se muestra el uso de los dispositivos de almacenamiento externo, en donde un delincuente puede hacerse de la memoria, insertar código malicioso para que se ejecute una vez sea insertada en el equipo.

Figura 5. Unidades externas de almacenamiento

Fuente: https://www.usbpersonalizado.es/blog/usb-vs-dvd/index.html

- Realizar pruebas de Pentesting en la organización que permitan identificar brechas de seguridad, antes de que estas sean usadas por un ciberdelincuente, las herramientas OSINT ayudan a identificar las vulnerabilidades expuestas.

- Realizar simulacros de seguridad con los empleados en donde se concientice y sensibilice sobre las técnicas de ingeniería social, su funcionamiento y la afectación que puede ocasionar a la organización.

- En caso del uso de redes sociales corporativas es necesario establecer y configurar la seguridad en el perfil, cambiar las contraseñas periódicamente y asignar como mínimo 12 caracteres alfanuméricos en donde se incluya mayúsculas, minúsculas, caracteres especiales y números, evita establecer contraseñas con fechas, nombres, direcciones de domicilio y números de teléfono de familiares.

5.4.2 Para usuarios o personas

- Crear contraseñas complejas, el uso mínimo de 12 caracteres alfanuméricos incluidos mayúsculas, minúsculas, caracteres especiales y números para cada cuenta evita que un ciberatacante pueda adivinar la contraseña, un ejemplo de una contraseña con 13 caracteres alfanuméricos es: L@v1d@3$B3LL@, es recomendable el cambio de las contraseñas periódicamente en cada cuenta online.

- Cambiar las contraseñas periódicamente, no almacenes ni grabes las contraseñas en los dispositivos móviles y computadores, mantener las cuentas destinadas al comercio separadas de las cuentas personales.

- Mantener actualizado el antivirus, Firewall de los equipos de cómputo y dispositivos móviles.

- Gestionar y mantener una copia de seguridad de la información de la computadora y de los dispositivos móviles.

- Tener precaución frente a las ofertas, sí una oferta es demasiado buena, termina siendo una estafa en la figura 6, se muestra una notificación de un premio, el usuario incauto puede al hacer click estar entregando información valiosa como son sus datos personales y adicional, su dirección IP, versión del sistema operativo, versión del navegador, sin contar que al hacer click en el enlace se descargue algún código malicioso que le permita al atacante recopilar más información.

Figura 6. Ofertas de premios

Fuente: https://www.iberdrola.com/innovacion/estafas-internet

- Mantener la información personal protegida y segura, no almacenes videos o imágenes intimas que pueden terminar en manos de otra persona y manipulando para que esta no sea ventilada.

- En caso de presentarse una situación de estafa o fraude reportar ante las autoridades competentes a través del enlace https://caivirtual.policia.gov.co/

5.4.2.1 Redes sociales

- Establecer los controles de seguridad necesarios a través de las redes sociales, permitiendo solo el acceso a amigos y familiares conocidos.

- Evite publicar lugares que frecuenta o asistencia, no publique información personal como teléfonos, lugar de trabajo, dirección de residencia entre otras, esta información puede ser usada por un atacante para realizar engaños a familiares, amigos o hasta usted.

- Evite publicar cambios del estado sentimental o algún problema relacionado, esta información puede ser usada por un atacante para establecer contacto con el ofrecimiento de ayuda con el fin de ir ganando la confianza de la víctima.

- En las redes sociales evite dar clic en los enlaces, lo puede dirigir a sitios de descarga de aplicaciones con código malicioso que puede obtener información del visitante y del equipo que se usa.

- Evite seguir notificaciones o enlaces vía mensajes de texto, correo electrónico relacionados a su perfil de cuenta, puede ser un engaño para obtener las credenciales de acceso a las cuentas.

5.4.2.2 Usando redes WiFi y Bluetooth

- No se conecte a redes públicas, un atacante puede haber suplantado la red inalámbrica para obtener las contraseñas de acceso.

- No permita que su dispositivo móvil se una automáticamente a una red desconocida, sí sale de casa desactive la red WiFi, si no la va a usar.

- No envié información confidencial o sensible a través de la red WiFi, sin asegurarse que se encuentra conectado a una red segura.

- Apagar o desactivar el bluetooth cuando no se encuentre en uso, deshabilitar el modo de emparejamiento automático.

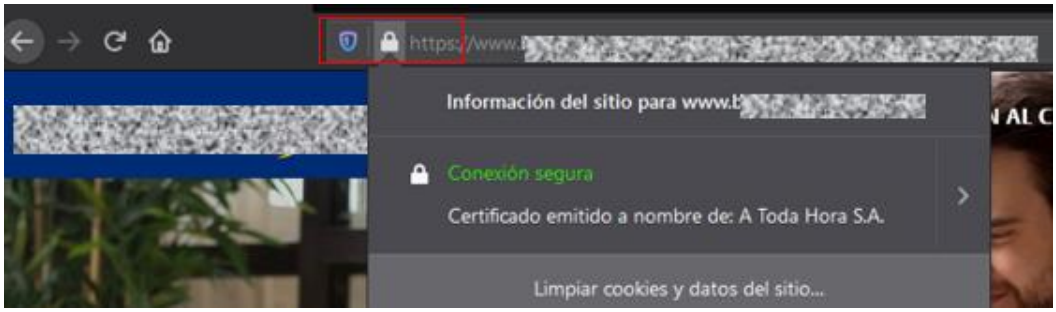
5.4.2.3 Usando el navegador Web

- Prestar atención y cuidado de los anuncios, concursos y sorteos que aparecen en el navegador, generalmente conducen a sitios falsos que parecen ser los originales.

- Al realizar pagos en línea verificar que el sitio Web sea seguro (Revisando y comprobando la barra de URL, el candado y el inicio de la URL debe iniciar

con HTTPS) como se muestra en la figura 7, y realizarlo a través de la red móvil en lugar de la red WiFi.

Figura 7. Verificación de candado, URL y protocolo HTTPS



Fuente: El autor

- Verificar las URL en los navegadores tanto en dispositivos móviles como equipos de cómputo, permite identificar el sitio al cual estamos accediendo, verificar el estado de nuestro navegador puede advertir al ingresar a un sitio, asegúrese de verificar el sitio al cual va a ingresar.

- No almacene los inicios de sesión y contraseñas en los navegadores Web.

5.4.2.4 Interactuando con aplicaciones

- Solo use las aplicaciones que se encuentran disponibles en la tienda oficial del dispositivo, no las descargue desde un navegador Web, sí las aplicaciones no se encuentran en la tienda desinstálelas.

- Siempre desconfíe de las aplicaciones desarrolladas por desconocidos o terceros.

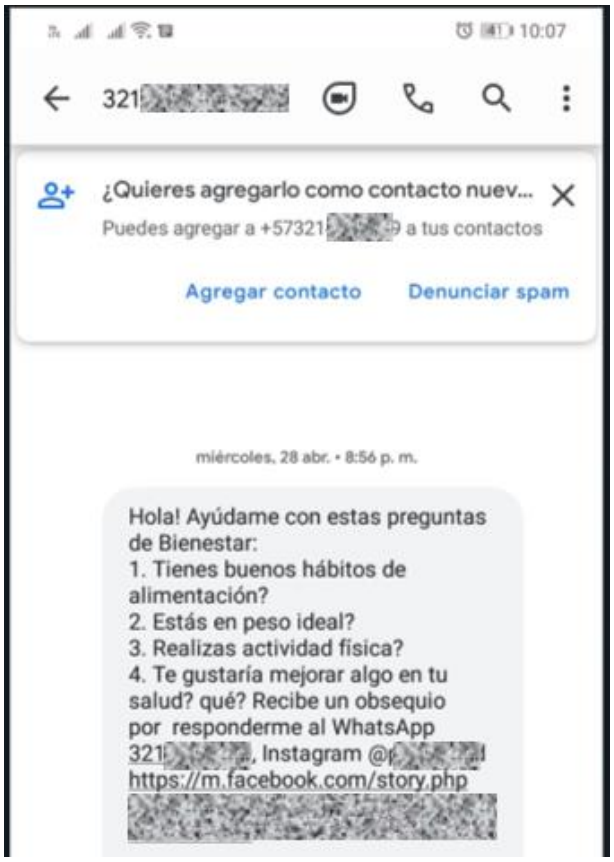
- Asegúrese de conceder o denegar los permisos mínimos a las aplicaciones, a menos que confíe en la aplicación.

5.4.2.5 Al recibir SMS o mensajes de texto

- Tener cuidado con los mensajes de texto que reciba ya que intentan que el usuario revele información.

- Desconfíe de los mensajes que llegan con enlaces de redes sociales, pueden dirigirlo a un sitio Web malicioso, en la figura 8, se muestra el interés de un usuario para recolectar información a través de un mensaje de texto, que redirige a un sitio de una red social.

Figura 8. Mensaje de texto que redirige a red social



Fuente: El autor

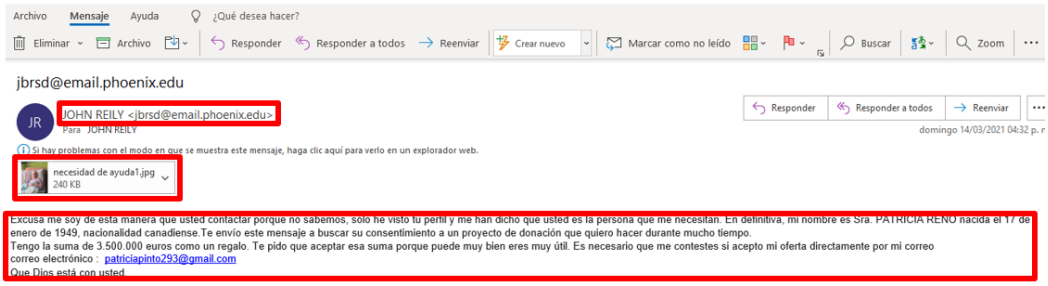
- Antes de dar clic en el enlace del mensaje trátelo como si fuera un correo electrónico.

5.4.2.6 En los correos electrónicos

- Verifique que el remitente no venga con un dominio extraño, generalmente el dominio identifica a una empresa, validar el usuario del correo.

- No dar clic en los enlaces o adjuntos que lleguen en los correos de origen desconocido, estos pueden llegar con un idioma diferente al nuestro, puede contener errores de ortografía o logotipos con errores, historias incoherentes y pretextos. En la figura 9, se muestra como un atacante trata de llamar la atención de la víctima a través de un señuelo al ofrecerle dinero como obsequio, adicionalmente adjunta una imagen que al ser descargada o abierta puede capturar los datos de la víctima.

Figura 9. Correo malicioso



Fuente: El autor

- Tener en cuenta que las entidades bancarias no piden información confidencial a través de cuentas de correo electrónico o teléfono.

5.4.2.7 Recibiendo llamadas telefónicas

- No responder a las solicitudes de información personal de entidades financieras por teléfono, para verificar puede comunicarse con la línea de su entidad financiera para corroborar la información.

- No suministre información de sus tarjetas de crédito, código de seguridad (CVV), fechas de vencimiento o clave secreta (PIN).

Con el seguimiento de las sugerencias anteriormente descritas es posible minimizar el riesgo de los ataques de ingeniería social a las infraestructuras de las organizaciones y a las personas, la seguridad debe ser un compromiso de todos los individuos y debe estar acompañado de capacitaciones constantes que le permitan a las personas estar actualizadas en temas de seguridad, teniendo en cuenta que también lo hacen los ciberdelincuentes.

6 CONCLUSIONES

A partir del estudio realizado se puede concluir la falta de concientización y sensibilización de los usuarios frente a la información expuesta en internet que puede ser usada por los ingenieros sociales al momento de usar ataques de ingeniería social, una de las técnicas favoritas de los ciberdelincuentes es hacer uso del Phishing ya que pueden llegar a un sinfín de usuarios manipulando los sentimientos de las personas, adicionalmente el atacante puede lanzar un ataque dirigido a un usuario u organización en especifico recopilando solo los datos de interés.

Se hace evidente que, a través de herramientas de inteligencia de fuentes abiertas, un atacante puede perfilar un objetivo en específico y lanzar un ataque de ingeniería social, el desconocimiento de los usuarios al momento de realizar publicaciones en fuentes públicas crea falencias en la seguridad de las personas y empresas, se logra evidenciar que no son conscientes de en donde se encuentra la información.

A partir del uso de herramientas OSINT, las empresas colombianas pueden identificar falencias en la seguridad de equipos y personas, claro está, que debe llevarse a cabo por el personal de seguridad, pues depende de ellos minimizar las vulnerabilidades halladas, previniendo los ataques de ingeniería social a través de capacitaciones al personal sobre el uso de las tecnologías de la información y las telecomunicaciones, la sensibilización y concientización al momento de exponer información en internet.

Mediante las herramientas de OSINT, se logró visualizar el tipo de información que puede ser obtenida de fuentes públicas y puede ser usada por un ciberatacante con cualquiera de las técnicas o ataques de ingeniería social, pues sin la debida concientización, instrucción y capacitación de las personas se seguirá encontrando

más información en internet, haciéndose un mundo propicio de información para los ciberdelincuentes.

Mediante la guía se presentan diferentes sugerencias de seguridad para ser tenidas en cuenta por las empresas y usuarios colombianos, la aplicación de la guía permite prevenir la exposición de información sensible en fuentes públicas y fortalecer la seguridad personal y de la organización.

7 RECOMENDACIONES

De acuerdo con los resultados obtenidos, se logró evidenciar que las herramientas para la recolección de información en fuentes públicas permite ver en donde se encuentran falencias en la seguridad, no solo de personas sino en empresas y que con el uso de estas se puede minimizar frente a los ataques de ingeniería social, claro está que es indispensable que las personas se concienticen y sensibilicen en donde dejan la información, pues se puede contar con los últimos equipos de tecnología en seguridad, las mejores prácticas, políticas y procedimientos pero si los empleados no se comprometen se seguirán viendo vulnerabilidades que pueden terminar siendo explotadas por los ciberdelincuentes.

Prestar atención a cualquier tipo de solicitud, notificación, mensaje de texto, correo electrónico o cualquier tipo de información que llegue a los sistemas de información que se usa a diario ya que a través de estos se puede estar entregando información maliciosa que pueda terminar en manos de un delincuente cibernético, la concientización hacia las personas sobre el uso de la información y su exposición debe hacerse periódicamente ya que los ataques cada vez son más elaborados que le permita a los usuarios estar actualizados en materia de seguridad sin que la información pueda terminar en manos no deseadas.

Seguir el documento guía, les permite a las organizaciones colombianas fortalecer su perímetro de seguridad no solo enfocado a las empresas sino a su personal, las sugerencias están dadas para que los usuarios y empresas se concienticen y sensibilicen sobre el uso adecuado de las tecnologías de la información y las telecomunicaciones frente a la exposición de la información en fuentes públicas.

Reportar ante las entidades oficiales cualquier actividad o ataque de ingeniería social sospechosa que pueda poner en riesgo la seguridad personal o de la organización; se puede realizar a través de los siguientes enlaces:

http://www.colcert.gov.co/?q=contenido/denunciar-ciberdelitos y https://caivirtual.policia.gov.co/.

8 BIBLIOGRAFÍA

ALIPRANDI, Carlo; DE LUCA, Antonio; DI PIETRO, Giulia; RAFFAELLI, Matteo; GAZZÉ, Davide. CAPER: Crawling and analysing Facebook for intelligence purposes. International Conference on Advances in Social Networks Analysis and Mining. [en línea]. 2014, Aug, 665-669. [Consultado 20 de noviembre 2020]. ISBN:978-1-4799-5877-1. DOI: 10.1109/ASONAM.2014.6921656

BANCO INTERAMERICANO DE DESARROLLO. Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Organización de los Estados Americanos. [en línea]. Jul 2020. [Consultado 20 de noviembre 2020]. DOI: http://dx.doi.org/10.18235/0002513

BEST, Clive. OSINT, the Internet and Privacy. 2012 European Intelligence and Security Informatics Conference. [en línea]. 2012, Aug. [Consultado 20 de noviembre 2020]. ISBN:978-1-4673-2358-1. DOI: 10.1109/EISIC.2012.71

BUTLER, Blake; WARDMAN, Brad; PRATT, Nate. REAPER: An automated, scalable solution for mass credential harvesting and OSINT. 2016 APWG Symposium on Electronic Crime Research (eCrime). [en línea]. June 2016 [Consultado 20 de noviembre 2020]. ISSN: 2159-1245. DOI: 10.1109/ECRIME.2016.7487944

CENTRO CIBERNÉTICO POLICIAL DE COLOMBIA. [Sitio web]. Bogotá: caivirtual, Balance cibercrimen 2020 semana 45. [Consulta: 20 de febrero 2020], Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO. [en línea]. Instituto Español de Estudios Estratégicos; Instituto Universitario General Gutiérrez Mellado, 2011-. [Fecha de consulta: 20 de noviembre 2020]. Disponible en: https://publicaciones.defensa.gob.es/ciberseguridad-retos-y-amenazas-a-la-seguridad-nacional-en-el-ciberespacio.html

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273. (2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá DC. El ministerio.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1341. (30, julio, 2009). Por la cual se definen principios y

conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. En: Diario Oficial. Julio, 2009. Nro.47.426

DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA. [Sitio web]. LEY 1928 DEL 24 DE JULIO DE 2018. [Consulta: 29 de noviembre de 2020] Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

DW. [Sitio web]. Seis ataques cibernéticos que sacudieron el mundo. [Consulta: 29 de noviembre de 2020], Disponible en: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

FAIRCOMPANIES. [Sitio web]. OSINT: El periodismo de investigación en la era del big data. [Consulta: 10 de diciembre de 2019], Disponible en: https://faircompanies.com/articles/osint-el-periodismo-de-investigacion-en-la-era-del-big-data/

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. [Sitio web]. España: GESI. Inteligencia de fuentes abiertas (OSINT): Características, debilidades y engaño. [Consulta: 28 de noviembre de 2019], Disponible en: http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. España: INCIBE-CERT. OSINT - La información es poder. [Consulta: 28 de noviembre de 2019], Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

INSTITUTO UNIVERSITARIO DE INVESTIGACIÓN SOBRE SEGURIDAD INTERIOR. [Sitio web]. España: IUISI, Las Redes Sociales como fuentes de información (OSINT). [Consulta: 02 de febrero 2020]. Disponible en: https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/5149.pdf

INTELTECHNIQUES. [Sitio web]. EE. UU, Open Source Intelligence Techniques. [Consulta: 11 de diciembre 2020] Disponible en: https://inteltechniques.com/book1.html

LA INFORMACIÓN SOBRE SEGURIDAD Y DEFENSA EN FUENTES ABIERTAS. [en línea]. Universidad de La Rioja, España. [Fecha de consulta: 7 de diciembre de 2019]. Disponible en: Https://dialnet.unirioja.es/descarga/articulo/4199026

LEE, Seokcheol y SHON, Taeshik. Open source intelligence base cyber threat inspection framework for critical infrastructures. IEEE: *Institute of Electrical and Electronics Engineers* [en línea]. San Francisco, CA, USA, 6-7 Dec. 2016,

[Consultado 28 de noviembre 2020]. ISBN:978-1-5090-4172-5. Disponible en: https://ieeexplore.ieee.org/document/7821730

Maltego CE. [Sitio web]. MALTEGO TECHNOLOGIES. [Consulta: 28 de noviembre de 2019], Disponible en: https://www.paterva.com/buy/maltego-clients/maltego-ce.php

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. [Sitio web]. Bogotá: MINTIC, Hacia la construcción de una estrategia de social media para la ciudadanía 2.0. [Consulta: 29 de noviembre 2019]. Disponible en: https://estrategia.gobiernoenlinea.gov.co/623/articles-8248_recurso_3.pdf

PINTO RICO, Ricardo; HERNÁNDEZ, Jose; PINZÓN, Cristian Camilo; DÍAZ, Daniel Orlando y GARCÍA, Juan Carlos. “Inteligencia de fuentes abiertas (OSINT) para operaciones de ciberseguridad. “Aplicación de OSINT en un contexto colombiano y análisis de sentimientos””. Revista Vínculos: Ciencia, Tecnología y Sociedad, vol 15, n° 2, julio-diciembre 2018,195-214. DOI: https://doi.org/10.14483/2322939X.13504.

SOPHOS. [Sitio web]. Results of an independent survey of 3,100 IT managers commissioned by Sophos. [Consulta: 29 de noviembre de 2020], Disponible en: https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. Bogotá: SIC. Protección de Datos Personales. [Consulta: 11 de diciembre de 2019], Disponible en: https://www.sic.gov.co/registro-nacional-de-bases-de-datos

TheHarvester. [Sitio web]. Penetration Testing Tools, theharvester Package Description. [Consulta: 28 de noviembre de 2019], Disponible en: https://tools.kali.org/information-gathering/theharvester

VISUAL CAPITALIST. [Sitio web]. The Rise and Fall of Social Media Platforms. [Consulta: 17 de octubre de 2019], de Visual Capitalist website: Disponible en: https://www.visualcapitalist.com/rise-and-fall-of-social-media-platforms/

Fecha de Realización:	07/04/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN DE FUENTES PÚBLICAS, USADAS PARA PREVENIR ATAQUES DE INGENIERÍA SOCIAL EN PERSONAS Y ORGANIZACIONES EN EL CONTEXTO COLOMBIANO
Autor(es):	Alvarado Murcia John Jairo
Palabras Claves:	Open Source Intellingence, Ingeniería social, Cyberdelincuentes, Redes sociales, Ataque, Seguridad
Descripción:	En este documento encontrará información importante referente a la ciberseguridad en temas como la ingeniería social, las diferentes herramientas que son usadas para la recolección de información y la forma en que los atacantes pueden hacer uso de los datos que hacen públicos en internet, también podrán visualizar el aumento de los ataques no solo a nivel Latinoamérica sino a nivel Colombia. Se espera que esta monografía sirva de soporte, sensibilización y concientización a usuarios y empresas colombianas frente al uso y manejo de la información que es expuesta en internet, aclarando el panorama de como los atacantes usan la información pública para buscar brechas de seguridad y perfilar los ataques a un objetivo en común, pero la intensión no solo es mostrar lo que los atacantes pueden hacer sino en que también las empresas lo puedan hacer con sus equipos de ingenieros de seguridad buscando las brechas, minimizarlas o eliminarlas, el uso de las herramientas OSINT permite encontrar toda la información que se encuentre pública y endurecer o fortalecer el perímetro a través de políticas de seguridad. Adicionalmente la sensibilización y la concientización del manejo de los datos a las

	personas se debe hacer constantemente entendiendo que el eslabón más débil de la cadena es el usuario y de aquí dependen todas las acciones y políticas que se establecen en las organizaciones para la mitigación de incidentes o riesgos a que se puedan estar expuestas.

ALIPRANDI, Carlo; DE LUCA, Antonio; DI PIETRO, Giulia; RAFFAELLI, Matteo; GAZZÉ, Davide. CAPER: Crawling and analysing Facebook for intelligence purposes. International Conference on Advances in Social Networks Analysis and Mining. [en línea]. 2014, Aug, 665-669. [Consultado 20 de noviembre 2020]. ISBN:978-1-4799-5877-1. DOI: 10.1109/ASONAM.2014.6921656

BANCO INTERAMERICANO DE DESARROLLO. Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Organización de los Estados Americanos. [en línea]. Jul 2020. [Consultado 20 de noviembre 2020]. DOI: http://dx.doi.org/10.18235/0002513

BEST, Clive. OSINT, the Internet and Privacy. 2012 European Intelligence and Security Informatics Conference. [en línea]. 2012, Aug. [Consultado 20 de noviembre 2020]. ISBN:978-1-4673-2358-1. DOI: 10.1109/EISIC.2012.71

BUTLER, Blake; WARDMAN, Brad; PRATT, Nate. REAPER: An automated, scalable solution for mass credential harvesting and OSINT. 2016 APWG Symposium on Electronic Crime Research (eCrime). [en línea]. June 2016 [Consultado 20 de noviembre 2020]. ISSN: 2159-1245. DOI: 10.1109/ECRIME.2016.7487944

CENTRO CIBERNÉTICO POLICIAL DE COLOMBIA. [Sitio web]. Bogotá: caivirtual, Balance cibercrimen 2020 semana 45. [Consulta: 20 de febrero 2020], Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO. [en línea]. Instituto Español de Estudios Estratégicos; Instituto Universitario General Gutiérrez Mellado, 2011-. [Fecha de consulta: 20 de noviembre 2020]. Disponible en: https://publicaciones.defensa.gob.es/ciberseguridad-retos-y-amenazas-a-la-seguridad-nacional-en-el-ciberespacio.html

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. [Sitio web]. España: GESI. Inteligencia de fuentes abiertas (OSINT): Características, debilidades y engaño. [Consulta: 28 de noviembre de 2019], Disponible en: http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. España: INCIBE-CERT. OSINT - La información es poder. [Consulta: 28 de noviembre de 2019], Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

INSTITUTO UNIVERSITARIO DE INVESTIGACIÓN SOBRE SEGURIDAD INTERIOR. [Sitio web]. España: IUISI, Las Redes Sociales como fuentes de información (OSINT). [Consulta: 02 de febrero 2020]. Disponible en: https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/5149.pdf

LA INFORMACIÓN SOBRE SEGURIDAD Y DEFENSA EN FUENTES ABIERTAS. [en línea]. Universidad de La Rioja, España. [Fecha de consulta: 7 de diciembre de 2019]. Disponible en: Https://dialnet.unirioja.es/descarga/articulo/4199026

LEE, Seokcheol y SHON, Taeshik. Open source intelligence base cyber threat inspection framework for critical infrastructures. IEEE: *Institute of Electrical and Electronics Engineers* [en línea]. San Francisco, CA, USA, 6-7 Dec. 2016, [Consultado 28 de noviembre 2020]. ISBN:978-1-5090-4172-5. Disponible en: https://ieeexplore.ieee.org/document/7821730

PINTO RICO, Ricardo; HERNÁNDEZ, Jose; PINZÓN, Cristian Camilo; DÍAZ, Daniel Orlando y GARCÍA, Juan Carlos. “Inteligencia de fuentes abiertas (OSINT) para operaciones de ciberseguridad. “Aplicación de OSINT en un contexto colombiano y análisis de sentimientos””. Revista Vínculos: Ciencia, Tecnología y Sociedad, vol 15, n° 2, julio-diciembre 2018,195-214. DOI: https://doi.org/10.14483/2322939X.13504.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. Bogotá: SIC. Protección de Datos Personales. [Consulta: 11 de diciembre de 2019], Disponible en: https://www.sic.gov.co/registro-nacional-de-bases-de-datos
TheHarvester. [Sitio web]. Penetration Testing Tools, theharvester Package Description. [Consulta: 28 de noviembre de 2019], Disponible en: https://tools.kali.org/information-gathering/theharvester

Contenido del documento:	La presente monografía contiene cuatro objetivos dentro de los cuales se desarrolla la explicación de las herramientas OSINT usadas para prevenir ataques de ingeniería social en personas y organizaciones en el contexto colombiano. Objetivo 1: Seleccionar a partir de conceptos básicos de ingeniería social, ataques que se realizan a través del uso de herramientas de inteligencia de fuentes públicas. Objetivo 2: Compilar las diferentes herramientas usadas para la recolección de información de fuentes públicas. Objetivo 3: Identificar el tipo de información obtenida de fuentes públicas que puede ser usada por un atacante. Objetivo 4: Elaborar un documento guía de referente informativo para las empresas colombianas que permita ayudar a prevenir la exposición de información sensible en fuentes públicas.
Conceptos adquiridos:	A través del desarrollo de la monografía se logró profundizar en los conceptos de ingeniería social y del uso de herramientas de recolección de información en fuentes públicas; estableciendo una guía para tener en cuenta por las personas y organizaciones para el endurecimiento de su seguridad. Adicionalmente se logró evidenciar que el OSINT no solo es usado por los ciberdelincuentes para obtener información, sino que es usado por periodistas, investigadores, países, grupos de hacker, ciberterroristas, Pentesting o ingenieros de hacking ético, pero el desconocimiento de estas herramientas hace que los países, empresas y personas no tomen en serio la seguridad al exponer datos sensibles en internet.
Conclusiones:	A partir del estudio realizado se puede concluir la falta de concientización y sensibilización de los usuarios frente a la

	información expuesta en internet que puede ser usada por los ingenieros sociales al momento de usar ataques de ingeniería social, una de las técnicas favoritas de los ciberdelincuentes es hacer uso del Phishing ya que pueden llegar a un sinfín de usuarios manipulando los sentimientos de las personas, adicionalmente el atacante puede lanzar un ataque dirigido a un usuario u organización en específico recopilando solo los datos de interés. Se hace evidente que, a través de herramientas de inteligencia de fuentes abiertas, un atacante puede perfilar un objetivo en específico y lanzar un ataque de ingeniería social, el desconocimiento de los usuarios al momento de realizar publicaciones en fuentes públicas crea falencias en la seguridad de las personas y empresas, se logra evidenciar que no son conscientes de en donde se encuentra la información. A partir del uso de herramientas OSINT, las empresas colombianas pueden identificar falencias en la seguridad de equipos y personas, claro está, que debe llevarse a cabo por el personal de seguridad, pues depende de ellos minimizar las vulnerabilidades halladas, previniendo los ataques de ingeniería social a través de capacitaciones al personal sobre el uso de las tecnologías de la información y las telecomunicaciones, la sensibilización y concientización al momento de exponer información en internet. Mediante las herramientas de OSINT, se logró visualizar el tipo de información que puede ser obtenida de fuentes públicas y puede ser usada por un ciberatacante con cualquiera de las técnicas o ataques de ingeniería social, pues sin la debida

	concientización, instrucción y capacitación de las personas se seguirá encontrando más información en internet, haciéndose un mundo propicio de información para los ciberdelincuentes. Mediante la guía se presentan diferentes sugerencias de seguridad para ser tenidas en cuenta por las empresas y usuarios colombianos, la aplicación de la guía permite prevenir la exposición de información sensible en fuentes públicas y fortalecer la seguridad personal y de la organización.