
# UNIVERSIDAD DE CUENCA

## FACULTAD DE INGENIERÍA

MAESTRÍA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

# "PROPUESTA METODOLÓGICA PARA LA EVALUACIÓN DE SEGURIDAD DE USUARIOS DE REDES SOCIALES CON RELACIÓN A ATAQUES DE INGENIERÍA SOCIAL"

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

**AUTOR:**

ING. LENIN MAURICIO MONTENEGRO GALLEGOS.
CI: 0104481932

**DIRECTORA:**

ING. IRENE PRISCILA CEDILLO ORELLANA, PHD.
CI: 0102815842

CUENCA – ECUADOR

2017

## Resumen

El amplio uso de las redes sociales expone a sus usuarios a problemas de seguridad provenientes de la información que éstos publican y comparten con estas redes; convirtiéndolos en blanco fácil de vulneraciones a su privacidad hasta de ataques de ingeniería social. Si bien existe mucha investigación que permite determinar las vulnerabilidades de seguridad en este tipo de aplicaciones, poco se ha abordado el tema de la Ingeniería Social y la concientización hacia la exposición de datos personales del usuario de estas aplicaciones.

En el presente trabajo, se provee un modelo que permite analizar las acciones de un usuario en la red social. Estas acciones del usuario pondrían en riesgo su seguridad y la de una organización, ya que permitiría la consecución de posibles ataques mediante técnicas de ingeniería social. Con el fin de verificar la factibilidad del modelo, se ha aplicado en un caso de estudio, realizando verificaciones de las acciones en perfiles de usuarios pertenecientes a una organización.

Para apoyar el modelo, se propone una metodología de evaluación de la seguridad de usuarios de redes sociales, enfocado a corregir inconvenientes encontrados.

Los resultados muestran que la propuesta permite reducir el riesgo de los usuarios y la organización ante ataques de ingeniería social.

**Palabras Clave**: INGENIERÍA SOCIAL, REDES SOCIALES, SEGURIDAD DE LA INFORMACIÓN.

## Abstract

Network services on the Internet allow people to communicate through different types of interactions among individuals or organizations. Such interactions have permitted several social networks to increase their number of users continually to reach the point that most of the people have a profile on at least one of them. This wide use tent to cause security problems among users, which arise from the information they publish and share with the help of these networks, making them easy targets for breaches of privacy and social engineering attacks. Although there is a lot of research that help determine security vulnerabilities in these types of applications, little has been discussed about the topic of Social Engineering and the awareness towards the exposition of user personal data of these applications.

This work presents a model that allows analysis of actions of a user on a social network. The actions of a user can put at risk not only their but also an organization security since this may allow the accomplishment of possible attacks using techniques of social engineering. In order to verify the feasibility of the model, a case study has been applied, carrying out verifications of the actions in user profiles that belong to an organization.

To support the model, a methodology of evaluation of the security of users on social networks has been proposed, focused on correcting problems encountered.

The results have shown that the proposal allows to reduce the risk of users as well as the organization attacks of social engineering.

**Keywords**: SOCIAL ENGINEERING, SOCIAL NETWORKS, INFORMATION SECURITY

# Índice:

# Índice de Tablas

# Índice de Figuras

Universidad de Cuenca
Cláusula de Propiedad Intelectual

Lenin Mauricio Montenegro Gallegos, autor de la Tesis, **"Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social"**, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 27 de noviembre de 2017

Lenin Mauricio Montenegro Gallegos

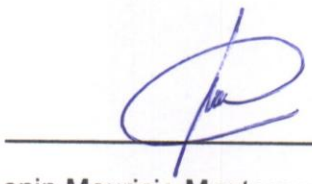
CI: 0104481932

Universidad de Cuenca
Cláusula de Licencia y Autorización para Publicación en el Repositorio Institucional

Lenin Mauricio Montenegro Gallegos, en calidad de autor y titular de los derechos morales y patrimoniales de la Tesis, **"Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social"**, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el Repositorio Institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 27 de noviembre de 2017



Lenin Mauricio Montenegro Gallegos

CI: 0104481932

# Agradecimientos

A Dios, por brindarme las habilidades y destrezas que permitieron que comparta mis conocimientos y experiencia adquirida en los días que Él me ha brindado.

A mi Directora, Priscila, por el tiempo brindado, apoyo a este proyecto y aporte significativo en la conclusión de este trabajo.

A mi Familia, por ser mi comprensión, apoyo y aliento constante, por las malas noches, por las ausencias y por la paciencia.

A mis Jefes y compañeros de trabajo, por permitirme aplicar mis conocimientos que permitieron la elaboración de este trabajo de titulación.

A mis Compañeros del programa de maestría, quienes me han apoyado a continuar con el proceso y por todas las experiencias de profesionalización.

# Dedicatoria

*a Pawa y Jere*

# Capítulo 1. Introducción

## 1.1 Motivación

En los últimos años, organizaciones y personas se han visto perjudicadas por el aumento significativo de ataques informáticos, en donde las distintas estrategias, soluciones y herramientas de protección no han logrado ser barreras suficientes que mitiguen de manera efectiva los múltiples tipos de ataques existentes en la actualidad; perdiendo así, grandes volúmenes de información o en ocasiones, pagando un rescate por la misma.

Además, con la implementación de hardware y software de protección, los ingenieros especialistas en seguridad de la información, han integrado las recomendaciones aceptadas a nivel internacional por estándares tales como la ISO 27001 (Servicio Ecuatoriano de Normalización INEN, 2016) en pro de garantizar la disponibilidad, integridad y confidencialidad de la información de una organización.

Por otra parte, dentro de la sociología, se denomina redes sociales a los conjuntos de individuos que laboran conjuntamente en una organización, forman equipos de trabajo, pertenecen a colegios de profesionales y participan de congresos o charlas relacionadas a sus ámbitos de especialización, como éstas, y otras muchas maneras, forman grupos colaborativos o sociales entre sí (Backstrom, Huttenlocher, Kleinberg, & Lan, 2006). En consecuencia, las redes sociales constituyen una estructura social compuesta por un conjunto de actores que interactúan entre sí; éstas han sido por siempre una manera efectiva de socializar y relacionarse entre profesionales, parientes, etc. De ahí, y con el advenimiento tecnológico, se han creado las redes sociales digitales basadas en Internet. El número de usuarios de redes sociales desplegados en Internet a nivel mundial ha aumentado desde el año 2010 de un promedio de 0.97 mil millones de usuarios activos hasta el año 2017 con 2.51 mil millones de usuarios activos y se pronostica para el año 2020 contar con 2.95 mil millones de usuarios activos (eMarketer, 2017), lo que sugiere que estas plataformas de comunicación en línea han tenido gran acogida y sigue aumentando su demanda. Estas redes sociales, brindan a sus usuarios la posibilidad de tener un perfil para interactuar con su círculo social; sin embargo, éstas también abren la puerta a extraños e incluso a personas no confiables y que pueden constituir un riesgo en la seguridad del individuo; dado que ellas posibilitan la compartición de datos personales e información sensible, convirtiéndose en un blanco

fácil de posibles atacantes y ciber-delincuentes. Si bien las redes sociales online han causado efectos positivos para personas e inclusive para organizaciones, su uso también puede abrir las puertas a riesgos que resultan preocupantes.

Por otra parte, el acceso a las redes sociales al ser multi-plataforma y multi-dispositivo, aumenta los posibles riesgos de seguridad hacia un usuario (Zhang, 2010) (Almorsy, Grundy, & Müller, 2016) a diferencia de un servicio fabricado a medida, lo que convierte a estos servicios en una fuente muy valiosa de información dentro de la planeación de un ataque de Ingeniería Social (Jaafor & Birregah Babiga, 2015). Estos riesgos aumentan, cuando el usuario hace caso omiso de las opciones de seguridad establecidas como predeterminadas o configurables por parte de las redes sociales o cuando el usuario publica información que pueda proporcionar datos para un posible ataque. En Ecuador, el uso de Internet y de teléfonos inteligentes ha aumentado en un 20% en los últimos 5 años, actualmente más de 4.2 millones de habitantes utilizan redes sociales online (Instituto Nacional de Estadísticas y Censos, 2017), cifras que han ido aumentando con un crecimiento exponencial. Las tácticas de ataques mediante ingeniería social han tomado fuerza, gracias a las redes sociales, incluso han sido consideradas de mayor importancia y amplitud que ataques sofisticados como los de día cero, según el propio Alex Stamos (Stamos, 2017), jefe de seguridad de Facebook; esto, sumado al creciente uso de las redes sociales, aumenta el riesgo de que una persona u organización sea víctima de malware.

## 1.2 Problemática y Justificación

Para un atacante a través de ingeniería social, los ataques dirigidos hacia personas o hacia compañías que antes veían un perfil de una red social como objetivo, hoy lo ven como el medio tanto para obtener información (F-Secure, 2017) como para introducir malware en computadores o teléfonos (McAffe Labs, 2016). Aunque la educación en ciberseguridad sigue siendo una responsabilidad social (ESET, 2017), no es de extrañarse que usuarios experimentados sean víctimas de este tipo de ataques (Symantec, 2017) y pongan en riesgo tanto su información personal como laboral.

Al no existir un estándar, marco de trabajo o modelo de validación en el que se especifiquen herramientas de análisis de seguridad o metodologías que valoren el nivel de riesgo de la seguridad en redes sociales en el ámbito local, en este trabajo de investigación se pretende elaborar una metodología para la evaluación de seguridad de

usuarios de redes sociales contra ataques de ingeniería social, mediante un análisis profundo apoyado en un modelo propio de seguridad según informes y tendencias actuales de seguridad. Al finalizar este trabajo de investigación de actualidad se pretende aportar significativamente a la evaluación y mejora de seguridad de usuarios de redes sociales contra ataques o posibles vulnerabilidades de ingeniería social.

## 1.3 Objetivos

El principal objetivo de este trabajo es elaborar una metodología para evaluar la seguridad de usuarios en redes sociales contra ataques de ingeniería social.

Se definen los siguientes objetivos específicos:

- Analizar las distintas brechas de seguridad que pueden ser atacadas por medio de la ingeniería social y que se puedan relacionar con las redes sociales.
- Entender las herramientas y alternativas propuestas por las redes sociales digitales para mitigar riesgos relacionados a ataques de ingeniería social.
- Elaborar un modelo de ataque de ingeniería social a un perfil en una red social.
- Realizar un caso de estudio en una organización pública, en donde se verificará el modelo y la metodología a evaluar, analizando sus cuentas de redes sociales.
- Evaluar la metodología propuesta en distintos perfiles de redes sociales para verificar su validez y exponer sus resultados.

## 1.4 Tareas de Investigación:

Se especifican los siguientes pasos para llevar a cabo la presente investigación:

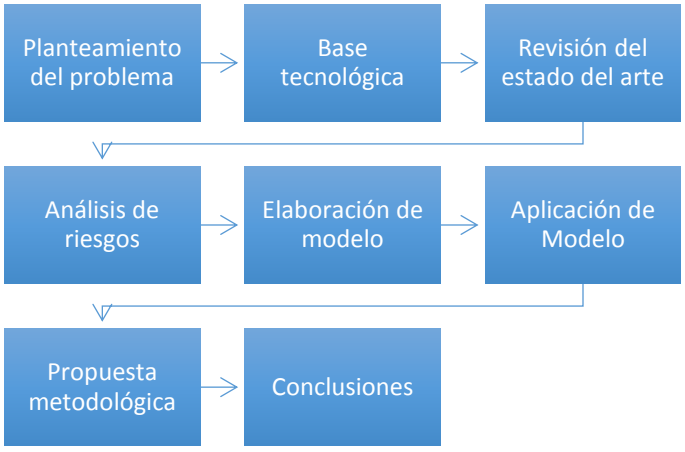



*Figura 1-1. Metodología de investigación utilizada*

- Planteamiento del problema: Se delimita el alcance del modelo y de los perfiles de redes sociales.
- Base tecnológica: Se especifican y detallan los conceptos necesarios que se utilizarán en el modelo y metodología.
- Revisión del estado del arte: Se revisan distintos modelos de ingeniería social para definir los pasos para un modelo enfocado a redes sociales.
- Análisis de riesgos: Contempla los riesgos a los que estaría expuesto un perfil de una red social y los tomados en cuenta por estándares.
- Elaboración de modelo: Se elabora un modelo de ataque de ingeniería social a perfiles de usuarios de redes sociales.
- Aplicación del modelo: se ejecuta un caso de estudio y se analizan los resultados.
- Propuesta metodológica: se elabora una metodología para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social.
- Conclusiones: se obtienen los descubrimientos destacados y se definen políticas de uso de redes sociales en una organización.

## 1.5 Estructura del trabajo

El presente trabajo se compone de 6 capítulos, los cuales se estructuran de la siguiente manera:

El capítulo 1 presenta la introducción, alcance y procedimiento e introducción que se seguirá para el desarrollo del trabajo.

El capítulo 2 sienta los conceptos base y herramientas de software que serán requeridos para el desarrollo del trabajo y entendimiento de la temática.

El capítulo 3 presenta el estado del arte en cuanto a modelos de ingeniería social y hace un análisis de riesgos de la organización del caso de estudio a aplicar.

El capítulo 4 propone un modelo de ataque de ingeniería social a un perfil en una red social, basado en los conceptos base y estado del arte. En este capítulo el modelo se explica con la aplicación del caso de estudio y sus resultados ya que el nivel de detalle sólo se considera en la ejecución del caso de estudio por los resultados obtenidos en cada uno de los pasos del modelo planteado.

El capítulo 5 se basa en el modelo de ataque propuesto y sus resultados para elaborar un método de evaluación de la seguridad según el uso de una red social, se detalla con el caso de estudio.

Finalmente, el capítulo 6 concluye con resultados, y propuestas de trabajos futuros.

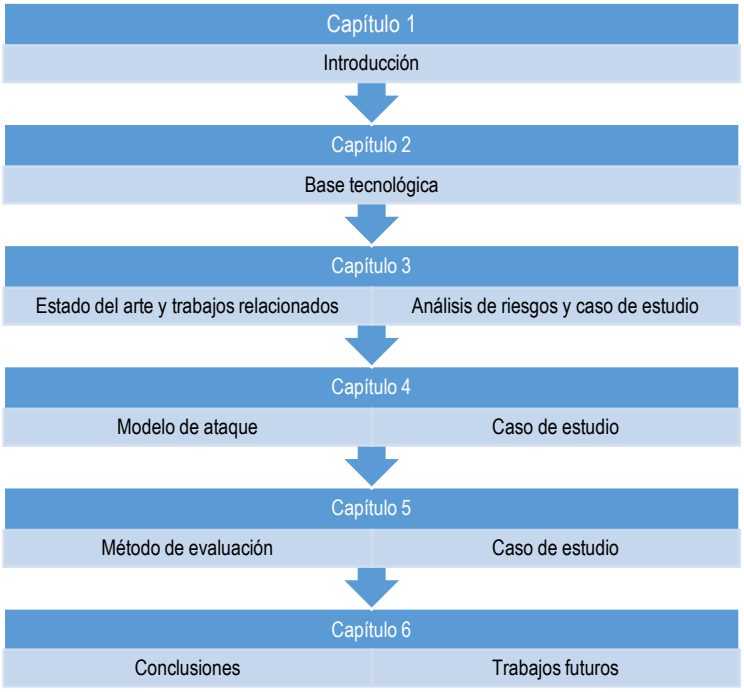



*Figura 1-2. Estructura del trabajo*

# Capítulo 2. Base Tecnológica

## 2.1 Definiciones

### 2.1.1 Seguridad de la Información

La Seguridad de la Información se refiere a las metodologías y procesos, diseñados e implementados para proteger la información en medios electrónicos, medios impresos o cualquier otra forma de datos, ya sea información sensible, privada o confidencial del acceso no autorizado, uso, revelación, destrucción, modificación o interrupción (SANS, 2016).

Un Sistema de Gestión de Seguridad de la Información (SGSI) preserva la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de un proceso de gestión del riesgo y brinda confianza acerca de la gestión adecuada de los riesgos (Servicio Ecuatoriano de Normalización INEN, 2016).

### 2.1.2 Hacker Ético

Hacker es uno de los términos más incomprendidos y más usados en seguridad, se define a un *hacker* como: “un experto en seguridad informática que usa sus conocimientos técnicos para superar un problema” (Oriyano, 2016).

La ética se define como: “el conjunto de creencias que tiene una sociedad sobre el conducirse de una buena o mala manera” (Reynolds, 2016). La conducta ética se conforma de las normas generalmente aceptadas, muchas de las cuales son casi universales (Reynolds, 2016). Las decisiones, elecciones y acciones (comportamientos) que hacemos, reflejan y promulgan nuestros valores (Ethics and Compliance Initiative).

El término *hacker* es usado con una connotación negativa, casi de manera generalizada, refiriéndose a alguien que logra vulnerar seguridades informáticas para robar información o causar daño. Es por ese motivo que se crea el concepto de *Hacker de Sombrero Blanco* (Rouse, 2007) o de Hacker ético, para referirse específicamente al experto informático que utiliza sus conocimientos con el fin de analizar para luego mitigar vulnerabilidades informáticas; normalmente es contratado por organizaciones para realizar evaluaciones de seguridad o pruebas de penetración (Oriyano, 2016).

### 2.1.3 Ingeniería Social

Es un término ampliamente usado en seguridad informática y se define como un conjunto de técnicas empleadas por ciberdelincuentes; las mismas que son diseñadas

para atraer usuarios desprevenidos con la finalidad de capturar datos confidenciales, infectar sus computadoras con malware o abrir enlaces a sitios infectados (Kaspersky Lab, 2017). Sin embargo, el fin no siempre es atraer usuarios, sino también producir interacciones humanas (habilidades sociales) con la finalidad de obtener o comprometer información sobre una persona, organización o sistema informático (US-CERT Publications, 2017).

La ingeniería social es considerada como uno de los pocos tipos de ataques informáticos no técnicos (examen de certificación de Hacker Ético de EC-Council v9). El tipo de ataque se basa en las debilidades o fortalezas de los seres humanos en lugar de la aplicación de la tecnología para la obtención de la información. Se ha demostrado que los seres humanos son manipulados muy fácilmente para proporcionar información u otros detalles que puedan ser útiles para un atacante (Oriyano, 2016).

Los sistemas de gestión de seguridad de la información que implementan políticas, protocolos y herramientas como antivirus o antimalware para prevenir y tratar de mitigar ataques digitales, no siempre pueden controlar las distintas acciones del lado del usuario (Akamai, 2017) (Cisco, 2017) (PwC, 2017) como visitar una página web, descargar archivos adjuntos en correos electrónicos o compartir información con terceros, es por ese motivo que los ingenieros sociales se enfocan en los hábitos y la naturaleza humana para hacer uso de sus habilidades y técnicas para obtener información valiosa dentro de su planeación o ataque.

Según Kevin Mitnick (Mitnick & Simon, 2002), hacker ético y experto en temas de ingeniería social, se define a la ingeniería social como un proceso cíclico, en donde se especifican cuatro procesos básicos:


*Figura 2-1. Ciclo de ingeniería social. (Mitnick & Simon, 2002).*

Mitnick creó el ciclo (Figura 2-1) con el fin de ilustrar patrones comunes de ataques de ingeniería social, estableciendo que los ataques de ingeniería social siempre tienen un objetivo claramente definido y los atacantes pasan por las diferentes etapas del ciclo hasta lograr su objetivo (Huber, Kowalski, Nohlberg, & Tjoa, 2009).

#### *2.1.3.1 Tipos*

Los ataques de ingeniería social más comunes son:

- *Baiting*: Cuando un atacante deja de manera arbitraria un dispositivo infectado con malware, como una memoria flash en un lugar donde pueda ser encontrado. La víctima que encuentra el dispositivo y lo conecta en su computador, instala involuntariamente el malware.
- *Phishing*: Correos electrónicos o comunicados falsos que pretenden suplantar la identidad de sitios confiables, logrando obtener información personal o proporcionar hiperenlaces que instalan malware.
- *Spear Phishing*: Es como el phishing pero enfocado en un individuo en específico o una organización determinada.
- *Pretexting*: El atacante finge ser la víctima para obtener acceso a más información personal o financiera de la misma para uso posterior.
- *Scareware*: Se pretende asustar a la víctima haciéndole pensar que su computador está infectado con malware y el atacante ofrece la solución que arreglaría el falso problema cuando en realidad la víctima se descarga e instala el malware del atacante.

Se podría decir que la ingeniería social es una ciencia ya que independientemente del campo se pueden encontrar sus usos en varias áreas (Hadnagy & Wilson, 2010).

### 2.1.4 Estándares de Seguridad de la Información

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), juntos desde 1987 participan en el desarrollo de normas internacionales por medio de comités técnicos (International Organization for Standardization, 2017) establecidos por varias organizaciones para colaborar en las actividades técnicas respectivas.

En Ecuador, el Servicio Ecuatoriano de Normalización (INEN) es el organismo técnico encargado de traducir y adaptar las normas internacionales e incluir las correcciones técnicas respectivas mediante comités técnicos de normalización, la mayoría de las veces, esta adaptación consiste únicamente en la traducción de la norma de su idioma original al español, este epígrafe se encuentra en cada una de las normas técnicas ecuatorianas (NTE) que dispone el INEN.

En la serie NTE INEN-ISO 27000, se aborda un gran número de estándares relacionados a Seguridad de la Información: gestión, controles, implementación, riesgos, auditoría, entre otros. Sin embargo, en los documentos ISO 27002 e ISO 27032 es en donde se abordan los temas relacionados a Ingeniería Social (Hinson, 2008) que son de interés de esta investigación.

#### *2.1.4.1 NTE INEN-ISO/IEC 27002:2017*

Se diseña esta norma nacional para que las organizaciones la usen como referencia al momento de seleccionar controles dentro del proceso de implementación de un SGSI basado en ISO/IEC 27001 o como documento guía para implementar controles de seguridad de la información o desarrollar directrices propias de gestión, teniendo en cuenta sus entornos específicos de riesgo de seguridad de la información (Servicio Ecuatoriano de Normalización INEN, 2017). La norma contiene 114 controles de seguridad, los controles necesarios para evitar ataques de Ingeniería Social son: seguridad en recursos humanos, control de acceso, seguridad física y del entorno y gestión de incidentes de seguridad de la información. Los controles a aplicar son:

| | | |
|---|---|---|
| **Seguridad en Recursos Humanos** | *Antes del empleo* | - Investigación de antecedentes<br>- Términos y condiciones del empleo |
| | *Durante el empleo* | - Responsabilidades de la dirección<br>- Concienciación, educación y formación en seguridad de la información<br>- Proceso disciplinario |
| | *Finalización o cambio de empleo* | - Responsabilidades ante la finalización o cambio de empleo |
| **Control de acceso** | *Requisitos de negocio para el control de acceso* | - Política de control de acceso<br>- Acceso a redes y servicios de red |
| | *Gestión de acceso de los usuarios* | - Registro y retiro de usuario<br>- Provisión de accesos a usuarios<br>- Gestión de privilegios de derechos de acceso<br>- Gestión de la información secreta de autenticación de los usuarios<br>- Revisión de los derechos de acceso de usuario<br>- Retiro y ajuste de los derechos de acceso. |
| | *Responsabilidades del usuario* | - Uso de la información secreta de autenticación |
| | *Control de acceso a sistemas y aplicaciones* | - Restricción del acceso a la información<br>- Procedimientos seguros de inicio de sesión<br>- Sistema de gestión de contraseñas<br>- Uso de programas utilitarios privilegiados<br>- Control de acceso al código fuente del programa |
| **Seguridad física y del entorno** | *Áreas seguras* | - Perímetro de seguridad física<br>- Controles físicos de entrada<br>- Seguridad de oficinas, despachos e instalaciones<br>- Protección contra las amenazas externas y ambientales<br>- Trabajo en áreas seguras<br>- Áreas de carga y entrega |
| | *Equipos* | - Ubicación y protección de equipos<br>- Instalaciones de suministro<br>- Seguridad del cableado<br>- Mantenimiento de los equipos<br>- Eliminación de activos |

| | | |
|---|---|---|
| | | - Seguridad de los equipos y activos fuera de las instalaciones<br>- Reutilización o eliminación segura de equipos<br>- Equipo de usuario desatendido<br>- Política de puesto de trabajo despejado y pantalla limpia |
| **Gestión de incidentes y mejoras** | *Gestión de incidentes de seguridad de la información* | - Responsabilidades y procedimientos<br>- Informe de los eventos de seguridad de la información<br>- Informe de debilidades de seguridad de la información<br>- Apreciación y decisión sobre los eventos de seguridad de la información<br>- Respuesta a incidentes de seguridad de la información<br>- Aprendizaje de los incidentes de seguridad de la información<br>- Recopilación de evidencias |

*Tabla 2-1. Controles de NTE INEN-ISO/IEC 27002:2017 para Ingeniería Social.*

#### *2.1.4.2 NTE INEN-ISO/IEC 27032:2015*

La norma nacional establece directrices para abordar la seguridad del Ciberespacio o cuestiones de ciberseguridad, proporciona una guía técnica para abordar riesgos de ciberprotección, tales como: ataques de ingeniería social, acceso secreto y no autorizado a sistemas informáticos, proliferación de software malicioso (malware), spyware y otros tipos de software potencialmente no deseables (Servicio Ecuatoriano de Normalización INEN, 2015).

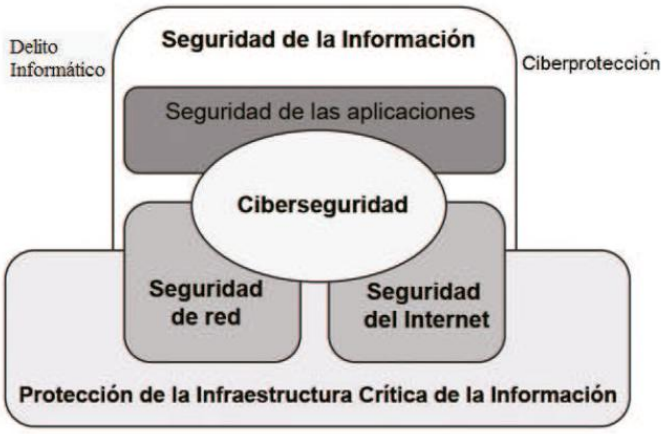



*Figura 2-2. Relación entre la Ciberseguridad y otros ámbitos de la seguridad (Servicio Ecuatoriano de Normalización INEN, 2015).*

La guía técnica proporciona controles para abordar estos riesgos, incluyendo controles para prepararse para ataques, detectar y monitorear ataques y responder a

los ataques. Esta norma nacional proporciona un marco para compartir información, coordinar y manejar incidentes (Servicio Ecuatoriano de Normalización INEN, 2015).

**Controles contra ataques de ingeniería social**

La guía se basa en la idea de que la única forma eficaz para mitigar la amenaza de la ingeniería social es a través de la combinación de: tecnologías de seguridad, políticas de seguridad que establezcan normas básicas de comportamiento personal (tanto como individuo y como un empleado), y, la educación y formación adecuada.

- *Políticas*

Determinar y documentar políticas básicas que regulen la información; en donde se relaciona a las redes sociales, que normalmente están más allá del alcance de la red de la empresa y de la seguridad de la información.

- *Métodos y procesos*

Se deben implementar procesos para la categorización y clasificación de la información, así como desarrollar y promulgar procedimientos sobre cómo manejar la propiedad intelectual de la empresa, los datos personales y otra información confidencial. De la mano van la concienciación y capacitación sobre seguridad, incluyendo la actualización periódica de los conocimientos y aprendizaje correspondientes; esto para los empleados de una organización y terceros contratistas como requisito. Para asegurar la atención de este riesgo, una organización debe considerar la realización de pruebas periódicas para determinar el nivel de conocimiento y cumplimiento con las políticas y prácticas relacionadas.

- *Las personas y la organización*

En una organización, los individuos son el principal objetivo y el principal punto de entrada para los ataques de ingeniería social. Como tal, las personas necesitan estar conscientes de los riesgos relacionados al interactuar o estar relacionados con el Ciberespacio, y las organizaciones deben establecer políticas y tomar medidas proactivas para patrocinar los programas para fin de asegurar la concienciación y competencia de las personas. Como regla general, todas las organizaciones (incluyendo empresas, proveedores de servicios y gobiernos) deben alentar a los consumidores en el Ciberespacio a conocer y entender los riesgos de ingeniería social en el Ciberespacio, y los pasos que deben tomar para protegerse contra posibles ataques.

- *Técnica*

Se deben considerar controles técnicos y adoptarlos en donde sea posible para minimizar la exposición y el aprovechamiento potencial de los delincuentes cibernéticos. Los controles que se mencionan en la norma son: autenticación de múltiples factores (MFA), certificado digital y asegurar un nivel mínimo de seguridad en los computadores de los usuarios, como la instalación de últimas actualizaciones de seguridad.

- *Disposición de la ciberseguridad*

Se especifican controles técnicos a nivel general y no específicos para ingeniería social, los mismos están establecidos en el *Anexo A: Disponibilidad de la ciberseguridad* y se refieren a monitoreo de redes oscuras (darknet), operaciones de hoyo (sinkhole) y rastreos (trackback).

#### *2.1.4.3 NIST SP800-50*

El Instituto Nacional de Estándares y Tecnología (NIST) es parte del Departamento de Comercio de los Estados Unidos y promueve la innovación y competitividad a través de tecnología, metrología y estándares para mejorar la estabilidad económica y la calidad de vida (National Institute of Standards and Technology, 2017). Entre las publicaciones especiales (SP) de NIST está la 800-50, denominada: *"Construcción de un programa de capacitación y concienciación en Seguridad de Tecnologías de la Información (Building an Information Technology Security Awareness and Training Program)"*.

El documento trata tres modelos comunes usados en la gestión del entrenamiento en seguridad:

- *Centralizado*: toda la responsabilidad reside en una autoridad central como el Director de Tecnología.
- *Parcialmente descentralizado*: las políticas de entrenamiento y la estrategia recaen en una autoridad central pero las responsabilidades de la implementación son distribuidas.
- *Totalmente descentralizado*: Sólo la política de desarrollo reside en una autoridad central, y todas las responsabilidades son delegadas a partes individuales de la organización.

El entrenamiento, concienciación y educación a los usuarios, quienes son la mayor audiencia dentro de una organización y son los que mayormente pueden ayudar a reducir errores no intencionales, así como vulnerabilidades de TI. Dentro de los usuarios se toma en cuenta a empleados, contratistas, investigadores, visitantes, invitados, entre otros colaboradores o asociados que requieran acceso a una organización.

Como soporte, el NIST elaboró la guía técnica SP800-115 para las pruebas y evaluación de seguridad de la información (*Technical Guide to information Security Testing and Assessmen*t); el capítulo 5.3 aborda las recomendaciones relacionadas a la Ingeniería Social refiriéndose al phishing, correos fraudulentos y adjuntos en correos electrónicos.

### 2.1.5 Certificaciones de Seguridad de la Información

Los profesionales en seguridad de la información además de capacitarse en técnicas, métodos y adquirir conocimientos empíricamente, obtienen certificaciones, las cuales aseveran que el individuo posee los conocimientos necesarios para la ejecución de determinadas funciones, en el ámbito de seguridad de la información y específicamente de ingeniería social, la certificación más enfocada y acertada, la de hacker en un ámbito y uso ético (*Certified Ethical Hacker*). Otras de las reconocidas certificaciones a nivel mundial son la CISSP (*Certified Information Systems Security Professional*) de ISC2 y la CISM (*Certified Information Security Manager*) de Isaca; sin embargo, en el entrenamiento y preparación no abordan temas específicos relacionados a la ingeniería social, sus métodos y medidas de protección.

#### *2.1.5.1 Certified Ethical Hacker*

La certificación de hacker ético (CEH) es una certificación del EC-Council (*International Council of Electronic Commerce Consultants*) que se otorga al obtener una alta puntuación en un examen predominantemente de opción múltiple, sin embargo, existen requisitos previos para poder acceder al examen, como haber tenido años de experiencia relacionada al área y formación educativa considerable. La versión a la que haremos referencia es la actual V9 (Oriyano, 2016), ya que en ésta se incluye un capítulo extendido de ingeniería social que especifica a las redes sociales.

**Ingeniería Social**

Los Ingenieros sociales están interesados en obtener información que puedan utilizar para llevar a cabo acciones como el robo de identidad o robo de contraseñas, o tratar

de encontrar información que pueda ser usada posteriormente. El objetivo final de cada vulneración mediante técnicas de ingeniería social es que la víctima pierda la guardia u obtener información para planificar un ataque posterior.

- *Fases*

La ingeniería social como otro tipo de ataques que explica CEH, consiste en fases diseñadas para guiar a un atacante cada vez más cerca de su objetivo. Para ello se consideran las siguientes fases, las mismas que se muestran en la Figura 2-3.

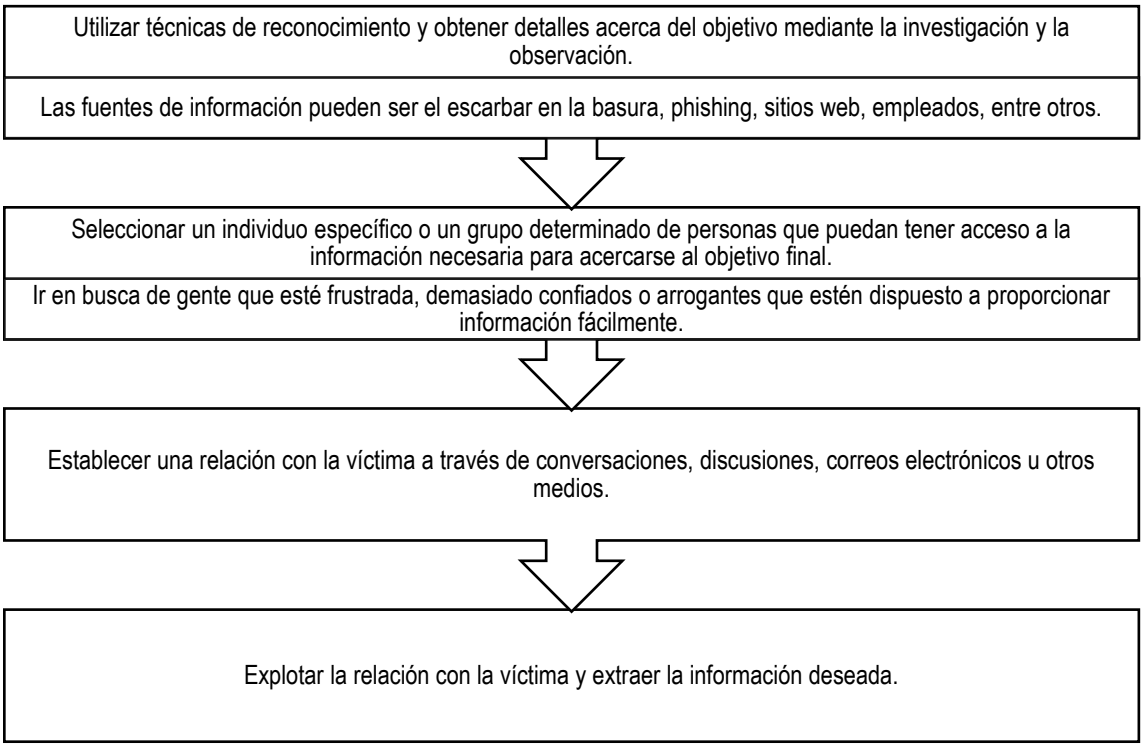



*Figura 2-3. Fases de Ingeniería Social según CEH.*

Se podrían considerar estas cuatro fases en tres componentes del proceso de Ingeniería Social:

- Investigación (paso 1)
- Desarrollo (pasos 2 y 3)
- Explotación (paso 4)

Un atacante o ingeniero social es el encargado de buscar potenciales víctimas que tengan algo más que ofrecer, los más comunes son recepcionistas, personal de mesa

de ayuda, usuarios, ejecutivos, administradores de sistemas, proveedores externos y personal de mantenimiento.

- *Obtener información de redes sociales*

En la última década, algunas de las más grandes amenazas a la seguridad se debe al uso de redes sociales. El rápido crecimiento de estas tecnologías permite cada día a millones de usuarios publicar contenido en Facebook, Twitter y muchas otras redes. La información que publican comúnmente es: información personal, fotos privadas o de instalaciones seguras, información de localización, información de amistades, información de negocios, preferencias y disgustos.

El peligro de tener esta información disponible permitiría a un atacante curioso recoger pistas de estas fuentes y obtener una foto nítida de un individuo o un negocio. Con esta información a la mano, un atacante puede llegar a pasarse por alguien de manera muy convincente y obtener acceso a una organización.

Las redes sociales permiten que el trabajo de un atacante sea mucho más fácil, esto ya que hay grandes volúmenes de datos e información personal disponible. En el pasado, no hubiese sido posible obtener esta información, ahora se lo hace con un par de clics y sin mucha inversión de tiempo.

Cuando los empleados de una organización publican información en las redes sociales u otros sitios, deben hacerlo siempre pensando en qué tan valiosa podría ser la información que publican y cuán fácil es que ésta caiga en las manos equivocadas o mejor no evitar publicarlo.

Las redes sociales pueden ser seguras si se toman en consideración ciertos aspectos; además, en muchos casos con un mínimo esfuerzo y cuidado se pueden disminuir y evitar problemas y riesgos de seguridad comunes.

- *Contraseña*: usar la misma contraseña en múltiples sitios permitiría a alguien que obtenga acceso a la contraseña, poder acceder a más datos o información personal que se almacene en otros sitios. Se debe tener en consideración que no todos los sitios web o sistemas almacenan apropiadamente la contraseña del usuario, evitando proteger la misma y permitiendo que alguien pueda robarlas. El amplio uso y crecimiento de estos sitios de redes sociales, en ocasiones evita que se tomen medidas adicionales para proteger a los usuarios y sus datos, y

puede llegar a ser demasiado tarde cuando se tomen las medidas necesarias. Además, en muchas ocasiones no se cuenta con políticas de cambio de contraseña periódicas, lo que hace que las cuentas de usuario se vean vulnerables a posibles ataques.

- *Demasiada información*: Con la proliferación de las redes sociales, la tendencia a compartir todo el tiempo se hace cada vez más común. Algunos usuarios de estas redes comparten información sin incluso tomarse el tiempo para leer completamente lo que están compartiendo, pensando que compartir no podría ser una estafa o robo. Sin embargo, la reputación de un individuo o de una organización podría verse comprometida si información incorrecta o falsa es compartida. Si bien no se ve inicialmente como un problema de seguridad sino de relaciones públicas, daría una percepción a la organización de que no consideran con mucha seguridad la información que manejan. Además de que estos tipos de estafas sirven para atrapar a usuarios usando frases que les inviten a investigar algo que normalmente no lo harían, por ejemplo: detalles secretos del fallecimiento de una celebridad, mide tu IQ, gana dinero resolviendo encuestas, entre otros.

- *Contramedidas en redes sociales*

Las redes sociales pueden ser usadas de manera confiable siempre y cuando se consideren ciertos aspectos y medidas básicas de seguridad, de tal manera que se pueda reducir el riesgo de utilizar estos servicios en la web.

- Disuadir la práctica de mezclar información personal y profesional en redes sociales. Aunque tal vez no se pueda eliminar la información compartida de la organización, debería mantenerse a un mínimo.
- Verificar siempre los contactos que se agregan, no conectar con desconocidos. Un problema común es que los usuarios normalmente aceptan invitaciones de individuos que no conocen.
- Evitar reutilizar contraseñas en varias redes sociales.
- No publicar nada en línea; todo lo publicado puede llegar a ser encontrado, incluso varios años después. Si algo no lo dices en una habitación llena de gente, no lo pongas en línea.

- Evitar la publicación de información personal que se pueda utilizar para determinar quién es, suplantar el perfil o convencer a alguien para revele información adicional.

Las medidas que debería tomar en consideración un profesional de seguridad de la información en una organización son:

- Educar empleados sobre publicaciones e identificación de información personal en línea, incluye números de teléfono, fotos de la casa, del trabajo, de la familia.
- Disponer o alentar el uso de cuentas de correo electrónico que no sean del trabajo para el uso de una red social u otros sistemas.
- Educar empelados en el uso de contraseñas fuertes.
- Evitar el uso de perfiles públicos, evitar que cualquiera pueda verlo.
- Educar a los empleados en el uso de las configuraciones de privacidad y modificación de las opciones por defecto.
- Instruir a los empleados sobre la presencia de estafas y phishing en redes sociales, y, cómo evitarlas y denunciarlas.

- *Robo de identidad*

El robo de identidad representa una de las amenazas más prominentes y en rápida evolución es el robo de identidad, que cae bajo el rótulo de la ingeniería social. Una vez que se consigue la información, un ladrón de identidad tiene varias opciones disponibles dependiendo de sus objetivos particulares. Se sabe que los ladrones cobran cargos en tarjetas de crédito, abren nuevas cuentas, reciben tratamiento médico o aseguran créditos y préstamos bajo el nombre de la víctima.

Los sitios de redes sociales son un gran blanco para los ciberdelincuentes que buscan información para robar y suplantar identidades. Ellos abusan de la naturaleza abierta de estos sitios y recopilan información personal sobre los usuarios, información que no está oculta, pero puede ser facilitada por los usuarios. Utilizando esta información, un atacante puede coaccionar o engañar a revelar datos que no revelaría de otra manera (Oriyano, 2016).

## 2.2 Herramientas de software

Para que algunos conceptos sean representados de una manera visual y para realizar cálculos basados en algoritmos, se han elegido dos herramientas principales de

software que permitirán el normal desarrollo de los objetivos planteados. Estas dos herramientas permiten ejecutar técnicas de análisis exploratorios de datos (EDA) (Tukey, 1977).

### 2.2.1 NodeXL Pro

- *Versión*: 1.0.1.387
- *Disponibilidad*: http://www.smrfoundation.org/nodexl
- *Licencia*: USD $ 29,00 ~ USD $ 749 / año.

Es un complemento para Microsoft Excel, que permite la importación y manipulación de datos que representan grafos, así como la visualización de redes basadas en algoritmos, análisis de redes sociales y agrupamiento por clústeres o atributos.

| | NodeXL Basic | NodeXL Pro | Requerido por el autor |
|---|---|---|---|
| **Visualización de redes** | ✓ | ✓ | ✓ |
| **Análisis de redes sociales** | ✓ | ✓ | ✓ |
| **Métricas avanzadas de redes** | | ✓ | ✓ |
| **Análisis de contenido** | | ✓ | |
| **APIs de redes sociales** | | ✓ | ✓ |
| **Importación de datos** | ✓ | ✓ | ✓ |
| **Exportación de datos** | | ✓ | ✓ |

*Tabla 2-2. Requerimientos funcionales de software NodeXL*

El licenciamiento gratuito *Basic* no contiene las funcionalidades requeridas (Tabla 2-2) para el desarrollo de este trabajo, por lo que se adquirió la versión *Pro Student User Licence*. La funcionalidad principal por la cual fue elegido este software es la posibilidad de usar la API de la red social Facebook para importar datos directamente desde la red hasta las tablas en Excel.

### 2.2.2 Gephi

- *Versión*: 0.9.1
- *Disponibilidad*: http://gephi.org
- *Licencia*: GNU GPL.

Es un software de código abierto que permite visualizar y explorar todo tipo de grafos y redes, trabaja con archivos en formato GraphML (Brandes, Eiglsperger, Herman,

Himsolt, & Marshall, 2002). Provee varios algoritmos de representación para optimizar la legibilidad de un grafo.

## 2.3 Redes sociales

Las estructuras o redes sociales se refieren a las conexiones compuestas por individuos, los cuales generalmente están relacionados por un motivo particular formando una red social (Wasserman & Faust, 1994), éstas pueden crecer si se combinan varias redes sociales que contienen los mismos actores. En este contexto y usando grafos para la representación de estas redes, cada actor pasa a ser un nodo de la red y cada arista o conexión se la denomina lazo interpersonal.

### 2.3.1 Lazos interpersonales

Los lazos interpersonales determinan la relación existente entre los actores o individuos. En una red no todos los individuos están conectados entre sí, por lo que la falta de una relación se ve reflejada en la inexistencia de un lazo interpersonal. A las relaciones existentes se les denomina lazos fuertes (*strong ties*). La hipótesis del lazo débil fue establecida por Rapoport (Rapoport, 1957) e indica que, si un nodo A está conectado a los nodos B y C, existe una probabilidad de que B y C estén conectados entre sí, a este enlace se le denomina lazo débil (*weak ties*).

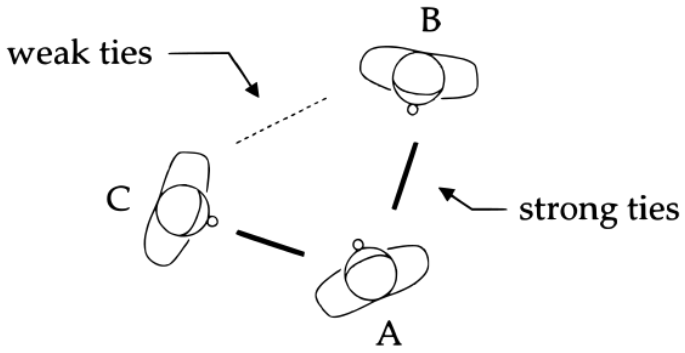



*Figura 2-4. Esquema de la hipótesis del lazo débil. (Rapoport, 1957)*

Los lazos fuertes acotarían predominantemente una red social o grupo de clique, y los lazos débiles cumplirían con una función de aristas de corte entre dos grupos densamente conectados de amigos cercanos. Cada lazo interpersonal puede tener un factor de peso que determine la fortaleza del lazo.

| **Nodo** | A | C | D | E | E | G | B | F | A | G | E | F | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| **Nodo** | B | B | B | C | B | B | F | D | E | D | G | A | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Peso** | **1** | **1** | **2** | **1** | **3** | **2** | **2** | **1** | **1** | **3** | **1** | **1** | **1** |

*Tabla 2-3. Datos de grafo con pesos en lazos interpersonales*

En la Tabla 2-3 se especifica el peso entre cada nodo en un grafo no direccionado y en la Figura 2-5 se representa gráficamente el peso del enlace aumentando o disminuyendo el grosor de la línea que une los nodos, este peso determina la fortaleza del lazo interpersonal entre dos individuos.

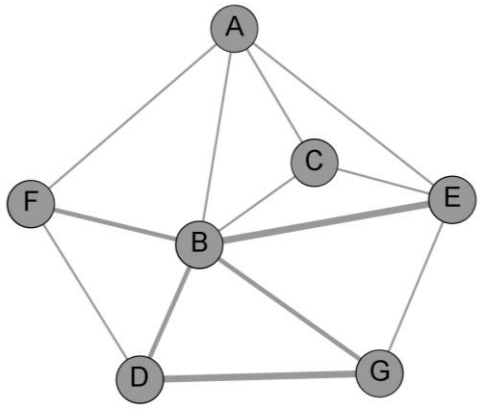



*Figura 2-5. Grafo con pesos en lazos interpersonales*

### 2.3.2 Ego networks

Las ego networks son redes sociales que se generan en base a un solo individuo, o que se forma en torno a un individuo en particular se le denomina *ego network*. En una sola red social pueden existir varios *ego networks*, para identificarlos se pueden utilizar algoritmos de particionamiento de técnica clúster, como DBSCAN (Arnaboldi, Conti, Passarella, & Pezzoni, 2012) y software como NodeXL (Hansen, Shneiderman, & Smith, 2011) o Gephi (Bastian, Heymann, & Jacomy, 2009). En visualización de grafos también existen algoritmos para ubicar los nodos de tal manera que mediante la observación se puedan identificar entre otras cosas, las *ego networks*. Entre los algoritmos más comunes de estas redes está el de Fruchterman-Reingold (Fruchterman & Reingold, 1991). Estos algoritmos usualmente no requieren de conocimientos específicos o avanzados acerca de teoría de grafos; tal es el caso de la planaridad, la cual es una característica de un grafo que permite ser dibujado sin que ninguna arista se cruce. El software y los algoritmos permiten identificar de manera visual una o varias *ego network*. En NodeXL generalmente se ejecuta el algoritmo con parámetros por defecto, mientras que en Gephi se pueden modificar las distintas variables del algoritmo.

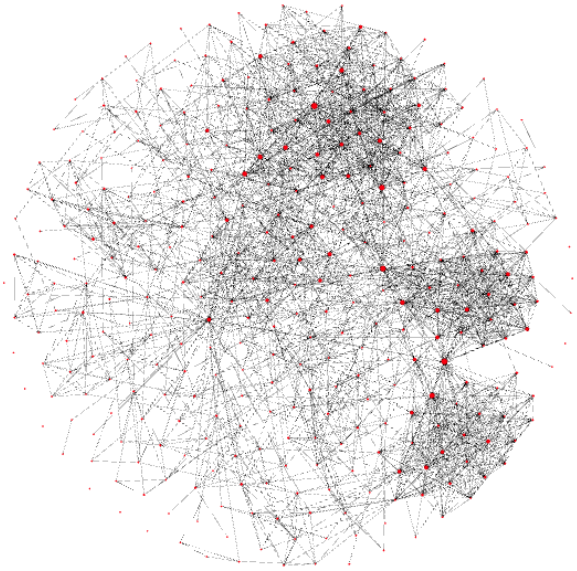


*Figura 2-6. Representación en grafo de una red social*

Usando Gephi, en la Figura 2-6 se visualiza una red social de amistades en Facebook (Žitnik, 2012) con el algoritmo Fruchterman-Reingold, en la Figura 2-7 se identifica con el puntero a una *ego network* incluida la red social representada de la Figura 2-6.

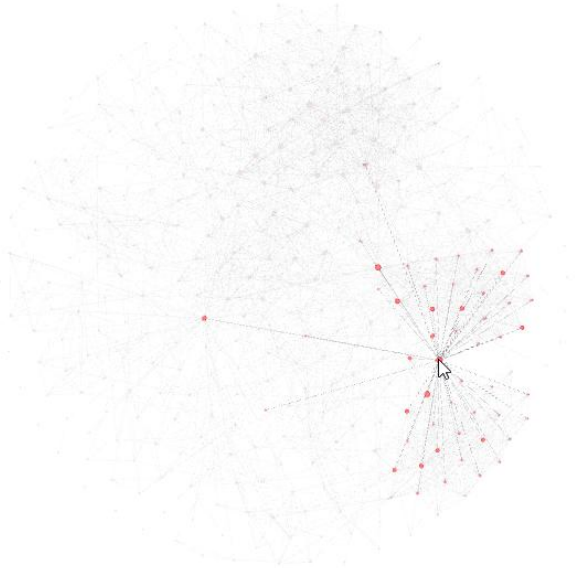


*Figura 2-7. Subgrafo de tipo ego network*

### 2.3.3 Redes Sociales Online

Se define a los sitios de redes sociales como servicios basados en la web que permiten a los individuos: (1) construir un perfil público o semi-público dentro de un sistema limitado, (2) formar una lista de otros usuarios con quienes compartan una conexión en particular, y (3) ver y recorrer su lista de conexiones y las realizadas por otros dentro del sistema. La naturaleza y nomenclatura de esas conexiones pueden variar entre sitio y sitio (Boyd & Ellison, 2007).

Los sitios web de redes sociales permiten a las personas interactuar con pares en línea al compartir sus opiniones, perspectivas, información, intereses y experiencias; además, pueden utilizar estos sitios para desarrollar nuevas relaciones personales y profesionales (Reynolds, 2016). Para entablar estas relaciones, en estos sitios se publica información personal como fotos, fecha de nacimiento, familiares, lugares de trabajo, ciudad y demás datos dependiendo del sitio web, esto con el fin de que los usuarios pueden identificarse claramente entre sí.

Facebook es considerada la red social online más usada a nivel global (Kemp, 2017), ésta representa varios aspectos del mundo real por los cuales los individuos comparten lazos interpersonales. Existen redes sociales online con dominios específicos y especializados; por ejemplo, LinkedIn, la misma que además de permitir vínculos entre individuos, representa las relaciones laborales con una organización y los miembros pertenecientes a las misma; también existen redes sociales online como Facebook, que abarcan muchos aspectos, además proveen información acerca de círculos de amigos, trabajo, lugares visitados, gustos, causas y demás; por otra parte, las redes sociales no sólo permiten la creación de perfiles personales, sino de páginas, que pueden ser: lugares, negocios, organizaciones, comunidades, artistas, marcas, entre otros.

# Capítulo 3. Estado del arte y trabajos relacionados

En este capítulo se analizan los trabajos relacionados con la ingeniería social en el ámbito de las redes sociales, sus procesos, contramedidas y riesgos. Se identifica la brecha existente en cada uno de ellos y, posterior, se identifican los riesgos comunes de ingeniería social para definir los riesgos del caso de estudio.

## 3.1 Modelos de Ingeniería Social

Los trabajos de investigación que se han tomado en cuenta para revisión, son los que se han basado en el ciclo de ingeniería social de Mitnick (Figura 2-1) y se analiza su vínculo con redes sociales en línea para finalmente proponer un modelo propio (59Capítulo 4).

### 3.1.1 The cycle of deception

Kowalski (Kowalski, 2002) y Nohlberg proponen *The cycle of deception* (Nohlberg & Kowalski, 2008), el cual abarca el ataque, la protección y la víctima, añadiendo elementos de control ofensivos y defensivos:

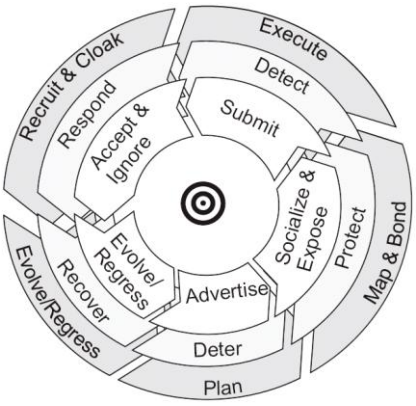



*Figura 3-1. Cycle of deception. Nohlberg (Nohlberg & Kowalski, 2008)*

El modelo propuesto en la Figura 3-1 está basado en investigaciones y análisis de casos de *grooming* y es posible obtener más información para el estudio de informes policiales en donde se realizan investigaciones más profundas de cada evento. *Grooming* es el término utilizado para cuando un adulto trata de convencer a un menor de edad de realizar actos sexuales (O'Connell, 2003).

El atacante debe tener éxito con los primeros tres pasos para que pueda continuar con los pasos cuatro y cinco de manera exitosa, basado en el razonamiento de que un atacante que no sea capaz de elaborar un plan y un método para el ataque, lo más

probable es que falle. Si no puede aprender sobre la víctima potencial, no podrá realizar el ataque, o el ataque fracasará. Si el atacante no puede ocultar el ataque, lo más probable es que lo atrapen.

Los autores de este modelo indican que a pesar de basarse en un estudio de *grooming*, este modelo, desde la perspectiva de las ciencias de la computación, puede ser usado en la implementación de un ataque automatizado de ingeniería social, permitiendo implementar sofisticados robots de inteligencia artificial.

Este modelo comprende como elemento a la organización, habitualmente los modelos incluyen únicamente al atacante y la víctima, sin embargo, la relación entre la víctima, el atacante y la organización es única, no establece un riesgo o elementos de control para los pares de la víctima, como sus compañeros de trabajo, familiares o amigos; el modelo tampoco establece parámetros o especificidades de qué información sería necesaria para concretar un ataque, se presenta únicamente a nivel general.

### 3.1.2 Social Engineering Attack Framework

Los autores elaboran un acercamiento a un modelo ontológico (Mouton, Leenen, Malan, & Venter, 2014) que defina el dominio de la ingeniería social basados en el análisis de las definiciones y taxonomías existentes de los términos: *ingeniería social*, *ataque de ingeniería social* e *ingeniero social*. En primera instancia dividen los ataques de ingeniería social en dos categorías principales: ataques indirectos y ataques directos.

Un ataque indirecto se refiere a un incidente en el que se utiliza un medio de terceros como forma de comunicación. Los medios suelen ser medios físicos: unidades flash, panfletos u otros, y los físicos como: páginas web. Cuando el objetivo es alcanzado a través de un tercero, sin interacción directa con el ingeniero social.

Un ataque directo es un incidente en el que dos o más personas están involucradas en una conversación directa. Esta conversación puede ser unilateral o bilateral, por lo que los ataques directos se clasifican además en comunicación bidireccional (ataques de suplantación) o unidireccional (phishing a través de correos o SMS).

El modelo ontológico propuesto (Figura 3-2) representa cada entidad de un ataque, así como las relaciones entre entidades.

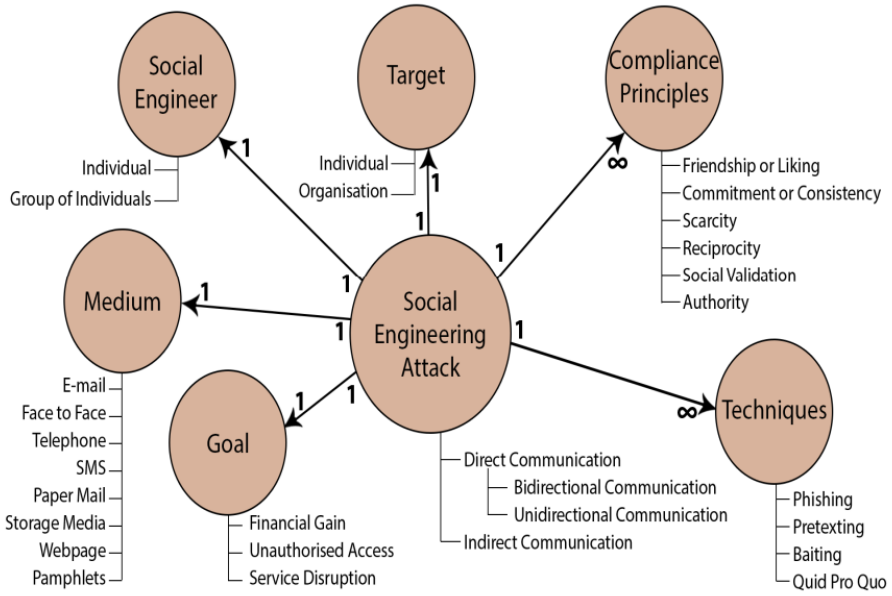



*Figura 3-2. Modelo ontológico que define el dominio de la ingeniería social (Mouton, Leenen, Malan, & Venter, 2014).*

El framework de ataque de ingeniería social (Mouton, Malan, Leenen, & Venter, 2014) propuesto aborda las deficiencias del ciclo de ataque de ingeniería social de Mitnick y se centra en cada paso del ataque de ingeniería social para en un principio determinar el objetivo de un ataque hasta la conclusión exitosa del ataque. El modelo ontológico contiene los componentes de un ataque de ingeniería social y el framework de ataque de ingeniería social (Figura 3-3) representa datos temporales como flujo y tiempo.

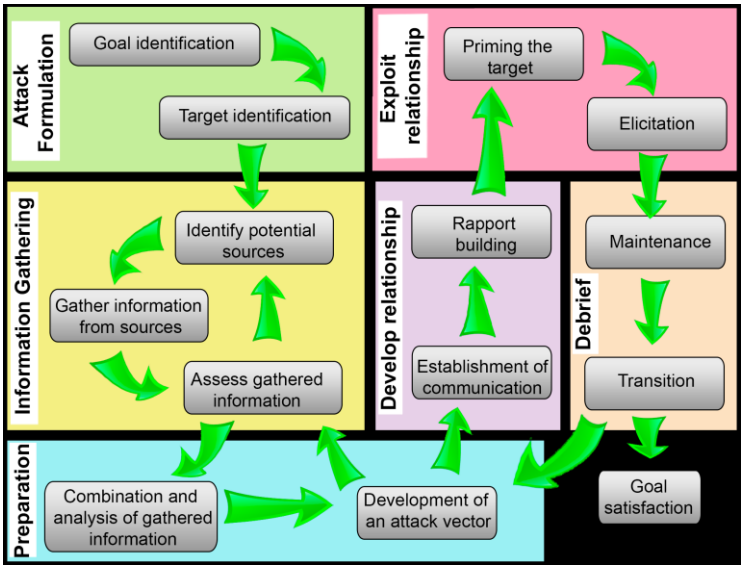



*Figura 3-3. Social Engineering Attack Framework (Mouton, Malan, Leenen, & Venter, 2014)*

El aporte de esta investigación es el modelo ontológico propuesto (Figura 3-2), que especifica una relación para el medio (*medium*) con el ataque de ingeniería social, en donde se establecen herramientas o activos de información que serían útiles para efectuar el ataque (por ejemplo una red social), además de técnicas (*techniques*) que son necesarias o recomendadas para concretar un ataque (por ejemplo *phishing*) y, en otra arista se establecen los principios de cumplimiento (*compliance principles*) como vulnerabilidades del individuo, sin embargo, en esta investigación no se considera que un tercero que es par a la víctima sea tanto un medio como una técnica, y mediante él se utilicen los principios de cumplimiento para la ejecución de un ataque de ingeniería social a través de redes sociales.

### 3.1.3 Social Engineering Framework

Se propone un marco de trabajo (Figura 3-4) para ayudar a profesionales de la seguridad a tener una mejor comprensión y más integral de la naturaleza y las características de los ataques de ingeniería social para poder desarrollar contramedidas eficaces. El framework de ingeniería social (Indrajit, 2017) está dividido en cuatro etapas:

#### *3.1.3.1 Preparation Stage*

- *Motivo de los ataques*: beneficio económico, ventaja política, desorden social, deterioro de imagen, trastorno cultural, desafío del pensamiento/valor, guerra y terrorismo.
- *Selección del objetivo*: en base al tipo y características del o las víctimas, se puede hacer una clasificación simple de la siguiente manera: individuo, grupo, organización, comunidad, público, híbrido y aleatorio.
- *Análisis del entorno*: el objetivo vive en un entorno cerrado que tiene su perímetro de seguridad intacto, se analiza parámetros internos y externos del entorno.
- *Exploración del perímetro*: se realiza actividad de escaneo físico y lógico.
- *Análisis de requisitos de información*: se define una lista de qué activos se necesitan para hacer que el trabajo sea exitoso, para ello se prepara un conjunto de requisitos técnicos y no técnicos.
- *Determinación de los propietarios de los activos*: según el conocimiento que tenga el individuo ante una información y tecnología, a la víctima se le divide en personas alfabetizadas o no alfabetizadas.

- *Desarrollo del escenario*: los ingenieros sociales establecen su definición final del alcance, objetivos, costo y tiempo del plan de explotación.

#### *3.1.3.2 Handshaking Stage*

- *Fingerprinting*: recolectar información del objetivo: perfiles, análisis de comportamiento y valores, sistema de conocimiento de relaciones, estado social y de autoridad, posibilidad de posibles vulnerabilidades.
- *Modelo de engaño*: elegir una técnica o combinación: phishing, pretexting, baiting, suplantación de identidad, quid pro quo, malware, observación física, hoaxing, elicitación, ingeniería social inversa.
- *Preparación de recursos*: personas, procesos y tecnología.
- *Tiempo y horario*: horarios antes del día D, tiempos durante el despliegue del ataque, período posterior al ataque.
- *Iniciación de relación*: el primer contacto debe ser una condición normal para no levantar sospechas, se debe desarrollar una relación lógica entre la víctima y el ingeniero social.
- *Construcción de relaciones*: desarrollar una relación cercana y armoniosa, sólo si el ingeniero social tiene la habilidad para realizarlo, se construye desde enfoques como: empatía, conformidad, solución, protección, escasez, comodidad y asistencia.
- *Construir confianza*: para tratar de influenciar, se pueden usar enfoques de: deber moral, deseo de ayuda, orden, persuasión, sugestión, entre otros.
- *Modelo de improvisación*: no siempre se puede llegar a construir una relación por no poder comunicarse o hablar con las víctimas debido a distintos factores, por lo que un ingeniero social debería poder improvisar.

#### *3.1.3.3 Attacking Stage*

- *Establecer zona de confort*: luego de que un ingeniero social haya construido confianza, debe poner a la víctima en su zona de confort. Los actos que deben establecerse son: escuchar bien, conversar coherentemente y temas impulsados por el valor.
- *Control del compromiso*: el ingeniero social debe tomar control de la víctima mediante tareas basadas en interacción y estímulo para formar un espíritu de cumplimiento de órdenes.

- *(Pre) modo de ataque*: en esta fase la víctima ha divulgado o está divulgando información específica, ya sea de manera explícita (divulgación de activos) implícita (información importante), que indiquen como adquirir tales datos confidenciales o información.
- *Confirmación de éxito*: en cuanto los datos o información se vayan adquiriendo, el ingeniero social debe verificar su validez.

#### *3.1.3.4 Post Action Stage*

- *Cierres*: el mensaje de "adiós" del ingeniero social hacia la víctima, generalmente se ejecutan dos cosas: mensaje de simpatía y ofrecimiento de asistencia.
- *Disipación*: todo enlace directo a la información en el perímetro del ingeniero social empieza a ser removido del sistema lentamente. Se realizan dos procesos: espera y desaparición.
- *Eliminación de rastros*: imprescindible tener un proceso para eliminar todos los rastros que pueda llevar a una trazabilidad de la víctima al ingeniero social. Se realizan dos procesos.

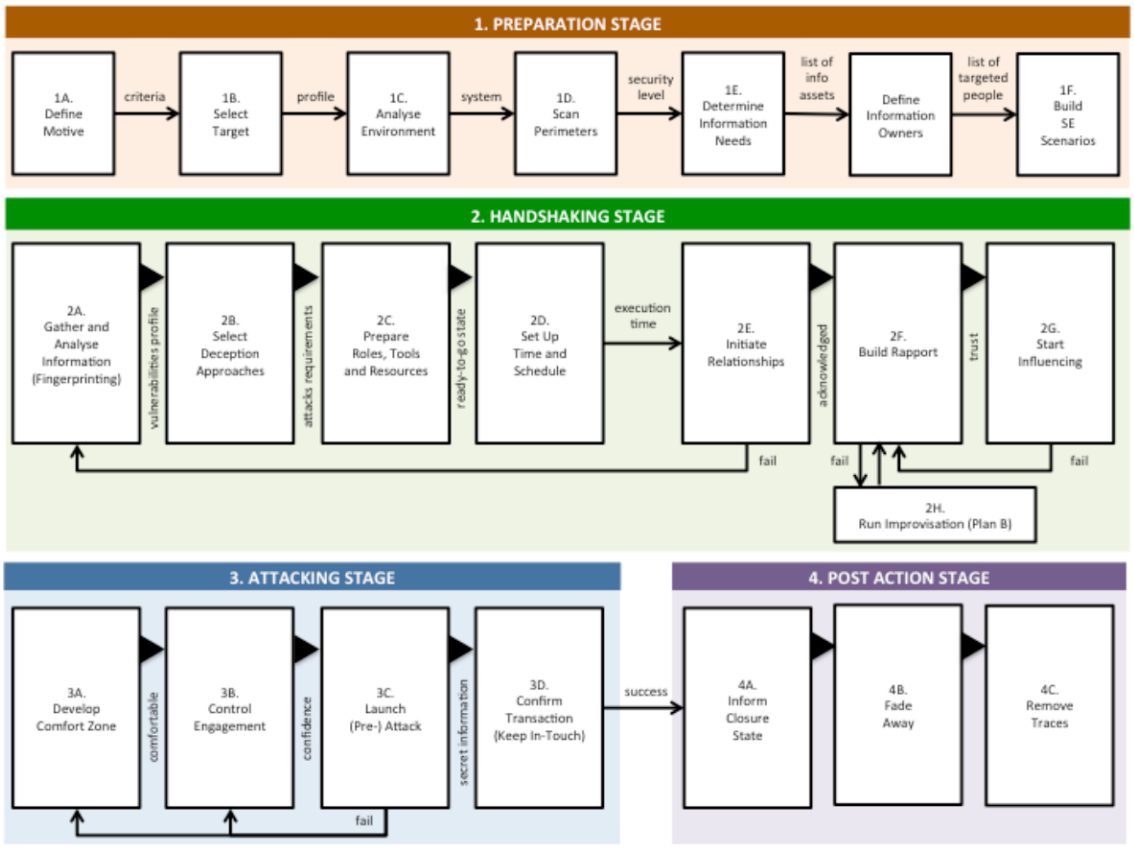



*Figura 3-4. Social Engineering Framework (Indrajit, 2017)*

En el marco de referencia propuesto, el autor sugiere utilizar herramientas y técnicas basadas en los medios sociales para obtener información de los miembros registrados a un servicio de una red social. En forma general, especifica no sólo fases o procesos como un marco de referencia, sino también subprocesos para cada etapa de un ataque de ingeniería social; no obstante, no se describe comprobación alguna del modelo propuesto sino únicamente se listan casos de ataques famosos de ingeniería social a través de la historia y en Indonesia para la elaboración del modelo. De este marco de referencia se utilizarán detalles de los subprocesos para ser probados en el caso de estudio.

### 3.1.4 Social Engineering Attack Detection Model: SEADMv2

Un modelo de detección de un ataque de ingeniería social (Mouton, Leenen, & Venter, 2015) propuesto, se basa en una revisión de varios modelos, en esta versión el modelo hace uso de un árbol de decisión y termina el proceso en componentes manejables que soporten la toma de decisiones.

El modelo (Figura 3-5) también describe el flujo de acción y como cualquier tipo de solicitud debe ser manejado por un *receptor*, entiendo este término como la persona que trata con la solicitud, mientras que el término *solicitante* se define como la persona y objeto que solicita la acción o información específica del receptor.

El modelo proporciona cuatro tipos diferentes de estados: la solicitud, el receptor, el solicitante y el tercero; que proporcionan una idea breve de lo que se puede esperar que se realice en cada estado.

Los autores han elaborado esta segunda versión de un modelo para detección de un ataque de ingeniería social, basándose en un marco de referencia para ataques de ingeniería social propuesto por los mismos autores (capítulo 3.1.2).

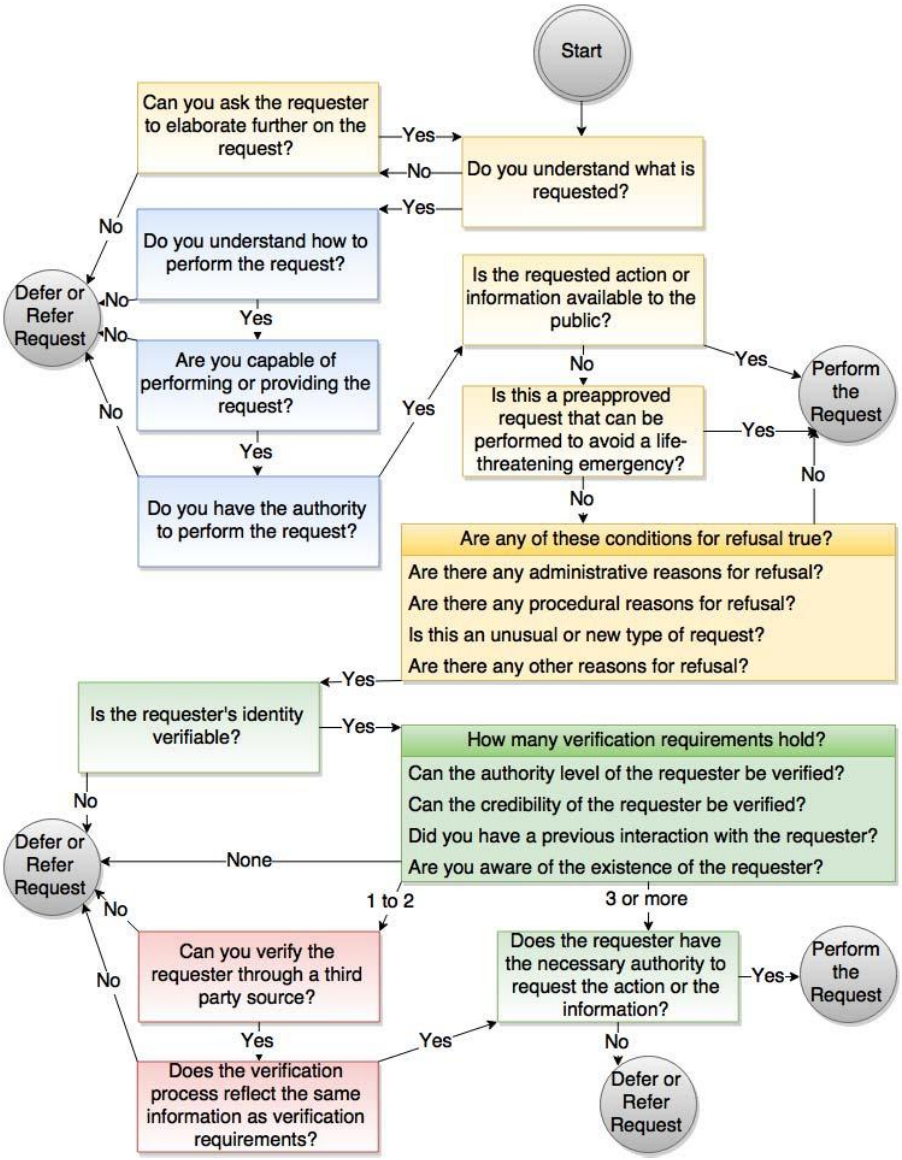



*Figura 3-5. Social Engineering Attack Detection Model: SEADMv2 (Mouton, Leenen, & Venter, 2015)*

Esta investigación realiza un análisis de taxonomías y modelos de ingeniería social para elaborar un modelo de detección de ataques, este modelo, aunque no presenta contramedidas específicas para evitar ser víctima de un ataque de ingeniería social, nos servirá de guía para la creación de la metodología de evaluación de perfiles en rede sociales, y será un soporte para la elaboración de políticas o procedimientos relacionados a la reducción de riesgos.

## 3.2 Facebook

### 3.2.1 Open Graph

Con el gran número de usuarios activos de Facebook, una actualización a la capacidad de búsqueda de Facebook se hizo a través del lanzamiento de *Graph Search*, esta función de búsqueda permite a los usuarios buscar en la red social utilizando consultas redactadas en inglés simple. Cuando se ejecuta una consulta, los resultados de la búsqueda pueden revelar información personal de amigos y desconocidos. Esta disponibilidad de información personal para terceros y extraños es una amenaza cibernética para las personas. Los ciberdelincuentes pueden usar *Graph Search* con intenciones maliciosas e ilegales.

En un análisis (Khan & Mashiane, 2014) de *Graph Search* se determinó que los amplios resultados de perfiles, fotos y muchos datos, en base a búsquedas simples, abría brechas de privacidad y confidencialidad que permite a extraños la posibilidad de filtrar perfiles de acuerdo a amplios parámetros y especificidades, por ejemplo: *Mujeres menores de 18 años que hayan realizado una visita a Café Vaca Matta, Suncoast Casino y que vivan en Durban*; de igual manera, estas consultas permitirían obtener información de autenticación y un posible rodo de identidad. Este tipo de consultas (query) sencillas permitiría a un ingeniero social, realizar un ataque de ingeniería social; al buscar a personas vulnerables de una organización.

### 3.2.2 Privacidad

Las configuraciones de privacidad (Facebook, 2016) son mecanismos de control de acceso que permiten a los usuarios decidir quién puede acceder a la información de su perfil. Los usuarios de Facebook pueden seleccionar una audiencia de una lista predefinida de grupos (amigos, amigos de amigos, pública, sólo yo) o crear sus propias listas. Facebook ha cambiado muchas veces su configuración de privacidad, incluso algunas funcionalidades de la plataforma han tenido que ser quitadas por demandas colectivas (Alsenoy, y otros, 2015). Luego, Facebook presentó *Privacy Basics*, un tutorial en donde los usuarios pueden controlar el acceso a su información, aunque estos controles son únicamente “sociales”, es decir, los controles en relación con lo que otros usuarios pueden ver o hacer, mas no controles que permiten a anunciantes o terceros poder seguir accediendo a determinados parámetros.

Como respuesta a un creciente uso indebido de herramientas para aplicaciones y desarrolladores, como medidas adicionales de privacidad y protección de información personal de los usuarios de su plataforma, ha decidido suspender el acceso a la misma desde su API a partir de la versión 2.0 (Facebook, 2017). Ya no es posible obtener información de los perfiles mediante aplicaciones desarrolladas para la plataforma que utilicen cualesquiera de los SDK que dispone para acceso y uso, lo que impide una automatización de extracción de información mediante el desarrollo de una aplicación que use la API actual. Sin embargo, es posible consultar información más detallada, pero de manera limitada mediante la plataforma Graph API Explorer (Facebook, 2017), la misma permite la extracción, modificación y eliminación de datos. La extracción de información del interés de esta investigación es posible, ya que permite obtener el perfil público, lista de amigos, lista de páginas, rango de edad, correo electrónico y demás información según la referencia de Graph API (Facebook, 2017).

## 3.3 Análisis de Riesgos

### 3.3.1 Situación actual

#### *3.3.1.1 Identificación de riesgos*

Los riesgos que involucran al usuario de redes sociales online no son muy distintos a los que comúnmente se exponen las personas que no hacen uso de estos servicios sobre internet, y, a pesar de que los proveedores de redes sociales online han destinado varias opciones para proteger a sus usuarios, los intrusos y atacantes son capaces de superar las medidas de seguridad mediante la explotación de la privacidad del usuario, la identidad y la confidencialidad utilizando varias técnicas. La mayoría de los usuarios de los sitios de redes sociales pueden no ser conscientes de la existencia de esas amenazas críticas. Un estudio (NaliniPriya & Asswini, 2015) especifica las vulnerabilidades a los que están expuestos los usuarios de redes sociales online:

| **Clasificación del ataque** | **Ataque** |
|---|---|
| *Amenazas clásicas* | Fraude en Internet, spammer, malware, ataque phishing, cross-site scripting, SQL injection attack |
| *Recientes tendencias en ataques* | Baiting, click-jacking, doxing, elicitation, pharming, phreaking, spoofing, ataque de suplantación de identidad, like-jacking, fake apps, plug-in scam, robo de identidad, socialbots, de-anonymization attacks |
| *Ataques de adolescentes* | Ciberacoso/stalking, online grooming, online-predators |

*Tabla 3-1. Clasificación de ataques de redes sociales online (NaliniPriya & Asswini, 2015).*

Existen características de redes sociales que permitirían no sólo ser víctimas de ataques cibernéticos, sino de ataques a la integridad física por el uso de redes sociales que utilizan la localización del usuario, generalmente dada por el GPS del dispositivo, ya sea para mejorar la experiencia de usuario o que sean funciones inherentes del servicio o aplicación; como es el caso de WeChat, se puede explotar las características de localización para predecir la ubicación física del usuario con eficacia desde cualquier lugar en el mundo (Peng, Meng, Xue, Hei, & Ross, 2015).

Otro tipo de vulnerabilidad al que se exponen las redes sociales es el ataque *sybil*. El ataque *sybil* es un tipo de ataque en el que un usuario malintencionado crea múltiples identidades falsas e interactúa en un sistema como si fueran verdaderos usuarios. De este modo, la presencia de ataques *sybil* en redes sociales, pueden generar reportes erróneos, usuarios pueden recibir spam e incluso provocaría la pérdida de privacidad.

Un estudio de percepción de los riesgos del uso de redes sociales (Goh, Di Gangi, Rivera, & Worrell, 2016) lista los riesgos sociales y técnicos percibidos:

- Contenido en línea puede ser usado para robo de identidad
- Infección por Malware
- Fuentes de información para ingeniería social
- Acceso no autorizado a cuentas de redes sociales
- Daño a reputación personal
- Cyber-stalking
- Contenido en línea se comparte para propósitos comerciales
- Cyber-bullying
- Acciones sin controlar
- Reducción de la productividad
- Exposición de información de manera involuntaria
- Contenido en línea puede ser almacenado o indexado

Los medios sociales crecieron por ser herramientas que promuevan la imagen personal de los individuos, así como imagen corporativa de una organización. Estas redes sociales al ser una herramienta que permita una interacción entre individuos y organizaciones, al mismo tiempo las expone a varios riesgos tecnológicos que afectarían la reputación de las organizaciones, un estudio de grupo Altimeter

(Webber, Li, & Szymanski, 2012) obtuvo los niveles de riesgo a nivel de medios sociales para las organizaciones (Figura 3-6).

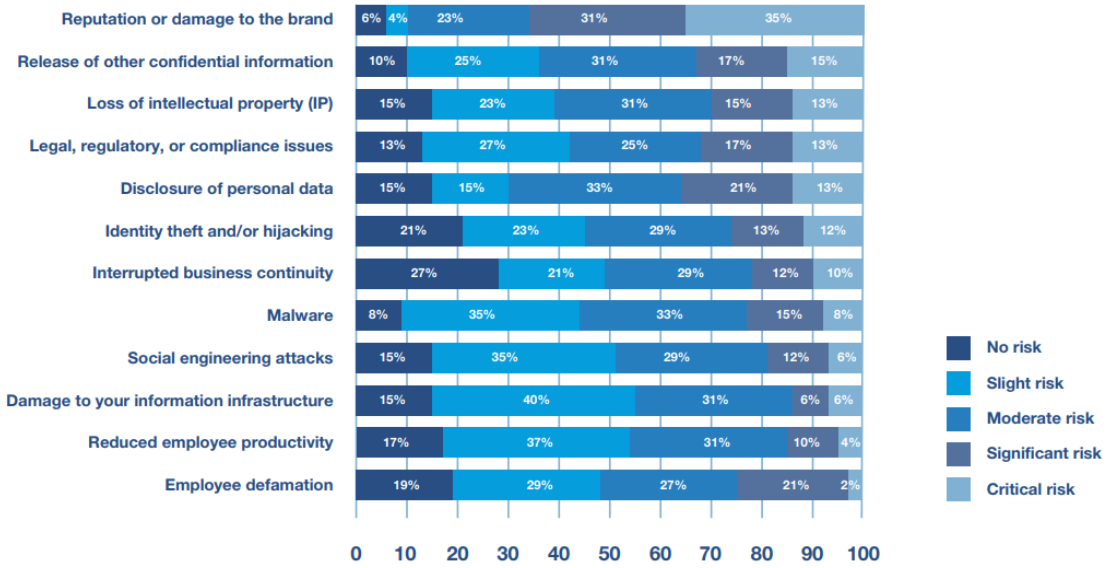



*Figura 3-6. Nivel de riesgo en medios sociales presente en las organizaciones. (Webber, Li, & Szymanski, 2012)*

En el estudio se presentan los distintos niveles de riesgo dependiendo del medio social que utilicen las distintas organizaciones (Figura 3-7). De esos resultados podemos determinar que las redes sociales con niveles significantes de riesgos son Facebook y Twitter.

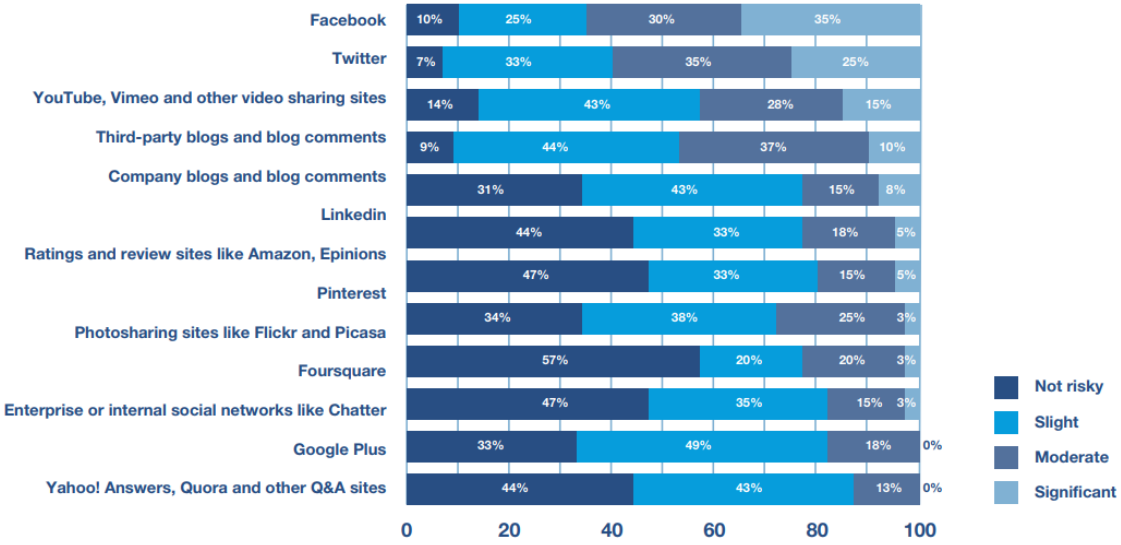



*Figura 3-7. Nivel de riesgo considerado en medios sociales para una organización. (Webber, Li, & Szymanski, 2012)*

#### *3.3.1.2 Preocupaciones y necesidades*

Los profesionales de seguridad de la información de las organizaciones tienen que constantemente actualizar sus conocimientos de seguridad y aplicar múltiples y recurrentes parches a sus sistemas, pero la mayoría de estas decisiones se basan en el riesgo y en las prioridades de los negocios, ya que parchar involucra costos de pruebas y otros costos indirectos como el tiempo fuera de servicio. Por otro lado, el cálculo del riesgo está en constante cambio, la mejor decisión tomada hace 6 meses basada en el riesgo ya no es aplicable el día de hoy en base al último reporte de Akamai (Akamai, 2017) ya que las pérdidas ante ataques son mucho más costosas en relación al año anterior, además de ataques mucho más sofisticados y en ocasiones, difíciles de detener con los recursos disponibles.

Una investigación enfocada en pruebas de seguridad (Osterman Research, 2016) reveló que la mayoría de organizaciones no son proactivas con respecto a pruebas de seguridad, y que la mayoría de organizaciones no ha hecho ninguna prueba de seguridad de ningún tipo en un período de 6 meses. La misma investigación revela que el 71% de entrevistados han sufrido un ataque de phishing y/o de ingeniería social en los 12 meses anteriores a la encuesta y 59% de ellos fueron víctimas de infiltración de malware (Figura 3-8).

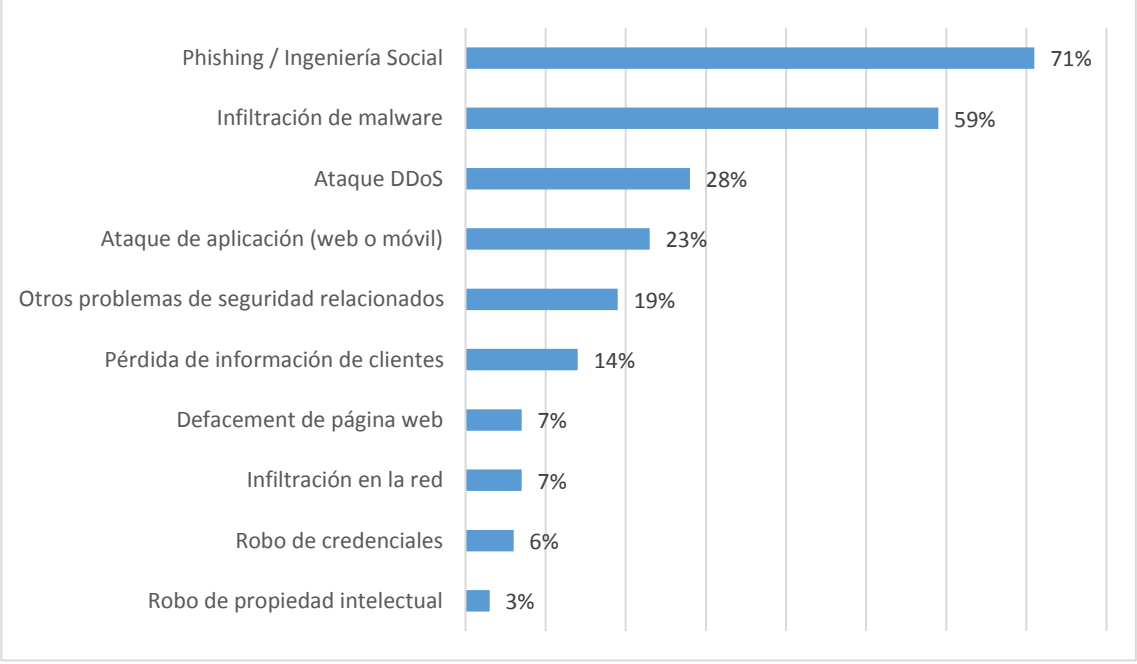



*Figura 3-8. Temas de seguridad que han experimentado las organizaciones en los últimos 12 meses (Osterman Research, 2016)*

El éxito de phishing y otras infiltraciones varía dependiendo de varios factores que incluyen: la culpa de la víctima, su entrenamiento, la vulnerabilidad de la aplicación, la infraestructura de la seguridad de la organización, entre otros. Sin embargo, hay cuatro razones claves por las cuales el phishing es exitoso hoy:

- Muchas aplicaciones comunes tienen una o más vulnerabilidades y el número de esas vulnerabilidades continúa en crecimiento, lo que significa que los criminales encuentran éxito fácilmente al introducir malware a través de ingeniería social y ataques phishing. Osterman Research (Osterman Research, 2016) descubrió que entrenamiento en seguridad en la mayoría de las organizaciones no es adecuado para ayudar a los usuarios a defenderse contra ataques phishing.
- Los usuarios comparten una enorme cantidad de información a través de las redes sociales, proporcionando a los cibercriminales información que pueden usar para generar ataques personalizados e inclusive mensajes mucho más creíbles.
- Los cibercriminales son cada día mejores en penetrar las defensas corporativas, incluyendo aplicaciones vulnerables. Mensajes perfeccionados y contenido personalizado hacen que los intentos de phishing sean más creíbles; es más probable que las victimas hagan clic en los links y en los archivos adjuntos.
- Algunas soluciones anti-phishing no tienen una base de datos con inteligencia en tiempo real, lo que las hace menos efectivas que aquellas que si tienen esa capacidad.

Entre los desafíos más importantes descubiertos en la encuesta, los más citados fueron la falta de personal, la falta de tiempo para realizar las pruebas de seguridad, y la necesidad de habilidades para apoyar pruebas más frecuentes.

### 3.3.2 Caso de estudio

La organización en donde se realizó el caso de estudio, es una institución pública que cuenta con presencia física de oficinas administrativas en cada una de las 24 provincias del Ecuador y una oficina matriz adicional en la capital. Por políticas de seguridad de la información y acuerdo de confidencialidad firmado por el autor, no se ha autorizado dar más detalles de los que se brinden en este estudio al respecto.

El estudio se realizó entre agosto de 2016 y abril de 2017, en ese entonces la organización no contaba con medidas de protección ante ataques de ingeniería social y

el uso de políticas de seguridad de la información basada en ISO 27001, se encontraba en socialización de empleados y proveedores.

Las cuentas de redes sociales de la organización eran administradas por empleados de la organización, y las cuentas personales de los voceros de la organización. En total fueron 25 cuentas institucionales y 4 de vocerías principales y 48 de vocerías secundarias, con un total de 77 cuentas, cada una de las 77 cuentas incluía al menos 2 redes sociales: Página de Facebook y Twitter, además de que ciertos voceros además de la página de Facebook tenían su cuenta personal de Facebook. Las cuentas institucionales tenían la misma organización que las oficinas administrativas, existía 1 cuenta matriz y 24 de cada una de las provincias, 4 de voceros de matriz y 2 de vocerías secundarias por cada provincia. Las 25 cuentas institucionales eran administradas por personal del área de comunicación, las 4 cuentas personales de vocerías principales las administraba el dueño de la cuenta y un asesor de confianza y las 48 cuentas personales de vocerías secundarias eran administradas por el dueño de la cuenta y en algunos casos por personal del área de comunicación de la organización. Cabe mencionar que algunas de las cuentas de vocerías secundarías no estaban habilitadas o se encontraban suspendidas por lo que no todas tenían el mismo nivel de uso y publicaciones, y que, como se dijo anteriormente, algunas vocerías sólo tenían habilitada una cuenta de página para emitir comunicados y no una cuenta adicional personal.

| | **Página de Facebook** | **Cuenta Personal** | **Cuentas personales de administradores de la red social** |
|---|---|---|---|
| **Matriz** | 1 Facebook | | 4 Facebook |
| | 1 Twitter | | 4 Twitter |
| **Cada provincia** | 1 Facebook | | 1 o 2 Facebook |
| | 1 Twitter | | 1 o 2 Twitter |
| **Cada vocería principal** | 1 Facebook | 1 Facebook | 2 Facebook |
| | | 1 Twitter | 2 Twitter |
| **Cada vocería secundaria** | | 1 Facebook | 1 o 2 Facebook |
| | | 1 Twitter | 1 o 2 Twitter |

*Tabla 3-2. Cuentas en redes sociales y organización administrativa*

Una de las preocupaciones de la organización era tener aseguradas sus cuentas institucionales de redes sociales, ya que uno de sus objetivos principales fue comunicar a la ciudadanía las acciones correspondientes tanto a nivel nacional como en cada provincia. Sin embargo, en cada provincia existen 2 empleados que son los de cargo

más representativo para desempeñar sus funciones día a día a los que se denominan voceros, y al representar a la organización se vio la necesidad de proteger también esas cuentas personales o páginas según corresponda. El principal motivo por el que expresaron su inquietud fue por un daño a la reputación, imagen y credibilidad que desencadenarían situaciones como: suplantación o robo de identidad, pérdida de información sensible y pérdida de la administración de sus redes.

La preocupación de la organización también venía apoyada desde el área de Tecnología, ya que, al administrar las cuentas de redes sociales desde la misma organización, hacían uso del servicio de Internet y tenían acceso sin restricciones a redes sociales por lo que podía ser la puerta de entrada para malware e infección a equipos y a la red.

#### *3.3.2.1 Metodología*

1. De los administradores de páginas y voceros, se eligen perfiles de Facebook que no hayan modificado las configuraciones de privacidad y seguridad.
2. Se le solicita instalar una aplicación de Facebook desarrollada para pruebas de seguridad.
3. Análisis de información pública en los perfiles.
4. Los perfiles elegidos son sometidos a pruebas de ingeniería social para extracción de información mediante un modelo de ataque.
5. Se aplicarán medidas correctivas para mitigación de riesgos.
6. Análisis de información pública en los perfiles.

#### *3.3.2.2 Matriz de riesgos*

Al realizar un análisis entre los riesgos existentes actualmente en el entorno, con las preocupaciones de la industria y de la organización a realizarse el caso de estudio, se elabora una matriz de riesgo para las cuentas de Facebook, con un posible impacto que puedan tener los individuos administradores, propietarios de cuentas personales o páginas y los activos de información y de tecnología, analiza el impacto para las áreas de Comunicación y Tecnología (Tabla 3-3).

| Riesgo | | | | Impacto | | Control Actual | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Amenaza | Vulnerabilidad | Probabilidad | Imagen y Reputación | Activos de Tecnología | Políticas SI | Capacitación | Configuración | Tecnología |
| **A** | Robo de identidad | Marca no registrada.<br>Cuentas no verificadas | 3 | 5 | 0 | No | No | No | N/A |
| **B** | Phishing | Falta de capacitación<br>Uso de correos electrónicos personales para el trabajo | 4 | 5 | 5 | Sí | No | No | Sí |
| **C** | Crisis de reputación de la marca | Falta de capacitación<br>Falta de personal | 3 | 5 | 0 | N/A | No | No | N/A |
| **D** | Infección por Malware | Falta de capacitación | 3 | 4 | 3 | Sí | No | Sí | Sí |
| **E** | Filtración de información | No existe acuerdo de confidencialidad y no divulgación | 3 | 3 | 2 | Sí | No | N/A | No |
| **F** | Acceso no autorizado cuentas de redes sociales | Seguridad no configurada | 2 | 5 | 0 | N/A | No | No | N/A |
| **G** | Robo de credenciales | Falta de capacitación | 2 | 4 | 0 | Sí | No | No | N/A |
| **H** | Apropiación de cuentas | Roles no definidos<br>No existe acuerdo de confidencialidad y no divulgación | 1 | 5 | 0 | No | No | No | N/A |
| **I** | Ataques de ingeniería social | Falta de capacitación | 5 | 4 | 4 | No | No | No | No |
| **J** | Extracción de información pública | Privacidad no configurada | 5 | 3 | 0 | No | No | No | N/A |
| **K** | Spam | Privacidad no configurada | 3 | 2 | 3 | Sí | No | Sí | Sí |
| **L** | Publicación contenido inapropiado | Roles no definidos | 1 | 5 | 0 | No | No | No | N/A |
| **M** | Vishing | Falta de capacitación | 2 | 3 | 0 | Sí | No | No | N/A |
| **N** | Ciber-acoso | Privacidad no configurada<br>Falta de capacitación | 2 | 2 | 0 | No | No | No | N/A |
| **O** | Aplicaciones falsas | Seguridad no configurada<br>Privacidad no configurada | 1 | 3 | 3 | Sí | No | No | No |

*Tabla 3-3. Matriz de Riesgos en Redes Sociales*

Aunque exista una amenaza a la misma organización para el ámbito de *Imagen y Reputación* (comunicación) y para *Activos de Tecnología* (tecnología), el impacto no será el mismo para ambas áreas. Por lo que se elabora una matriz de riesgo para cada área.

| PROBABILIDAD | IMPACTO | | | | | |
|---|---|---|---|---|---|---|
| | Sin impacto | Insignificante | Menor | Moderada | Mayor | Catastrófica |
| Casi seguro | J | | | | I | |
| Probable | | | | | | B |
| Posible | A,C | | E | D,K | | |
| Improbable | F,G,M,N | | | | | |
| Raro | H,L | | | O | | |

*Tabla 3-4. Nivel de riesgos de activos de tecnología*

En la Tabla 3-4 se puede observar que un impacto nulo se registra para la mayoría de amenazas analizadas, y esto se debe a que, aunque existan o no los controles, el dominio no siempre corresponde o afecta directamente al área de tecnología, sin embargo se identifican dos amenazas que se consideran un riesgo extremo (color rojo) en activos de tecnología, dos amenazas de riesgo alto (color naranja) y tres de riesgo moderado (color amarillo).

En la Tabla 3-5, no existen amenazas que se puedan considerar tipo riesgo bajo (color verde), las amenazas I y B coinciden con el nivel de riesgo de la Tabla 3-4, adicional, existen 9 de riesgo alto que se tomarán en consideración para la mitigación de los riesgos así como verificación de cumplimiento y comparación con requisitos normativos.

| PROBABILIDAD | IMPACTO | | | | | |
|---|---|---|---|---|---|---|
| | Sin impacto | Insignificante | Menor | Moderada | Mayor | Catastrófica |
| Casi seguro | | | | J | I | |
| Probable | | | | | D | B |
| Posible | | | K | E | | A, C |
| Improbable | | | N | M | G | F |
| Raro | | | | O | | H, L |

*Tabla 3-5. Nivel de riesgos de imagen y reputación*

De estas dos matrices de riesgos se definen las amenazas que a serán tratadas con prioridad por la organización:

- Phishing

- Ataques de Ingeniería Social
- Infección por malware
- Extracción de Información Pública
- Robo de Identidad

A pesar de que existen más amenazas de riesgo alto, se espera que, en una primera acción, con la mitigación en controles, se reduzca el nivel de probabilidad de ocurrencia en un nuevo análisis de riesgos.

### 3.3.3 Determinación de acciones requeridas

La organización al contar como control unas Políticas de Seguridad de la Información aprobada pero aún sin una inducción completa, se revisan y analizan los controles que mitigarían la amenaza *Ataques de Ingeniería Social* a través de Redes Sociales. A esta política hacemos el análisis de los controles (NTE INEN-ISO/IEC 27002:2017) de seguridad de la información y se suman las directrices de ciberseguridad (**¡Error! No se encuentra el origen de la referencia.**). En base a las políticas se ajustan y definen parámetros a ser considerados para personal de Comunicación y administradores de cuentas en redes sociales.

| **Controles** | | **Ajustes para Redes Sociales** |
|---|---|---|
| **Seguridad en recursos humanos** | • *Antes del empleo* | • Establecer de responsabilidad en términos y condiciones del empleo |
| | • *Durante el empleo* | • Establecer responsabilidades.<br>• Inducción en Seguridad de la Información.<br>• Procesos disciplinarios. |
| | • *Finalización del empleo* | • Responsabilidades de uso de credenciales. |
| **Control de acceso** | • *Requisitos del negocio* | • Acceso a redes y servicios de redes sociales. |
| | • *Gestión de acceso de los usuarios* | • Establecimiento de privilegios administrativos de páginas de Facebook según responsabilidades y requerimientos.<br>• Actas de entrega y traspaso de credenciales de acceso. |
| | • *Responsabilidades del usuario* | • Firma de acuerdo de confidencialidad y buen uso de información secreta de autenticación. |
| | • *Control de acceso a sistemas y aplicaciones* | • Establecimiento de procesos seguros de inicio de sesión. |
| | • *Áreas seguras* | • Controles físicos de entrada a oficinas. |

| | | |
|---|---|---|
| **Seguridad física y del entorno** | • *Equipos* | • Seguridad de equipos y activos fuera de las instalaciones.<br>• Reutilización o eliminación segura de equipos. |
| **Gestión de incidentes de seguridad de la información** | • *Responsabilidades y procedimientos* | • Preparación de formularios de comunicación de eventos de seguridad de la información. |
| | • *Respuesta a incidentes de seguridad de la información* | • Comunicación de la existencia del incidente de seguridad de la información para personas internas o externas o terceras organizaciones con necesidad de conocer. |

*Tabla 3-6. Evaluación de controles de ingeniería social con ISO 27002 para redes sociales*

Se han definido controles ajustados para redes sociales (Tabla 3-6) que cumplirían los requisitos normativos establecidos para prevenir ataques de ingeniería social. Sin embargo, estos controles no brindan la protección necesaria para reducir en gran medida ataques de tipo phishing o ingeniería social hacia perfiles personales e institucionales en Facebook. Por este motivo, se realiza una evaluación de controles de ingeniería social a nivel de ciberespacio (Tabla 3-7), con esto se entiende se incluiría los sitios web de redes sociales. De este análisis se espera obtener directrices y controles específicos que reducirían los riesgos de ingeniería social y phishing.

| **Controles** | | **Ajustes para Redes Sociales** |
|---|---|---|
| **Políticas contra ataques de ingeniería social** | • *Política de información* | • Creación, recolección, procesamiento y uso de la información en redes sociales |
| **Métodos y procesos** | • *Categorización y clasificación de la información* | • Implementar procesos para la categorización y clasificación de la información<br>• Protección de la información corporativa clasificada y de la información personal delicada.<br>• Desarrollar y documentar controles de seguridad específicos para la protección contra la exposición accidental y acceso no autorizado. |
| | • Concienciación y capacitación | • Concienciación de funciones y responsabilidad en el Ciberespacio.<br>• Definir qué información necesita ser protegida y cómo protegerla. |
| | • Pruebas | • Pruebas escritas |

| | |
|---|---|
| | • Pruebas CBT (entrenamiento basado en computadora), al menos con: sitios phishing controlados, spam, correos fraudulentos. |
| **Personas y la organización** | • Establecer competencia de las personas para con la organización en redes sociales. |
| **Técnica** | • Establecer al menos segundo factor de autenticación<br>• Utilizar certificados digitales para correos electrónicos y en navegación<br>• Controles adicionales para establecer niveles mínimos de seguridad en equipos como instalación de últimas actualizaciones de seguridad. |

*Tabla 3-7. Evaluación de controles de ingeniería social con ISO 27032 para redes sociales*

Para evaluar la suficiencia y eficacia de los controles, se propone ampliar lo establecido en la norma ISO 27032 (capítulo 2.1.4.2) y configurar las pruebas a realizar hacia un entorno de redes sociales, específicamente Facebook, para esto, se diseña un modelo de ataque siguiendo las normas y metodologías de seguridad de la información.

# Capítulo 4. Modelo de ataque de Ingeniería Social a un perfil en una red social

La mayor parte de vulneraciones de tipo Ingeniería Social tienen que ver con la privacidad de las personas, en redes sociales, lo más común es que el usuario no modifique las configuraciones de seguridad y privacidad que Facebook implementa y dispone para el usuario. Los usuarios se limitan a probar y utilizar la red social al considerarse divertidas y útiles, formando hábitos en torno a cada una de ellas. La información privada más compartida es la relativa a la fecha y lugar de nacimiento, aunque el recibir muchas felicitaciones el día de cumpleaños en una red social puede ser algo normal y agradable para muchos usuarios, algunos servicios como instituciones financieras que administran nuestro dinero realizan preguntas personales que influyen la información publicada, por lo que un tercero accedería instantáneamente a la misma. Otro ejemplo común es indicar quienes son nuestros parientes e incluso nuestras mascotas, información que también es requerida por instituciones financieras para verificar la identidad de una persona (Malenkovich, 2014).

En el caso de figuras públicas, o voceros de organizaciones, el uso de estas redes sociales pone en riesgo potencial de ser un objetivo de un ataque de ingeniería social, ya que su uso no se limita a una o dos veces al día como un usuario normal, sino a usar más de una red varias veces al día; este uso podría resultar en la omisión de ciertos detalles que permitirían detectar un ataque de ingeniería social y que el individuo pueda convertirse en una víctima, ya sea el *community manager* o el dueño de la cuenta.

Para analizar la vulnerabilidad de los perfiles en Facebook de los administradores de cuentas institucionales o de cuentas de voceros, se propone realizar un modelo que defina los pasos y herramientas para llevar a cabo o simular un ataque de ingeniería social enfocado a un perfil de Facebook. La creación de modelos basados en marcos de trabajo relacionados a ataques de ingeniería social, permite la generación de escenarios y análisis de ataques previos, útiles para el desarrollo de concientización, propósitos de entrenamiento y desarrollo de contramedidas de ataques de ingeniería social.

La propuesta de un modelo al que se le ha llamado SAMSON (Social engineering Attack Model on Social Networks) se fundamenta principalmente en las fases de ingeniería social de CEH (capítulo 2.1.5.1) y trabajos relacionados expuestos en el

Capítulo 3; así también, se basa en la utilización de un símil o par al individuo víctima para la ejecución del ataque, estableciendo a este tercero como medio y técnica (Capítulo 3.1.2).

SAMSON utiliza la teoría de lazos interpersonales, para detectar relaciones existentes entre la víctima y sus amigos de Facebook, este grafo de tipo *ego network* permite la revisión hasta de los amigos de sus amigos, las relaciones existentes entre páginas y la víctima también son analizadas y evaluadas para establecer vectores de ataque efectivos.

## 4.1 Captura y visualización de métricas

En un primer paso para la elaboración del modelo, se analiza la información que comparte cada perfil en Facebook con otros perfiles y aplicaciones (Tabla 4-1), esta información se obtiene de la referencia de Graph API (Facebook, 2017).

| | |
|---|---|
| **Datos personales (Profile:User)** | Identificador único (id) |
| | Nombre completo |
| | Fecha de nacimiento |
| | Correo electrónico |
| | Género |
| | Ciudad natal |
| | Ciudad de residencia |
| | Estado civil |
| | Religión |
| | Sitio web |
| | Lugares donde ha trabajado (list<WorkExperience>) |
| | Lugares donde ha estudiado (list<EducationExperience>) |
| | … |
| **Aristas (edges)** | Páginas de Facebook que administra (accounts) |
| | Álbumes de fotos (albums) |
| | Libros listados en el perfil (books) |
| | Familiares (family) |
| | Amigos (friends) |
| | Juegos (games) |
| | Grupos que administra (groups) |
| | Páginas que le gusta (likes) |

| | |
|---|---|
| | Películas que le gusta (movies) |
| | Música que le gusta (music) |
| | Fotos en las que está etiquetado o que ha subido (photos) |
| | Videos en donde la persona está etiquetada o que ha subido (videos) |
| | Visitas que ha registrado la persona (checkins) |
| | Lista de publicaciones y fotos que incluyan información de localización (locations) |
| | … |

*Tabla 4-1. Información disponible en un perfil de Facebook.*

Cada película, artista o página en la que ha realizado una acción de *Me Gusta*, tiene sus propias características (Tabla 4-2). Esto incluye a lugares donde ha trabajado y lugares en donde ha estudiado.

| | |
|---|---|
| **Datos de página (Page)** | Identificador único (id) |
| | Nombre de la página |
| | Información de la página |
| | Año de nacimiento. Para páginas que representen personas. |
| | Visitas registradas. Para páginas que representan lugares físicos (chekins) |
| | Correos electrónicos |
| | Teléfono |
| | Sitio web |
| | … |

*Tabla 4-2. Información disponible en una página de Facebook.*

Para el análisis, siguiendo la metodología del caso de estudio, se analizaron perfiles de personas y se revisaron los siguientes factores para realizar grafos que aporten conocimiento a la elaboración del modelo:

- Relación de amistad (*friend*)
- Parentesco familiar (*family*)
- Relación laboral (*work*)
- Lugares visitados (*check-in*)
- Páginas de Facebook de tipo *trabajo* o *lugar* que le gustan (*like*)

Para este procedimiento se desarrolló una aplicación en Facebook que obtenga parte de la información del perfil mencionada anteriormente y se solicitó a los sujetos que la instalen, ya que al hacerlo el código se encargaba de realizar el procedimiento respectivo de extracción de información.

La aplicación se desarrolló en lenguaje de programación PHP, usando hosting y dominio propio, y bajo Facebook PHP SDK versión 5.5. Los archivos de código y del SDK se subieron sobre un dominio distinto al de la organización y validado por Facebook para aplicaciones, y los archivos necesarios para el funcionamiento de la misma. La aplicación obtiene la información y la exporta en formato CSV, para ser importada y procesada por NodeXL. Los verdaderos nombres de los individuos y de las páginas han sido cambiados por otros para mantener el acuerdo de privacidad firmado con la organización donde se aplicó el caso de estudio.

| A,B,Relation |
|---|
| Ana Lucia,The Island,CheckIn |
| Ana Lucia,Benjamin Linus,Friend |
| Ana Lucia,Christian Shephard,Friend |
| Ana Lucia,LAPD,Work |
| Ana Lucia,LAPD,Like |
| Ana Lucia,Teresa Cortez,Family |
| Christian Shephard,Carole Littleton,Family |
| Christian Shephard,Carole Littleton,Friend |
| Christian Shephard,Margo Shephard,Family |
| Christian Shephard,St. Sebastian Hospital,Work |
| Christian Shephard,St. Sebastian Hospital,Like |
| Claire Littleton,Aaron Littleton,Family |
| Claire Littleton,Alex Rousseau,Friend |
| Claire Littleton,Carole Littleton,Friend |
| ... |

*Tabla 4-3. Muestra del archivo CSV que genera la aplicación de Facebook*

Cada perfil es tomado como el nodo principal de una *ego network*, las aristas son las relaciones con otros nodos que se definieron (*friend, family, work, like, check-in*).

En la Figura 4-1 se puede visualizar los enlaces y marcado en color rojo el nodo que representa la *ego network* de donde se obtuvo la información para la representación, el gráfico está construido con el algoritmo Fruchterman-Reingold (Fruchterman & Reingold, 1991). En este gráfico no es posible graficar más de una arista entre dos nodos, por lo que la información obtenida se exporta al formato GraphML para

representar en Gephi y por cada arista existente entre nodos, se suma el peso de la arista, cada arista tiene un peso de una unidad; es decir, si entre dos individuos existe una relación de amistad (*friend*) y además un parentesco familiar (*family*), el peso de la arista entre los dos nodos sería de 2, obteniendo así la Figura 4-2, en la misma, el grosor de las aristas representa el peso de cada una y de igual manera se marca la misma *ego network* y está representada con los parámetros por defecto en Gephi del algoritmo Fruchterman-Reingold .

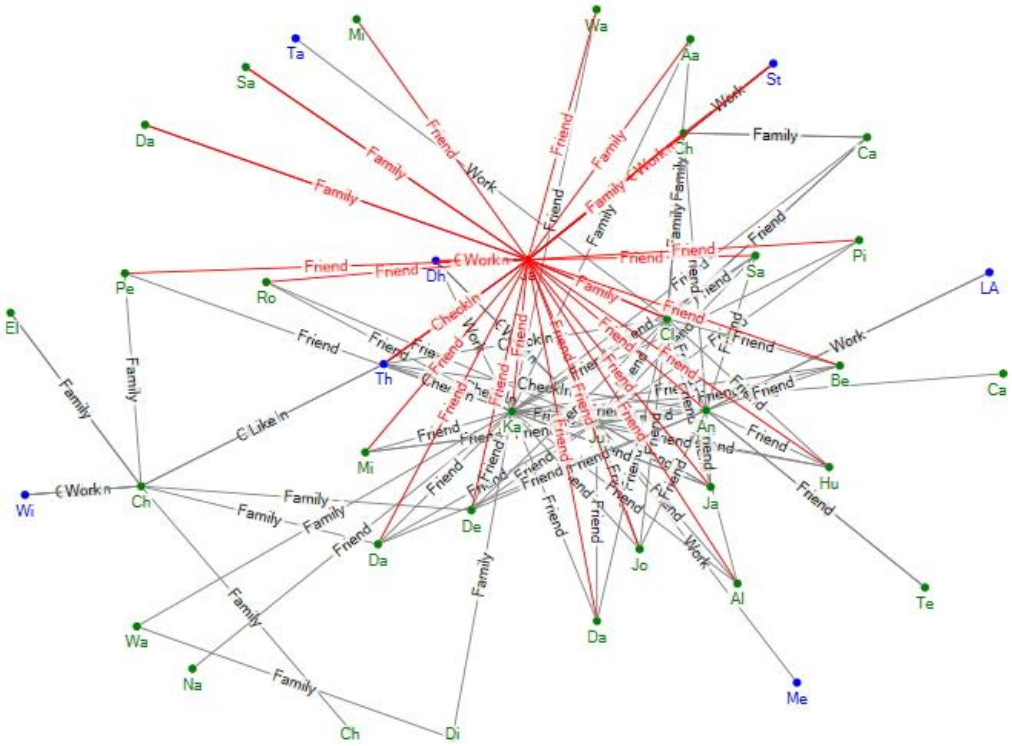



*Figura 4-1. Grafo de relaciones analizadas de un perfil personal de Facebook en NodeXL*

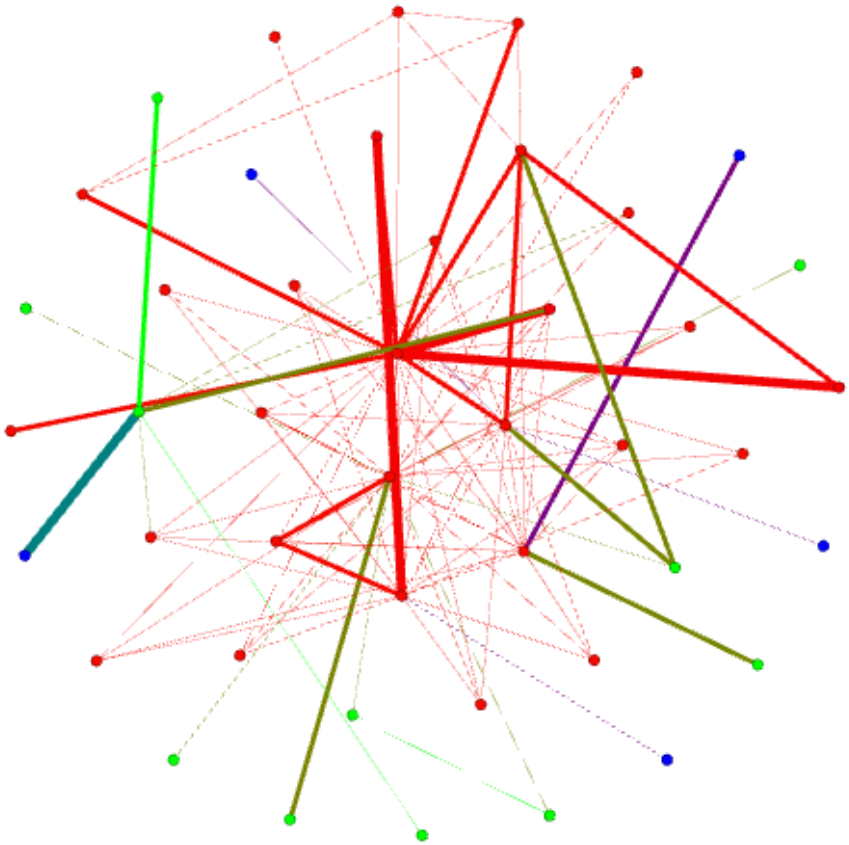


*Figura 4-2. Grafo de relaciones con pesos de un perfil personal de Facebook en Gephi.*

Estos datos cuantitativos son la base del paso 1 y 2 de la metodología ya que ayudan al Ingeniero Social a elaborar un análisis y poder evaluar el nivel de vulnerabilidad existente para diseñar un ataque y obtener información de valor de parte del perfil analizado.

## 4.2 Modelo de ataque SAMSON

En este caso de estudio se elige uno de los perfiles analizados y se presume que el Ingeniero Social eligió a esta persona de entre varias de una organización para obtener información de valor y que su objetivo principal sea el acceso informático a la red de la organización. Con estos antecedentes, el Ingeniero Social logra identificar el perfil de la víctima en Facebook y realiza el análisis en base al modelo propuesto (Figura 4-3).

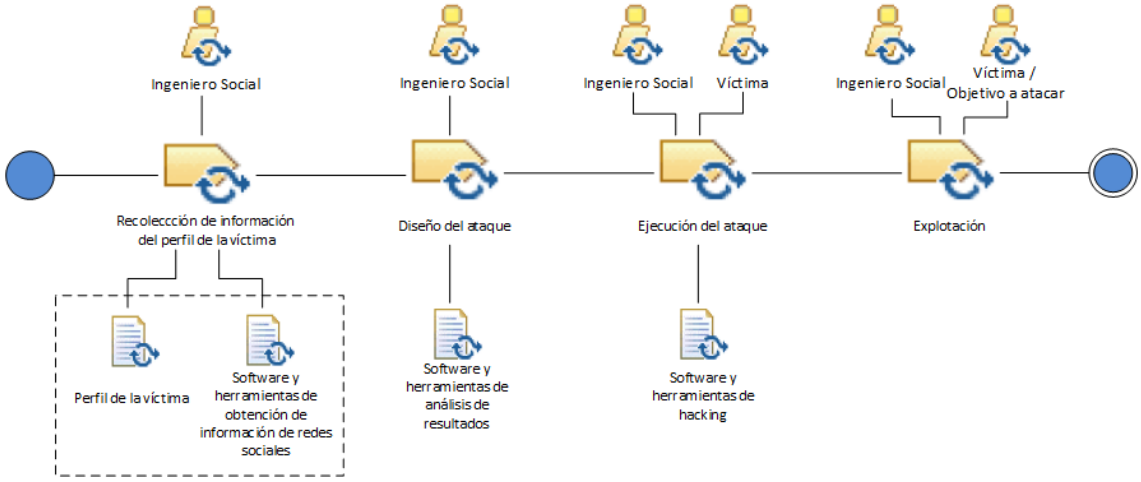



*Figura 4-3. Modelo SAMSON.*

Para las pruebas que se hicieron para verificar el modelo se solicitaron personas miembros de una misma organización, a las cuales se les solicitó los siguientes datos: URL de perfil en Facebook y correo electrónico personal. También se les informó que se iban a realizar pruebas en sus perfiles personales, solicitando permiso a través de un consentimiento informado y se les dio instrucciones para que sigan utilizando la red de manera habitual. También se les indicó que este ejercicio no iba a comprometer su información personal ni datos privados. En total participaron 9 individuos elegidos al azar entre los miembros con perfiles personales en Facebook.

| | | |
|---|---|---|
| **Rol** | *Ingeniero Social* | Profesional ético de seguridad de la información encargado de ejecutar las acciones relacionadas a la recolección de información del perfil de la víctima. |
| | *Víctima* | Community Manager o individuo dueño de la cuenta personal de Facebook. En este paso el rol de la víctima es necesario ya que las acciones de la misma serán las que definan el éxito de los pasos anteriores. |
| | *Objetivo a atacar* | Si el objetivo es la misma víctima, se reemplaza el rol, sin embargo, una víctima puede ser la puerta de entrada hacia el verdadero objetivo de un ataque, ya sea si el objetivo es una persona o una organización. |
| **Producto de trabajo** | *Perfil de la víctima* | El nombre de usuario o URL correspondiente al perfil personal del individuo objetivo |
| | *Software y herramientas de obtención de información de redes sociales* | Para este caso se utilizó NodeXL Pro v1.0.1.386, Gephi v0.9.1 y Facebook Graph API Explorer. Se sugieren las aplicaciones mencionadas, pero no se limitan a ellas |

| | | |
|---|---|---|
| | *Software y herramientas de análisis de resultados* | Dependiendo del número de nodos obtenidos en el primer paso, si resulta demasiado grande el grafo formado entre individuos y organizaciones de la víctima, podría ser imprescindible software de procesamiento de grandes volúmenes o incluso un procesamiento en la nube. Sin embargo, para este caso de estudio se utilizó NodeXL Pro v1.0.1.386, Gephi v0.9.1 y R-3.4.1, todos ellos tienen algoritmos de clustering, necesarios para un diseño efectivo. |
| | *Software y herramientas de hacking* | Aquí serán necesarios: un hosting web, dominio, direcciones falsas, diccionarios de datos, números de celular falso y otras que permitan ejecutar procedimientos de phishing, llamadas y sobre todo evitar dejar rastros. |

*Tabla 4-4. Definiciones para Modelo SAMSON*

### 4.2.1 Recolección de información del perfil de la víctima

Con el Graph API de Facebook se obtiene el ID del perfil a analizar, con el ID es posible obtener datos de valor e información que conste como pública en el perfil: nombre completo, rango etario, fecha de nacimiento, dispositivos, lista de instituciones educativas, correo electrónico, género, lugar de nacimiento, lugar de residencia, idiomas, localización, afinidad política, estado de relación conyugal, religión, lista de deportes, lista de lugares de trabajo, sitio web e imágenes como foto de perfil y foto de portada. Si al perfil se lo identificara como un nodo, las aristas que desembocarían en otra información que brinda Facebook son las siguientes: amigos, libros, álbumes, eventos, familiares, juegos, grupos, páginas que le gusta (likes), películas, música, fotos en las que aparece etiquetado, programas de televisión, lugares que ha visitado y todas las publicaciones del perfil personal (timeline).

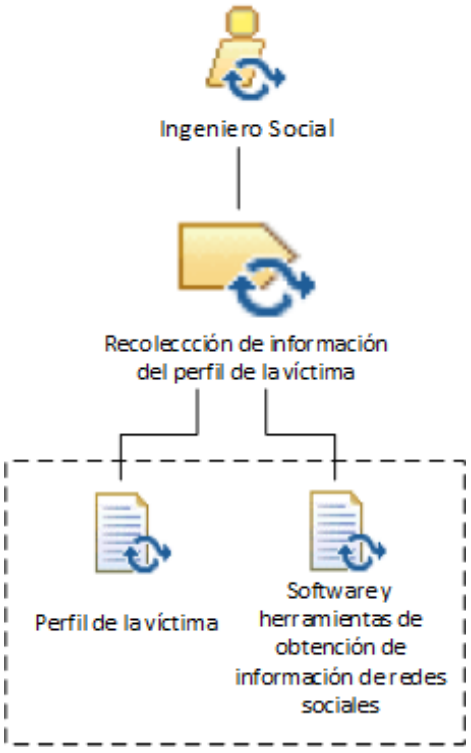



*Figura 4-4. SAMSON. Paso 1. Recolección de información del perfil de la víctima.*

Los ejemplos de grafos obtenidos con datos de valor se visualizaron en la Figura 4-1 y Figura 4-2. En base a estas relaciones e información el Ingeniero Social identifica lazos fuertes y lazos débiles para el siguiente paso. Para la identificación en el caso de que sean demasiados datos, se puede apoyar en las métricas que NodeXL calcula para cada uno de los vértices en base a todo el grafo. En la Tabla 4-5 se puede ver una muestra de las métricas calculadas por NodeXL con los mismos datos la Figura 4-2. Estas métricas permiten al ingeniero social identificar nodos que puedan ser considerados para un test de suplantación de identidad.

| Vertex | Degree | Betweenness Centrality | Closeness Centrality | Eigenvector Centrality | PageRank | Clustering Coefficient |
|---|---|---|---|---|---|---|
| **A** | 3 | 0.000 | 0.010 | 0.022 | 0.606 | 1.000 |
| **B** | 6 | 44.660 | 0.012 | 0.035 | 1.119 | 0.667 |
| **C** | 2 | 0.000 | 0.010 | 0.010 | 0.461 | 1.000 |
| **D** | 1 | 0.000 | 0.009 | 0.007 | 0.296 | 0.000 |
| **E** | 1 | 0.000 | 0.008 | 0.006 | 0.301 | 0.000 |
| **F** | 1 | 0.000 | 0.009 | 0.006 | 0.300 | 0.000 |
| **G** | 1 | 0.000 | 0.009 | 0.006 | 0.300 | 0.000 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **H** | 1 | 0.000 | 0.006 | 0.001 | 0.362 | 0.000 |
| **I** | 28 | 317.596 | 0.016 | 0.079 | 4.965 | 0.169 |
| **J** | 4 | 0.533 | 0.010 | 0.012 | 0.819 | 0.833 |
| **K** | 7 | 15.600 | 0.011 | 0.024 | 1.322 | 0.381 |
| **L** | 4 | 0.533 | 0.010 | 0.012 | 0.819 | 0.833 |
| ... | | | | | | |

*Tabla 4-5. Métricas calculadas por NodeXL para los vértices de un grafo*

Se utiliza el Graph API Explorer para obtener información adicional sobre el objetivo y se cataloga y organiza de acuerdo a los descubrimientos. Esta información puede incluir:

- Respuestas a publicaciones. Conocidas como *comentarios*, estos pueden incluir datos como: texto, fecha, hora, foto, video, enlace y menciones a otros usuarios.
- Publicaciones en otros perfiles o páginas.
- Publicaciones en la línea de tiempo (perfil o *timeline*): Estos pueden incluir características adicionales indicando el tipo de publicación como: logro, hito, mudanza, etc. Del mismo modo estas pueden tener datos o acciones de otras funcionalidades de la red social como: invitación a eventos, juegos, búsqueda de recomendaciones, entre otros.

### 4.2.2 Diseño del ataque

El Ingeniero Social puede identificar círculos sociales en el grafo (McAuley & Leskovec, 2014) de tipo clúster, que tengan una relación en particular para orientar el ataque de manera más efectiva; descubriendo así grupos de amigos que no se hayan identificado únicamente por los lazos interpersonales analizados. El objetivo de encontrar lazos débiles sirve para realizar ataques de suplantación de identidad. Todo el proceso de usar la información de diferentes fuentes se la conoce como inferencia (Oriyano, 2016), aunque podría en algunos casos resultar información abundante, en ese caso se pueden utilizar técnicas propias del Ingeniero Social para saber identificar una arista que pueda ser usada.

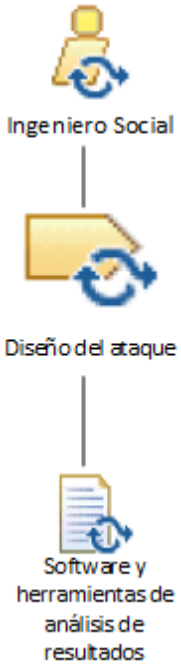



*Figura 4-5. SAMSON. Paso 2. Diseño del ataque*

Otros datos necesarios para la planeación es la identificación de clústeres en los horarios de los posts, generalmente conocido como “horas pico” de posts basados en los comentarios emitidos o en el timeline, esto se lo puede obtener según las recomendaciones de NodeXL (Hansen, Shneiderman, & Smith, 2011), del mismo modo se identifican clústeres con algoritmos, esto nos da un indicio de en qué horario y en qué día de la semana, el individuo utiliza la red social con más frecuencia o está en línea, así como los horarios a las que no hace uso de la misma. Esta información orientaría una prueba que se le ha llamado “ataque de lazo fuerte”, por ejemplo: un individuo A (víctima) generalmente publica los días lunes entre las 07h00 y 10h00 y un individuo B muy conocido del individuo A (lazo fuerte) que no trabaja en la misma organización generalmente publica los días lunes en la noche entre las 18h00 y las 21h00; el ataque consistiría suplantar la identidad del individuo B para contactar con el individuo A, un lunes entre las 07h00 y las 10h00.

Para el fin de esta investigación se utilizarán enlaces tipo phishing, únicamente de rastreo de la ejecución positiva de la acción y luego de obtener el dato, la página del enlace realiza una redirección de regreso hacia la red social (Figura 4-6). Este proceso puede llegar a ser transparente para el usuario y no tendrá afectación alguna en el dispositivo o perfil de la víctima.

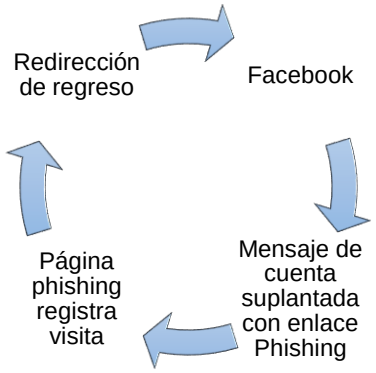



*Figura 4-6. Phishing con spoofing*

Para el análisis usando phishing mediante spoofing, se utilizará la información del grafo obtenido, de las aristas entre el individuo y las páginas combinado con el tipo de relación entre otros individuos y las mismas páginas. Por ejemplo: El individuo A tiene un lazo fuerte con una página X y un individuo B tiene un lazo fuerte también con la página X, se crea contenido en el mensaje que se envía desde la cuenta suplantada haciendo mención a la página X, pueda ser esta un lugar de estudio, un lugar de trabajo o una afición en particular.


*Figura 4-7. Ejemplo de correo phishing que pretende ser una notificación de Facebook.*

De igual manera, se elabora un texto y diseño de un correo electrónico, alusivo a la página X o individuo B con el formato de notificaciones por correo de Facebook (Figura 4-7) para ser enviado a la víctima.

### 4.2.3 Ejecución del ataque

El Ingeniero Social tiene ya los datos e información para iniciar las pruebas. Iniciando con la creación de al menos tres perfiles de suplantación de identidad de tipo lazo débil a los que llamaremos AD, BD y CD. Estos perfiles empiezan a agregar amistades no relacionadas con lazos fuertes con el individuo al cual se está suplantando, incluye amistades entre las cuentas nuevas, esto con el objetivo de tener amistades en común para el momento de contactar con el perfil a analizar. De igual manera, se crea un único perfil de lazo fuerte al que llamaremos AF. En este procedimiento se utilizaron cuatro líneas de telefonía móvil prepago de un Operador Móvil Virtual (OMV) local para activar los perfiles y que no sean suspendidos por Facebook (Facebook Inc., 2017). La creación de los perfiles se llevó a cabo tres semanas antes de contactar con la víctima, para darle un tiempo de antigüedad al perfil creado para que el mensaje no sea filtrado por los sistemas de Facebook (Facebook, 2017) y llegue a la bandeja principal de mensajes. Cabe destacar que, a la fecha de elaboración de este escrito, la plataforma de mensajería de Facebook llamada Messenger ha implementado un nuevo sistema de recepción de mensajes, en donde ha creado una nueva bandeja para mensajes recibidos de usuarios que no tienen relación de amistad con el destinatario. Esto reduciría la efectividad de un mensaje de phishing de una cuenta suplantada de tipo lazo fuerte.


*Figura 4-8. SAMSON. Paso 3. Ejecución del Ataque.*

Para la auto publicación a las horas descubiertas en el paso 2, se creó una aplicación en Facebook que tenía los permisos de publicación y mensajería en los perfiles AD, BD, CD y AF; la aplicación verificaría el estado en línea de la víctima según su ID y notifica al Ingeniero Social para que el contacto (publicación o mensaje) se lo haga en forma manual.

Con los datos obtenidos en el paso 2, se utilizó la plataforma de publicidad Facebook Ads, segmentando de manera muy detallada para que la víctima se encuentre dentro del *target* o grupo objetivo definido en la publicidad creada. Se creó una campaña publicitaria en donde se invitó al usuario a instalar una aplicación con mensajes alusivos a las páginas que le gustan y lugares que ha visitado. Se sigue el mismo procedimiento (Figura 4-6) de únicamente registrar la acción y redireccionar al usuario de regreso a la red social.

Para tener diversificación y medir qué tipo de mensaje e imagen incluidos en la publicidad, se utilizó *Split Testing*, que consta en enviar dos o más comunicaciones distintas hacia el mismo grupo objetivo. Para esa campaña, no sólo se espera tener el registro de acción de la víctima sino de otros usuarios que se encuentren dentro del target definido, según la segmentación, los usuarios de la red a los que llegaría la publicidad era un máximo de 150 perfiles. En los resultados finales de la campaña que

duró 2 días, que fue el tiempo máximo para realizar todas las pruebas que se hicieron mediante Facebook, hicieron clic 13 personas, de las cuales sólo 5 fueron del grupo seleccionado para estas pruebas.

Para el envío de *phishing* se utilizó como destinatario la dirección de correo obtenida en el paso 1, el tiempo establecido para el retorno efectivo de esta prueba fue de 5 días, luego de 5 días de ser enviado el correo electrónico, si la víctima realizó una acción positiva, la misma no fue contabilizada en los resultados totales. También se realizó un envío que intentaba ser un *scareware*, una supuesta solución de software que invitaba a ser instalada en los equipos ante una falsa amenaza.


Gmail

**Un mensaje importante sobre la seguridad de tu cuenta**
1 mensaje

5 de agosto de 2017, 14:29
Para:

Estimados compañeros/as

El día 1/8 hemos sufrido un ataque externo que comprometió la seguridad de nuestras bases de datos. Ese mismo día hemos actuado reforzando la seguridad y evitando que se extienda el problema, pero es probable que los atacantes se hayan hecho con la base de datos que contiene direcciones de email y contraseñas encriptadas. No han sido comprometidos números telefónicos ni credenciales de acceso, como así tampoco direcciones del sistema de correo Quipux.

**Hemos tomado estas medidas para proteger a nuestros usuarios:**

- Forzamos un reseteo de contraseña para todos los usuarios potencialmente afectados. Por este motivo te pedimos que ingreses a la intranet con tus datos de acceso habituales para crear una nueva contraseña. Si no te pide nueva contraseña, tu cuenta está a salvo.
- Es necesario y urgente instalar una actualización del antivirus en sus equipos de trabajo para evitar que la infección se propague en la red. **DESCARGAR**
- Estamos trabajando en una solución para pedirle a los usuarios que proactivamente actualicen sus direcciones de email vinculadas al sistema de rol de pagos.
- Seguimos trabajando para mejorar nuestros sistemas que detectan y previenen accesos no autorizados a nuestras cuentas de usuarios.

*Figura 4-9. Ejemplo de correo scareware que invita a descargar una supuesta actualización.*

En la prueba de *scareware*, se utilizó como remitente una dirección ficticia del lugar de trabajo de la víctima, fingiendo ser los administradores de la red o de sistemas y para el enlace “DESCARGAR” se utilizó una página que registraba la visita y hacía

redirección (Figura 4-6), que, en lugar de regresar a la red social, enviaba a instalar un antivirus gratuito.

Las llamadas de tipo vishing (Ollmann, 2007) fueron realizadas en un intervalo separado de 4 días, para esto se simuló ser en la primera iteración una persona del lugar de trabajo y para la segunda iteración un agente de cuenta bancaria o un agente vendedor de una operadora móvil. En las dos iteraciones en primera instancia se les solicitó el número de cédula de identidad, conocido previamente para validación en caso de cuestionamiento, y dependiendo de la interacción en la llamada se le llegaba a pedir el nombre completo, la dirección de correo electrónico, horario que sea mejor para contactarle (fuera del horario laboral) y finalmente la dirección del domicilio y si una persona estaría en el sitio para recibir ofertas, cupones y promociones.

Las pruebas ejecutadas daban éxito en más de una ocasión, por lo que se estableció un máximo de 2 iteraciones positivas para todas las pruebas realizadas.

### 4.2.4 Explotación


*Figura 4-10. SAMSON. Paso 4. Explotación*

El modelo expuesto es únicamente de análisis, los procedimientos realizados han respetado la privacidad y seguridad de los 9 individuos participantes, quienes estuvieron conscientes del nivel de alcance de las pruebas; y, ya que esta prueba simula las fases de un ataque, tienen únicamente fines investigativos y no maliciosos, la explotación de la información obtenida no representa un objetivo de nuestro estudio por lo que aquí irían las acciones finales del Ingeniero Social contra el individuo o la organización (objetivo a atacar) según los resultados obtenidos del paso 3, ya sean éstos la infección de un dispositivo, extracción de información sensible, utilización de credenciales, entre otros.

### 4.2.5 Resultados

Con los resultados de la información obtenida en el primer paso, se diseñaron pruebas específicas según los lazos interpersonales obtenidos de cada individuo y sus amigos, así como según los clústeres. Las pruebas se realizaron bajo la modalidad de hacking ético en un máximo de 2 iteraciones por ejecución correcta a 9 perfiles controlados.

| Ataque | Víctimas | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | *P1* | *P2* | *P3* | *P4* | *P5* | *P6* | *P7* | *P8* | *P9* | *TOTAL* |
| Phishing vía publicación de perfil lazo débil | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 2 | 0 | 4 |
| Phishing vía publicación de perfil lazo fuerte | 1 | 2 | 2 | 1 | 2 | 2 | 0 | 2 | 1 | 13 |
| Phishing vía mensaje de perfil lazo débil | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | 11 |
| Phishing vía mensaje de perfil lazo fuerte | 2 | 0 | 2 | 0 | 2 | 1 | 1 | 0 | 0 | 8 |
| Phishing vía correo electrónico | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | 1 | 5 |
| Instalar aplicación maliciosa mediante publicidad dirigida | 2 | 1 | 0 | 0 | 2 | 1 | 2 | 0 | 0 | 8 |
| Scareware vía correo electrónico | 0 | 1 | 1 | 0 | 1 | 1 | 2 | 0 | 1 | 7 |
| Vishing vía llamada | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 2 |
| TOTAL | 7 | 6 | 7 | 2 | 11 | 7 | 8 | 6 | 4 | |

*Tabla 4-6. Resultados de aplicación de SAMSON.*

Según la Tabla 4-6, se infieren índices de mayor recurrencia en determinados ataques, así como los distintos comportamientos de las víctimas y su vulnerabilidad ante los distintos ataques, además de que estos índices indicarían la correcta ejecución del paso 4, lo que supondría un alto riesgo para el individuo o para la organización, que, a pesar de tener controles técnicos establecidos o seguir las recomendaciones establecidas en estándares de seguridad de la información; la ingeniería social con el apoyo de las redes sociales, sería un método no técnico muy efectivo, por lo cual debería considerarse por parte de los Directores de Tecnología y Oficiales de Seguridad de la Información de una organización el establecer normativas del uso de las redes sociales dentro y fuera de la organización así como evaluar perfiles de redes sociales.

# Capítulo 5. Método de evaluación de la seguridad según el uso de una red social

En este capítulo se diseña el proceso de evaluación que se debería aplicar a cada perfil, este método busca verificar el uso seguro o no que un miembro de una red social haga de la misma. Este proceso es recomendado por la firma de seguridad Kaspersky a las organizaciones, indica que se debe evaluar perfiles de redes sociales para valorar el riesgo al que se exponen sus usuarios ante ataques de ingeniería social (Esposito, 2016).

Si bien los creadores de sistemas de redes sociales en línea (por ejemplo Facebook), han tomado medidas para precautelar la seguridad y privacidad acorde a estándares internacionales y políticas de privacidad que rigen a nivel de los países donde se aplican y a inversión en investigación para aplicar las técnicas necesarias y procedimientos específicos que garanticen que la solución de software cumple los parámetros de seguridad y de calidad necesarios; el inconveniente detectado en dichas redes que aplican estas medidas, denota que no es el software el que tiene un inconveniente de seguridad, sino es el uso incorrecto y la sobre exposición de datos personales lo que permite que existan brechas de privacidad. Haciendo una analogía con la seguridad de ingreso a una casa: si la puerta de entrada es totalmente de metal, tiene cerradura con llave y además candado con combinación numérica, no sirven de nada si el usuario dueño de casa no pone candado ni cierra la puerta correctamente. Lo mismo sucede en Facebook, si un usuario no hace uso adecuado de la red social, expone su información a terceros que no están autorizados a conocerla o usuarios que harían uso malintencionado de los datos publicados.

## 5.1 Método de evaluación ISASNET

Al no contar con módulos de evaluación que contengan especificaciones, características y métricas que evalúen la seguridad de un sistema acuerdo al uso, se propone un método basado en los resultados del caso de estudio con el modelo SAMSON y en la bibliografía presentada en el Capítulo 3. A esta propuesta se le ha puesto el nombre de ISASNET (*Information Security Assessment on Social Networks*).

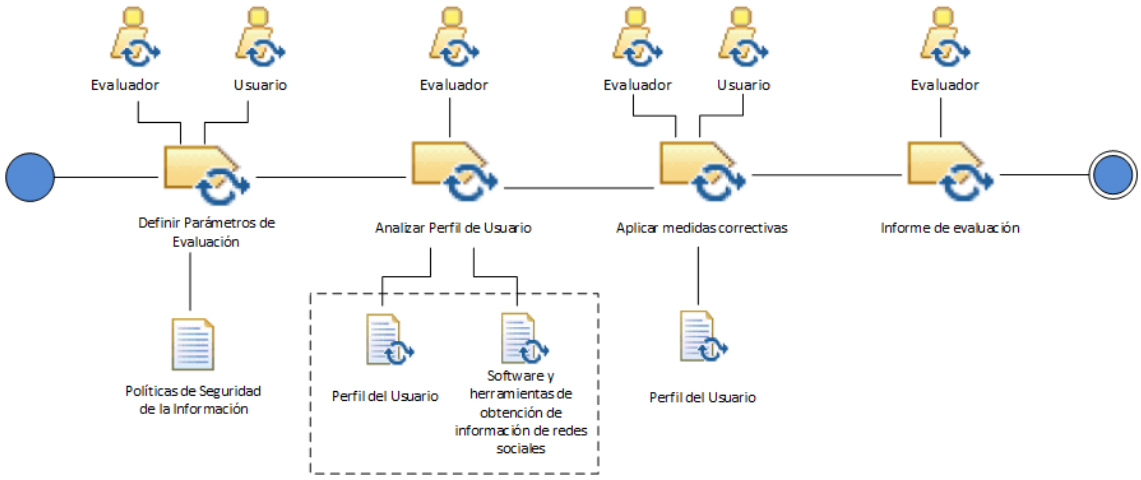



*Figura 5-1. Proceso total de ISASNET.*

| | | |
|---|---|---|
| **Rol** | *Evaluador* | Profesional de seguridad de la información perteneciente a la organización, puede ser el CISO (*Chief Information Security Officer*) en el caso de que existiera. |
| | *Usuario* | Persona que usa a nombre propio o community manager de la página que administre. |
| **Producto de trabajo** | *Políticas de Seguridad de la Información* | Este producto además de incluir las Políticas de Seguridad de la Información aprobadas, debe incluir también la documentación relacionada a la Clasificación de la Información, tanto de la organización como de la dependencia a la cual pertenezca el usuario. |
| | *Perfil del usuario* | El nombre de usuario o URL correspondiente al perfil personal del individuo a analizar |
| | *Software y herramientas de obtención de información de redes sociales* | Para este caso se utilizó NodeXL Pro v1.0.1.386, Gephi v0.9.1 y Facebook Graph API Explorer. Se pueden utilizar además herramientas de big data y procesamiento en la nube, entre ellas está: Oracle Social Cloud |

*Tabla 5-1. Definiciones para Metodología ISASNET*

### 5.1.1 Definir parámetros de evaluación

El primer paso es que la organización defina lo que considera información privada, sensible y confidencial de acuerdo a las políticas de seguridad de la información y a documentación de clasificación de la información.


*Figura 5-2. ISASNET. Paso 1. Definir parámetros de evaluación.*

Por otra parte, en un acuerdo entre la organización y el usuario se definirá qué información debería considerarse privada para el usuario como persona civil y que no deba ser expuesta en redes sociales por seguridad personal. Estos datos e información serán llevados a manera de indicadores a una matriz con el formato propuesto (Tabla 5-2), el formato es una muestra y sirve de ejemplo para la elaboración, no es definitiva ni limitada; también se especifican los pasos 3 y 4 referentes a configuraciones de privacidad y configuraciones de seguridad esperadas en el perfil del usuario.

| Dimensión | Descriptores | Detalle | Indicador | Nivel de riesgo B | M | A |
|---|---|---|---|---|---|---|
| Información organización | Datos de la organización | Infraestructura de red | | | | |
| | | Nombre de un servidor de base de datos | | | | |
| | Datos del departamento | Ubicación de la oficina | | | | |
| | | Seguridad de la oficina | | | | |
| | | Miembros pertenecientes | | | | |
| | Datos del empleado | Correo electrónico del trabajo | | | | |
| | | Número de celular del trabajo | | | | |
| | | Extensión telefónica | | | | |
| | | Tarjeta de Identificación | | | | |
| | | Dirección IP | | | | |
| | | Nombre de usuario | | | | |
| | | Contraseña | | | | |
| | … | … | | | | |
| Información personal | Datos personales y/o familiares (Tabla 4-1) | Número de identificación (Cédula) | | | | |
| | | Correo personal | | | | |
| | | Número de celular | | | | |
| | | Número de cuenta bancaria | | | | |

| | | |
|---|---|---|
| | Datos de familiares | Nombres de Padres, cónyuge, hijos |
| | Datos de vivienda y pertenencias | Ubicación |
| | | Seguridad |
| | | Objetos de valor |
| | | Ausencia |
| | … | … |
| **Privacidad** | Perfil | Quién puede ver publicaciones |
| | | Quién puede enviar solicitudes de amistad |
| | | Quién puede encontrarle con la dirección de correo |
| | | Quién puede encontrarle con el número de teléfono |
| | | Se encuentra el perfil en motores de búsqueda |
| | | Quién puede publicar en el perfil |
| | | Quién puede etiquetarle en fotos |
| | | Quien puede ver las fotos en las que está etiquetado |
| | | Habilitado reconocimiento facial para fotos subidas |
| | Amistades | Quién puede ver la lista de amistades |
| | | Desconocidos en lista de amigos |
| | | Usa listas de amigos |
| | | Amigos con acceso restringido |
| | | Amigos o perfiles bloqueados |
| | Aplicaciones | Aplicaciones desconocidas con acceso |
| | | Aplicaciones bloqueadas |
| | Páginas | Páginas bloqueadas |
| | | Administrador de página |
| | Información para anunciantes (publicidad) | Rastreo de páginas web |
| | | Aplicaciones |
| | | Acciones sociales |
| | | Estado civil |
| | | Lugar de trabajo |
| | | Puesto en el trabajo |
| | | Lugares de estudio |
| | | Intereses |
| **Seguridad** | Inicio de sesión | Lugares donde ha iniciado sesión |
| | | Dispositivos que no requieren 2FA |
| | | 2FA: Mensaje de texto a celular |
| | | 2FA: Llave USB o NFC |
| | | 2FA: Generador de códigos |
| | | Alertas de inicios no autorizados |
| | | Amigos de confianza designados |
| | | Contraseña fuerte |
| | | Contraseña usada en otros servicios |
| | | No usa correo institucional |
| | | Códigos de recuperación |
| | Otras configuraciones | Cifrado de correos electrónicos |
| | | Contraseñas de un uso para aplicaciones |
| | | Métodos de pago, Tarjetas de Crédito |

*Tabla 5-2. Matriz de evaluación de privacidad y seguridad del perfil.*

### 5.1.2 Analizar perfil de usuario

Para este paso se hacen análisis manuales y automatizados con herramientas de software para visualizar y extraer publicaciones realizadas por el perfil del usuario en búsqueda de datos según los parámetros de evaluación establecidos y se llena la Tabla 5-2 para la aplicación de medidas correctivas o elaboración de un informe según corresponda.

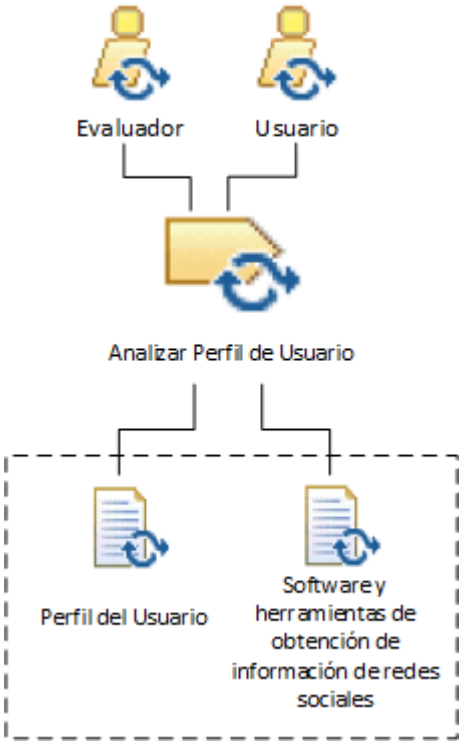



*Figura 5-3. ISASNET. Paso 2. Analizar perfil del usuario*

El evaluador realizará un proceso similar al que realiza el Ingeniero Social en el primer paso de SAMSON (Capítulo 4.2.1), adicional a esto, conjuntamente con el usuario, se verificará a modo de lista de chequeo las configuraciones de privacidad, seguridad y publicidad que el usuario tenga en el perfil.

### 5.1.3 Aplicar medidas correctivas

El evaluador establecerá el nivel de riesgo de cada una de las evidencias encontradas y solicitará al usuario las acciones requeridas en el perfil de la red social analizada (Figura 5-4).


*Figura 5-4. ISASNET. Paso 3. Aplicar medidas correctivas.*

El evaluador solicitará al usuario ejecutar las acciones correctivas, para ello se sigue el siguiente árbol de decisión establecido (Figura 5-5) y se escribe en el informe las decisiones tomadas por el usuario.

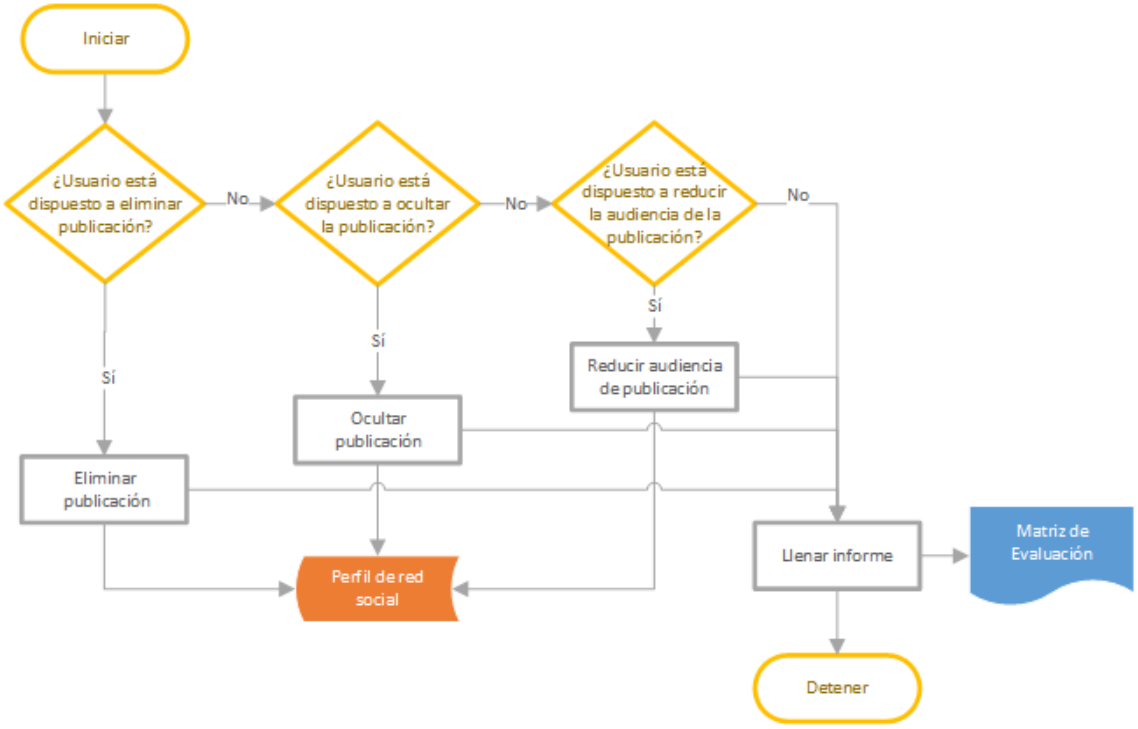



*Figura 5-5. Árbol de decisión para publicaciones.*

La publicación que tenga información sensible con criticidad Alta deberá ser eliminada, otras publicaciones con criticidad media o baja serán consideradas por el evaluador la acción correctiva a tomar. Para el análisis se consideran todas las publicaciones o contenido que tenga configurado la privacidad como: “Público”, ya que, de este modo, todas las personas dentro o fuera de la red social podrá visualizar el contenido con la información sensible.

#### *5.1.3.1 Eliminar publicación*

Cuando sea necesario eliminar la publicación, el evaluador verificará la eliminación efectiva en el perfil del usuario o en donde haya sido encontrada la novedad, mediante el enlace obtenido manualmente o con las herramientas en el paso 2 de ISASNET.


*Figura 5-6. Eliminar publicación*

#### *5.1.3.2 Ocultar publicación*

Para la ejecución de esta tarea, el usuario deberá cambiar la privacidad de la publicación a: “Solo yo”, de este modo únicamente el usuario podrá visualizar la publicación, sin embargo, esto no excluye de que haya quedado registrado en algunos motores de búsqueda o indexadores de contenido. De igual manera, esto permitiría al usuario cambiar la privacidad a posterior y que la publicación vuelva a aparecer a todos los usuarios dentro y fuera de Facebook. Esta opción es tomada cuando el usuario desea mantener una publicación ya sea por los comentarios recibidos, por el número de Me Gusta que tiene o simplemente por vanidad, generalmente es usada esta opción cuando los miembros pertenecientes a la organización, desean volver a publicar el contenido cuando su relación laboral con la misma haya finalizado.


*Figura 5-7. Ocultar publicación*

#### *5.1.3.3 Reducir audiencia de publicación*

El usuario deberá cambiar la privacidad de publicación a una de las opciones que limiten el acceso a la misma, la opción “Público” no es válida. Las opciones válidas son: Amigos, Amigos excepto conocidos, Amigos concretos o Personalizado. De este modo, se garantiza que únicamente los amigos del usuario puedan visualizar la publicación o contenido. Esto no garantiza que el usuario haya aceptado invitaciones de amistad de desconocidos o de personas malintencionadas.


*Figura 5-8. Reducir audiencia de publicación*

Las tareas de *ocultar publicación* y *reducir audiencia de publicación* pueden realizarse a todas las publicaciones anteriores de la línea de tiempo del usuario mediante una opción implementada por Facebook llamada “Limitar publicaciones antiguas” (https://goo.gl/C9PbpX) que permite configurar masivamente la privacidad de

todas las publicaciones existentes, ya que este procedimiento llevaría demasiado tiempo si el número de incidencias detectadas en el paso 2 de ISASNET son demasiadas.

#### *5.1.3.4 Llenar informe*

El evaluador tomará nota de cada una de las acciones realizadas o no en el perfil del usuario para presentar junto a la matriz de evaluación en el siguiente paso.

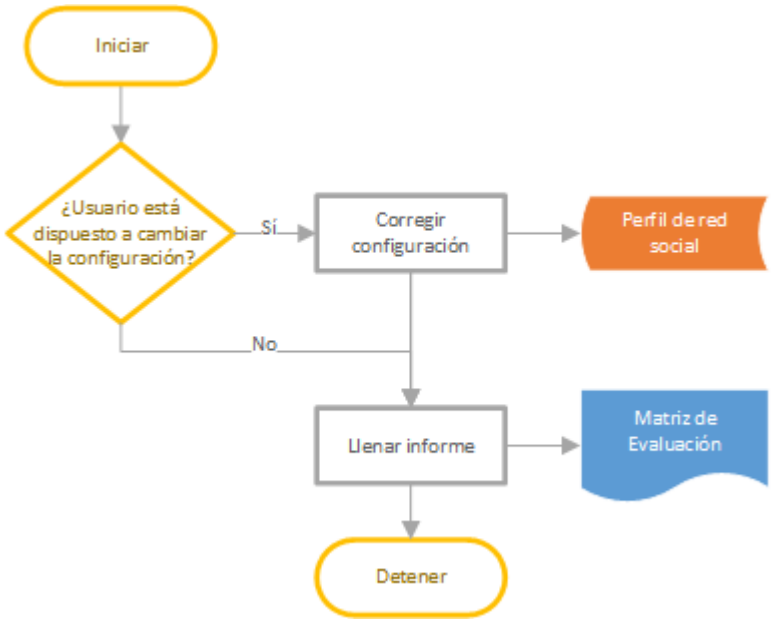



*Figura 5-9. Árbol de decisión para configuraciones.*

Según la matriz de evaluación, los puntos 3 y 4 no son relativos al contenido sino a la configuración, por lo cual se sigue el árbol de decisión para configuraciones (Figura 5-9). La mayoría de configuraciones son interruptores de encendido/apagado, activado/desactivado, y otros tienen que ver con la limitación de privacidad como en el árbol de decisión para publicaciones: Público/Amigos/Amigos de amigos/Nadie. Otros parámetros tienen que ver con el uso o no de opciones disponibles, el uso de medidas de seguridad previene la vulneración de una cuenta, estos resultados serán igualmente analizados en el siguiente paso.

### 5.1.4 Informe de evaluación

Para la realización del informe, el evaluador utilizará la matriz de evaluación y los resultados del paso 4 de ISASNET. Esto definirá el nivel de riesgo al que el perfil de un usuario está expuesto según criterio del evaluador. El informe será analizado y revisado por personal de seguridad de la información, quienes elaborarán los respectivos

informes de riesgos para que el usuario firme un documento aceptando los riesgos a los que se expondría en el caso de no haber aplicado las medidas correctivas necesarias en el paso 3 de ISASNET.


*Figura 5-10. EVASIF. Paso 4. Informe de evaluación.*

El nivel de riesgo debería ser cero, es decir, que no existan novedad alguna, sin embargo, se hará una media del nivel de riesgo dependiendo las incidencias de nivel bajo, medio y alto según las siguientes métricas.

| Parámetro | Valor |
|---|---|
| No existe riesgo | 0 |
| Riesgo bajo (B) | 1 |
| Riesgo nedio (M) | 2 |
| Riesgo alto (A) | 3 |
| Configuración privacidad: oculto | 1 |
| Configuración privacidad: limitado | 2 |
| Configuración privacidad: público | 3 |
| Corrección de configuración positiva | 0 |
| Corrección de configuración negativa | 3 |

*Figura 5-11. Métricas de evaluación del riesgo.*

Se debe realizar un informe ejecutivo que resuma los resultados realizados en perfiles de redes sociales, este informe deberá ser entregado a las máximas autoridades de la organización, quienes, junto a personal de seguridad de la información tomarán decisiones que definan procesos o procedimientos para empleados de la organización, contratistas, etc. Para el caso de estudio, personal de seguridad de la información han tomado la decisión de levantar un documento con nuevas políticas de seguridad de la información enfocado a redes sociales. Al ser este un perfil de red social de una persona,

en el país no se ha legislado correctamente al respecto para asunción de responsabilidades civiles y penales en caso de vulneraciones o mal uso, así como también la vinculación a la organización en donde el individuo labora, no se puede disponer e imponer acciones en perfiles basados en servicios de internet que no sean propiedad de la organización, sin embargo, en las páginas que sí lo son, se han aplicado medidas de seguridad basadas en el documento, al cual se lo llamó "Documento General de Buenas Prácticas de Gestión de Redes Sociales", el documento original interno ha sido actualizado en la elaboración de este trabajo y consta como ANEXO 1 de este documento.

## 5.2 Resultados

El método ISASNET ha sido realizado y aplicado a los mismos 9 perfiles en los que se aplicó el modelo SAMSON, esta revisión se ejecutó luego de aplicarse el modelo SAMSON, los resultados del paso 2 de ISASNET se exponen en la Tabla 5-3.

| **Evaluación de perfiles** | | | | **Nivel de riesgo** | | |
|---|---|---|---|---|---|---|
| **Dimensión** | Descriptores | Detalle | Indicador | B | M | A |
| **Información organización** | Datos de la organización | Documentos internos | - | | | |
| | | Datos internos | - | | | |
| | Datos del departamento | Ubicación de la oficina | Posición | 2 | | |
| | | Seguridad de la oficina | | | | 1 |
| | | Miembros pertenecientes | Foto | | | 7 |
| | Datos del empleado | Correo electrónico del trabajo | Texto | | 1 | |
| | | Número de celular del trabajo | - | | | |
| | | Extensión telefónica | - | | | |
| | | Tarjeta de Identificación | Foto | 7 | 2 | |
| | | Dirección IP | - | | | |
| | | Nombre de usuario | - | | | |
| | | Contraseña | - | | | |
| | … | … | | | | |
| **Información personal** | Datos personales y/o familiares (Tabla 4-1) | Número de identificación (Cédula) | | 1 | | |
| | | Correo personal | | | | 3 |
| | | Número de celular | | | 2 | |
| | | Número de cuenta bancaria | - | | | |
| | Datos de familiares | Nombres de Padres, cónyuge, hijos | - | | | |
| | Datos de vivienda y pertenencias | Ubicación | | | 1 | |
| | | Seguridad | - | | | |
| | | Objetos de valor | - | | | |
| | | Ausencia | | 1 | | |
| | … | … | | | | |
| **Privacidad** | Perfil | Quién puede ver publicaciones | | | | 9 |
| | | Quién puede enviar solicitudes de amistad | | | 3 | 6 |
| | | Quién puede encontrarle con la dirección de correo | | | | 8 |
| | | Quién puede encontrarle con el número de teléfono | | | | 9 |
| | | Se encuentra el perfil en motores de búsqueda | | | | 8 |
| | | Quién puede publicar en el perfil | | | 3 | 6 |
| | | Quién puede etiquetarle en fotos | | | 1 | 8 |
| | | Quien puede ver las fotos en las que está etiquetado | | | | 9 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Habilitado reconocimiento facial para fotos subidas | | | | 9 |
| | Amistades | Quién puede ver la lista de amistades | | | 3 | 6 |
| | | Desconocidos en lista de amigos | | | | 9 |
| | | Usa listas de amigos | | | | 9 |
| | | Amigos con acceso restringido | - | | | |
| | | Amigos o perfiles bloqueados | | 2 | | |
| | Aplicaciones | Aplicaciones desconocidas con acceso | | | | 9 |
| | | Aplicaciones bloqueadas | - | | | |
| | Páginas | Páginas bloqueadas | - | | | |
| | | Administrador de página | | 3 | | |
| | Información para anunciantes (publicidad) | Rastreo de páginas web | | | | 9 |
| | | Aplicaciones | | | | 9 |
| | | Acciones sociales | | | | 9 |
| | | Estado civil | | | | 9 |
| | | Lugar de trabajo | | | | 9 |
| | | Puesto en el trabajo | | | | 9 |
| | | Lugares de estudio | | | | 9 |
| | | Intereses | | | | 9 |
| **Seguridad** | Inicio de sesión | Lugares donde ha iniciado sesión | | | | 6 |
| | | Dispositivos que no requieren 2FA | | | | 8 |
| | | 2FA: Mensaje de texto a celular | | | | 8 |
| | | 2FA: Llave USB o NFC | | | | 9 |
| | | 2FA: Generador de códigos | | | | 8 |
| | | Alertas de inicios no autorizados | | | | 8 |
| | | Amigos de confianza designados | | | | 9 |
| | | Contraseña fuerte | | 1 | 5 | 2 |
| | | Contraseña usada en otros servicios | | | | 3 |
| | | No usa correo institucional | | | 1 | |
| | | Códigos de recuperación | | | | 9 |
| | Otras configuraciones | Cifrado de correos electrónicos | | | | 9 |
| | | Contraseñas de un uso para aplicaciones | | | | 9 |
| | | Métodos de pago, Tarjetas de Crédito | | | | 3 |

*Tabla 5-3. Resultados de paso 2 de ISASNET a 9 perfiles*

Analizando todos los resultados (Figura 5-12), se determina que en general existe un porcentaje considerable de riesgo de los perfiles analizados, y entre las métricas de riesgo, el riesgo alto es el que ocurre al menos en la mitad de los perfiles.

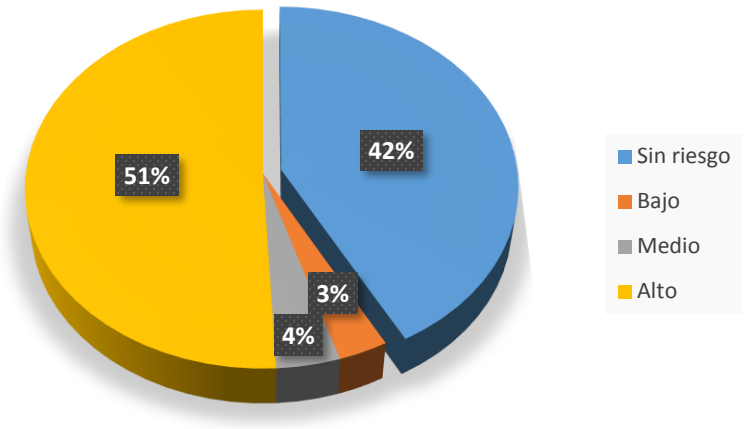



*Figura 5-12. Niveles de riesgo de los perfiles revisados con EVASIF*

Analizando por la dimensión de información de la organización (Figura 5-13), el nivel de riesgo es muy bajo, esto nos indica que los usuarios, de cierto modo, están conscientes de que no deben exponer o publicar lo que es considerado como información sensible por la organización, o datos de la información que puedan poner en riesgo a la misma o al individuo.

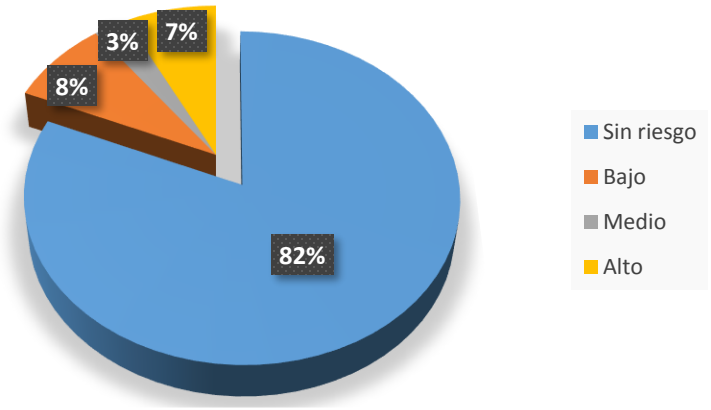



*Figura 5-13. Niveles de riesgo de la Dimensión 1.*

Revisando la dimensión de información personal (Figura 5-14), el nivel de riesgo es aún más bajo que la dimensión de información de la organización. Esta diferencia, aunque no significativa, nos indica que, la preocupación del usuario final en cuanto a datos que publican en las redes es un poco más amplia y de más cuidado, algunos de

los usuarios al ser consultados acerca de esta diferencia indicaron que, en caso de un ataque al perfil, los involucrados o afectados serían directamente los dueños de las cuentas, no ocurriendo así con cuentas que pertenecen a la organización, generalmente el objetivo no es el individuo sino la organización.

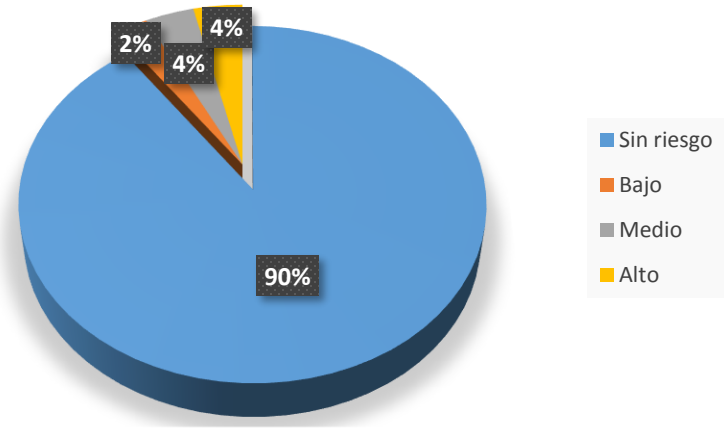



*Figura 5-14. Niveles de riesgo de la Dimensión 2*

Las dimensiones de configuraciones, como era de esperarse, presentan altos índices de riesgos (Figura 5-15), esto debido a que, cuando se tomó la muestra para el caso de estudio, se requería de perfiles cuyas configuraciones no hayan sido alteradas desde que crearon la cuenta en Facebook. En esta dimensión el 100% de los perfiles revisados no había cambiado la configuración para anunciantes, esta configuración permite a los publicistas que utilizan Facebook Ads como plataforma para crear campañas hacia usuarios de la red, los anunciantes pueden filtrar datos específicos de los usuarios a los que desean llegar con anuncios, de este modo, según se realizó una prueba con SAMSON, es posible tener muchas especificidades para que alguien con dinero que invertir en publicidad con fines maliciosos, pueda tener éxito.

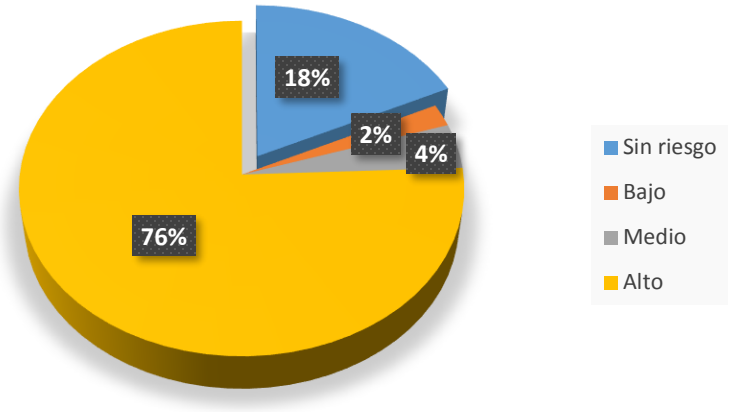



*Figura 5-15. Niveles de riesgo de la Dimensión 3.*

En la revisión de las configuraciones de seguridad (Figura 5-16), se pueden apreciar valores muy cercanos a los riesgos analizados en la Dimensión 3 (Figura 5-15). Y, aunque el riesgo alto de configuraciones de seguridad es más bajo que el analizado en la Dimensión 3, el nivel de configuraciones correctas (sin riesgo) es mayor a los perfiles sin riesgo de la Dimensión 3. La mayoría de riesgo existe en las configuraciones de segundo factor de autenticidad en el inicio de sesión. Únicamente un perfil tenía habilitado esta opción, sin embargo, como 2FA existen varias posibilidades, pero la más común en sistemas en internet es la confirmación mediante un código OTP enviado por mensaje de texto a un teléfono móvil propiedad del dueño de la cuenta. Otro método 2FA usado comúnmente es el Generador de códigos. El usuario de la red social tiene instalada la aplicación de Facebook en su dispositivo móvil, y cuando inicia sesión en otro dispositivo o mediante el navegador, debe ingresar un código aleatorio y cambiante que se obtiene de la aplicación.

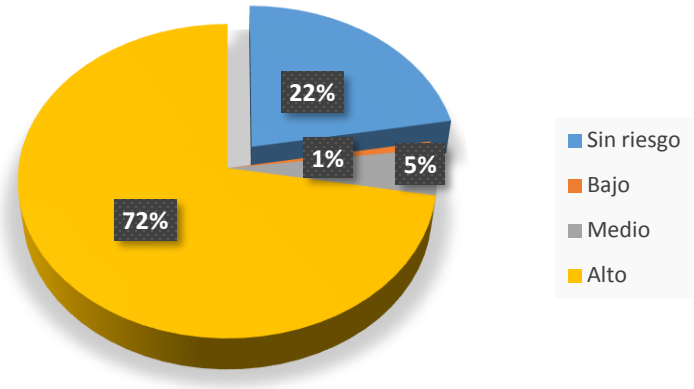



*Figura 5-16. Niveles de riesgo de la Dimensión 4.*

Los resultados de todo el proceso de ISASNET, es decir, luego de que se aplicaran las medidas correctivas en los perfiles, se presentan en la siguiente tabla:

| **Evaluación de perfiles** | | | | **Nivel de riesgo** | | |
|---|---|---|---|---|---|---|
| **Dimensión** | Descriptores | Detalle | Indicador | B | M | A |
| **Información organización** | Datos de la organización | Documentos internos | - | | | |
| | | Datos internos | - | | | |
| | Datos del departamento | Ubicación de la oficina | Posición | | 2 | |
| | | Seguridad de la oficina | | | | |
| | | Miembros pertenecientes | Foto | | 5 | 2 |
| | Datos del empleado | Correo electrónico del trabajo | - | | | |
| | | Número de celular del trabajo | - | | | |
| | | Extensión telefónica | - | | | |
| | | Tarjeta de Identificación | Foto | | 1 | |
| | | Dirección IP | - | | | |
| | | Nombre de usuario | - | | | |
| | | Contraseña | - | | | |
| | … | … | | | | |
| **Información personal** | Datos personales y/o familiares (Tabla 4-1) | Número de identificación (Cédula) | - | | | |
| | | Correo personal | | 1 | | |
| | | Número de celular | - | | | |
| | | Número de cuenta bancaria | - | | | |
| | Datos de familiares | Nombres de Padres, cónyuge, hijos | - | | | |
| | Datos de vivienda y pertenencias | Ubicación | - | | | |
| | | Seguridad | - | | | |
| | | Objetos de valor | - | | | |
| | | Ausencia | - | | | |
| | … | … | | | | |
| **Privacidad** | Perfil | Quién puede ver publicaciones | | | 9 | |
| | | Quién puede enviar solicitudes de amistad | | | 5 | 4 |
| | | Quién puede encontrarle con la dirección de correo | | | 4 | 4 |
| | | Quién puede encontrarle con el número de teléfono | | | 3 | 2 |
| | | Se encuentra el perfil en motores de búsqueda | | | | 4 |
| | | Quién puede publicar en el perfil | | | 5 | |
| | | Quién puede etiquetarle en fotos | | 2 | 7 | |
| | | Quien puede ver las fotos en las que está etiquetado | | | 9 | |
| | | Habilitado reconocimiento facial para fotos subidas | | | 9 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Amistades | Quién puede ver la lista de amistades | | | 3 | 6 |
| | | Desconocidos en lista de amigos | - | | | |
| | | Usa listas de amigos | | | 1 | 8 |
| | | Amigos con acceso restringido | - | | | |
| | | Amigos o perfiles bloqueados | | 2 | | |
| | Aplicaciones | Aplicaciones desconocidas con acceso | - | | | |
| | | Aplicaciones bloqueadas | - | | | |
| | Páginas | Páginas bloqueadas | - | | | |
| | | Administrador de página | | 3 | | |
| | Información para anunciantes (publicidad) | Rastreo de páginas web | - | | | |
| | | Aplicaciones | - | | | |
| | | Acciones sociales | - | | | |
| | | Estado civil | | | | 2 |
| | | Lugar de trabajo | - | | | |
| | | Puesto en el trabajo | - | | | |
| | | Lugares de estudio | | | | 2 |
| | | Intereses | | | | 4 |
| **Seguridad** | Inicio de sesión | Lugares donde ha iniciado sesión | - | | | |
| | | Dispositivos que no requieren 2FA | | | | 4 |
| | | 2FA: Mensaje de texto a celular | | | | 2 |
| | | 2FA: Llave USB o NFC | | | | 9 |
| | | 2FA: Generador de códigos | | | | 1 |
| | | Alertas de inicios no autorizados | - | | | |
| | | Amigos de confianza designados | - | | | |
| | | Contraseña fuerte | - | | | |
| | | Contraseña usada en otros servicios | - | | | |
| | | No usa correo institucional | - | | | |
| | | Códigos de recuperación | | | | 2 |
| | Otras configuraciones | Cifrado de correos electrónicos | | | | 9 |
| | | Contraseñas de un uso para aplicaciones | - | | | |
| | | Métodos de pago, Tarjetas de Crédito | | | | 3 |

*Tabla 5-4. Resultados de ISASNET a 9 perfiles*

En una comparativa entre los riesgos detectados y las correcciones realizadas (Figura 5-17), es evidente que además de reducir ampliamente los niveles de riesgos, aún no es posible llegar a mitigarlos por completo, ya que estas acciones dependen finalmente del usuario y la organización no puede obligar a un individuo a cambiar algo que no desea, pero sí asumir el riesgo al que se expone y expone a la organización.

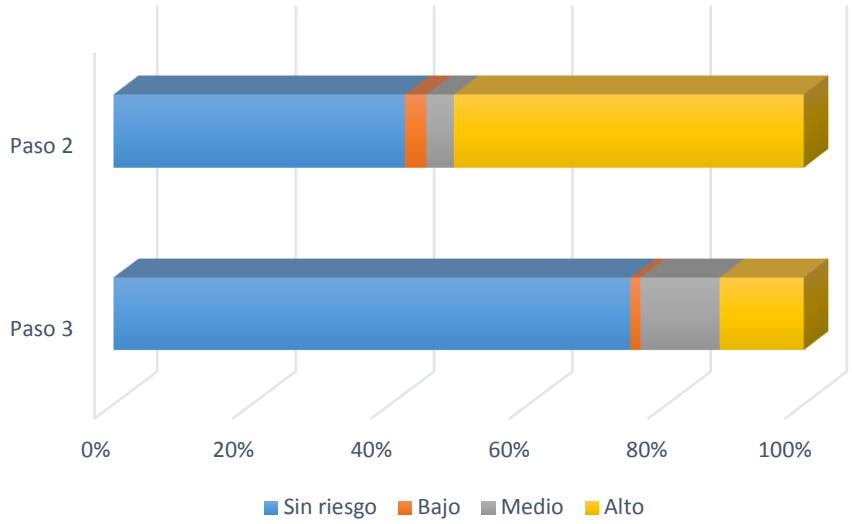



*Figura 5-17. Comparativa de resultados de ISASNET entre paso 2 y paso 3*

La aplicación del método de evaluación propuesto, ISASNET, nos permite además de obtener los niveles de riesgo, realizar las correcciones en el procedimiento. Las pruebas realizadas con SAMSON han servido de base para proponer ISASNET, la aplicación de la metodología y el modelo en un caso de estudio, han generado concienciación del riesgo al que pueden exponerse los perfiles de redes sociales, tanto para el individuo como para la organización. Algunos parámetros o datos tanto de la organización como del individuo no han sido tomados en cuenta en la matriz de evaluación, sin embargo, se han considerado los de más vulnerabilidad con resultados positivos.

# Capítulo 6. Conclusiones y trabajos futuros

## 6.1 Conclusiones

Las organizaciones usualmente emplean avanzadas técnicas de seguridad para minimizar los ataques o intentos no autorizados o maliciosos de obtener información, sin embargo, cada organización es susceptible a ataques de ingeniería social utilizando como medio a los individuos que en ella laboran, sin que los controles técnicos sean suficientes o efectivos.

El uso de redes sociales en línea se ha masificado tanto para personas como para organizaciones, y se encuentra en constante evolución, permitiendo realizar consultas en lenguaje natural, considerado como un avance hacia la web semántica; del mismo modo, permite a los usuarios de Facebook estar expuestos a varios tipos de vulneraciones como pérdida de privacidad y ataques de ingeniería social.

Con esta preocupación y motivación se elaboró un método de ataque, analizando procedimientos comunes de ingeniería social para obtener información, pero enfocado a perfiles de redes sociales, utilizando el eslabón más débil en la cadena de seguridad: la susceptibilidad humana. De este modo se analizaron métodos de ataque comunes y mediante la aplicación en un caso de estudio se demostró la efectividad del método.

Los resultados del modelo, en base a índices, estadísticas y reportes de las distintas firmas de seguridad, se considera que tienen un alto grado de efectividad en relación a ataques no dirigidos u otros modelos de ataques de seguridad de la información de alto riesgo como vulnerabilidades de día cero. El modelo verifica la seguridad de la información en perfiles de usuarios de redes sociales online, sin embargo, estos perfiles no dejan de ser personales y no podrían ser controlados por una organización.

Teniendo en cuenta la efectividad del modelo, y basándose en el mismo, se elaboró un método de evaluación de dichos perfiles en la red social Facebook, tomando en cuenta las preocupaciones de la organización, así como los controles ya implementados. El método además de evaluar, reduce el nivel de riesgo en el proceso.

La aplicación de SAMSON y ISASNET en la organización, redujo el riesgo y permitió que en la organización no exista ningún tipo de vulneración a la seguridad de la

información mediante técnicas de ingeniería social a través de redes sociales durante el período establecido como crítico debido a la coyuntura a la que la organización necesitaba estar preparada de manera adecuada.

Se han cumplido y abarcado todos los objetivos propuestos para el desarrollo de este proyecto de tesis y han servido para demostrar la efectividad de aplicar pruebas de ingeniería social como una especie de auditoría a políticas de seguridad de la información en una organización, así como han logrado un aporte académico en conocimiento y que, el método y modelo de evaluación propuestos sean de utilidad en otros ámbitos de la industria de tecnologías de la información y que ayude a profesionales de seguridad de la información a identificar y reducir riesgos que los estándares no los han detallado.

## 6.2 Trabajos futuros

Los resultados positivos de la propuesta metodológica, aplicadas en un caso de estudio, motivan a plantear como trabajo futuro el generar políticas específicas de seguridad de la información para el uso de redes sociales en distintos tipos de organizaciones públicas y privadas, y, también evaluar su aplicación y efectividad.

También se ve la necesidad de refinar y extender el SAMSON e ISASNET hacia los distintos tipos de redes sociales en línea, y así generar un marco de trabajo generalizado que permita generar contramedidas que se adapten a las propuestas realizadas.

Se plantea para futuros trabajos, una contribución que involucre una investigación basada en la experimentación para que la metodología ISASNET se ajuste a organizaciones que hayan implementado marcos de trabajo para el gobierno de tecnologías de la información como COBIT.

Por otro lado, es necesario ver como trabajo futuro las percepciones y facilidad de uso, tanto la ejecución de SAMSON para un hacker ético, como la aplicación de ISASNET para un evaluador.

Este trabajo, se lo mira también como una contribución a la usabilidad de sistemas de información, por lo que sería una propuesta elaborar y evaluar métricas de seguridad que puedan dar soporte a la medición de calidad en un sistema de información.

# Glosario de Términos

- **2FA:** Segundo factor de autenticación. Un paso adicional para confirmar el inicio de sesión en un sistema basado en usuario y contraseña.
- **Adware:** Software Publicitario. Aplicaciones que durante su funcionamiento despliegan publicidad a los usuarios o colectan información sobre los movimientos o la conducta en línea del usuario.
- **API:** Interfaz de programación de aplicaciones (*Application Programming Interface*). Conjunto de subrutinas, funciones y procedimientos que ofrece una biblioteca para ser utilizada por otro software como una capa de abstracción.
- **Autenticación de múltiples factores (MFA):** Método de control de acceso informático que garantiza que únicamente el usuario autorizado acceda a un sistema o información basándose en al menos dos de las siguientes categorías: conocimiento (algo que sabe), posesión (algo que tiene) e inherencia (algo que es).
- **Capa de abstracción:** Forma de ocultar los detalles de implementación de ciertas funcionalidades.
- **Certificado digital:** En criptografía, es un documento electrónico emitido por una autoridad certificadora que incluye una firma digital para cifrar las comunicaciones como el envío de un correo o el acceso a sitios web.
- **Cibercrimen (Delito Informático):** Actividad delictiva, donde se utilizan los servicios o aplicaciones en el ciberespacio para o son objeto de un delito, o donde el Ciberespacio es la fuente, herramienta, blanco o el lugar de un delito.
- **Ciberespacio:** entorno complejo que resulta de la interacción de las personas, software y servicios a través de Internet por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna.
- **Ciberprotección:** Condición de estar protegido contra consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, laborales, sicológicas, educaciones u otro tipo de consecuencias por falla, daño, error, accidente, o cualquier evento en el Ciberespacio que podría ser considerado no deseable.
- **Ciberseguridad:** Preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio.

- **Community Manager:** Profesional de la comunicación que se encarga de publicar y responder a nombre de una persona u organización en una o varias redes sociales.
- **Confidencialidad:** Propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.
- **CSV:** Archivo plano de texto con datos tabulares, las columnas se separan por comas.
- **Darknet:** Conjunto de direcciones IP que no se utilizan en las organizaciones, no están asignados a ningún sistema operacional de servidores o de PC.
- **Día cero:** Tipo de ataque que se aprovecha de vulnerabilidades aún no descubiertas por los fabricantes de hardware, desarrolladores de software o especialistas de seguridad,
- **Disponibilidad:** Condición de la información de encontrarse a disposición de quienes deben acceder a ella.
- **GNU:** Sistema operativo de tipo Unix de código abierto creado por Free Software Foundation.
- **GNU GPL:** Licencia Pública General de GNU. Licencia de derecho de autor de software libre y código abierto.
- **Integridad:** Propiedad de la información que mantiene los datos libres de modificaciones no autorizadas.
- **Malware:** Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directamente o indirectamente al usuario y/o al sistema informático del usuario.
- **NFC:** *Near Field Communications*. Tecnología de comunicación inalámbrica de corta distancia, generalmente usado en tarjetas y dispositivos móviles.
- **OTP:** *One Time Password*. Es una contraseña o número de confirmación que puede ser utilizado una única vez, y la mayoría de las veces tiene un tiempo de vida establecido en segundos o en pocos minutos.
- **Phishing:** Proceso fraudulento o intento de adquirir información privada o confidencial de manera enmascarada haciéndose pasar por una entidad confiable en una comunicación electrónica.

- **SDK:** Kit de desarrollo de software (*Software Development Kit*). Conjunto de herramientas que permiten a un programador crear aplicaciones para un sistema concreto.
- **Sinkhole:** Método para redirigir el tráfico IP específico a un dispositivo con el propósito de analizar el tráfico, desviar los ataques y detectar conductas anómalas en una red.
- **Spam:** Correo basura. Abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.
- **Spyware:** Software engañoso que recopila información privada o confidencial de un usuario de computador.
- **Stalking:** Fisgoneo amplio en el perfil de un individuo en una red social, en búsqueda de información que sirva para un objetivo específico, generalmente acoso.
- **Trackback:** Técnicas de rastreo automático para agilizar el seguimiento de ataques maliciosos como ataques de denegación de servicio.

## Referencias bibliográficas

Akamai. (2017). *State of the Internet/Security, Q1 2017 Report.* Akamai, SOTI Security. Cambridge: Akamai Technologies, Inc. Obtenido de https://www.akamai.com/StateOfTheInternet

Akamai. (2017). *State of the Internet/Security, Q2 2017 Report.* Cambridge: Akamai Techonologies, Inc.

Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. *17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop.* Sydney: Cornell University Library. Obtenido de https://arxiv.org/abs/1609.01107v1

Alsenoy, B. V., Verdoodt, V., Heyman, R., Ausloos, J., Wauters, E., & Acar, G. (2015). From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms. *SPION*, 1-67.

Arnaboldi, V., Conti, M., Passarella, A., & Pezzoni, F. (2012). Analysis of Ego Network Structure in Online Social Networks. *International Conference on Social Computing (SocialCom) and International Conference on Privacy, Security, Risk and Trust (PASSAT)*, 31-40. doi:10.1109/SocialCom-PASSAT.2012.41

Backstrom, L., Huttenlocher, D., Kleinberg, J., & Lan, X. (2006). Group formation in large social networks: membership, growth, and evolution. *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining.* Philadephia. doi:10.1145/1150402.1150412

Bastian, M., Heymann, S., & Jacomy, M. (2009). Gephi: An Open Source Software for Exploring and Manipulating Networks. *Third International AAAI Conference on Weblogs and Social Media ICWSM*, *8*, págs. 361-362. Obtenido de http://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/154

Boyd, D. M., & Ellison, N. B. (Octubre de 2007). Social Network Sites: Definition, History, adn Scholarship. *Journal of Computer-Mediated Communication, XIII*(1), 210-230. doi:10.1111/j.1083-6101.2007.00393.x

Brandes, U., Eiglsperger, M., Herman, I., Himsolt, M., & Marshall, M. S. (2002). GraphML Progress Report Structural Layer Proposal. *International Symposium on Graph Drawing* (págs. 501-512). Berlin: Springer. doi:10.1007/3-540-45848-4_59

Cisco. (2017). *2017 Annual Cybersecurity Report.* San José: Cisco Systems, Inc. Obtenido de https://www.cisco.com/go/acr2017

eMarketer. (10 de 06 de 2017). *Statista Inc.* Obtenido de https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

ESET. (2017). *La seguridad como rehén Tendencias 2017.* Bratislava: WeLiveSecurity.

Esposito, J. (4 de Marzo de 2016). *¿Tu perfil en redes sociales es objetivo de ataque?* (Kaspersky Lab Daily) Obtenido de https://latam.kaspersky.com/blog/tu-perfil-en-redes-sociales-es-objetivo-de-ataque/6778/

Ethics and Compliance Initiative. (s.f.). *Ethics Research Center. Ethics and Compliance Glossary.* Recuperado el 26 de junio de 2017, de http://ethics.org/resources/free-toolkit/toolkit-glossary

Facebook. (29 de Septiembre de 2016). *Data Policy*. (Facebook Ireland Ltd.) doi:https://www.facebook.com/about/privacy/

Facebook. (2017). *Facebook for developers - Graph API Explorer*. Obtenido de https://developers.facebook.com/tools/explorer/

Facebook. (2017). *Facebook for developers - Graph API Reference*. Obtenido de https://developers.facebook.com/docs/graph-api/reference

Facebook. (2017). *Facebook for Developers, Graph API, Facebook Platform Changelog*. Obtenido de https://developers.facebook.com/docs/apps/changelog#v2_0

Facebook. (12 de Abril de 2017). *Facebook Security: Improvements in protecting the integrity of activity on Facebook*. Obtenido de https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766

Facebook Inc. (14 de Abril de 2017). *Facebook Security: Disrupting a major spam operaton*. Obtenido de https://www.facebook.com/notes/facebook-security/disrupting-a-major-spam-operation/10154327278540766/

Fruchterman, T. M., & Reingold, E. M. (1991). Graph drawing by force-directed placement. *Software: Practice and experience, XXI*(11), 1129-1164.

F-Secure. (2017). *State of Cyber Security.* Helsinki: F-Secure Corporation.

Goh, S. H., Di Gangi, P. M., Rivera, J. C., & Worrell, J. L. (2016). Graduate Student Perceptions of Personal Social Media Risk: A Comparison Study. *Issues in Information Systems, XVII*(4), 109-119.

Hadnagy, C., & Wilson, P. (2010). *Social Engineering: The Art of Human Hacking.* (J. W. Sons, Ed.) Indianapolis, Indiana, Estados Unidos: Wiley Publishing, Inc.

Hansen, D. L., Shneiderman, B., & Smith, M. A. (2011). *Social Media Networks with NodeXL. Insights from a connected world.* (M. James, & D. Bevans, Edits.) Burlington: Elsevier.

Hinson, G. (Mayo de 2008). Social Engineering Techniques, Risks, and Controls. *EDPACS. The EDP Audit, Control and Security Newsletter, XXXVII*(4-5), 32-46.

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards Automating Social Engineering Using Social Networking Sites. *International Conference on Computational Science and Engineering CSE'09. III*, págs. 117-124. Vancouver: IEEE. doi:10.1109/CSE.2009.205

Indrajit, R. E. (Marzo de 2017). Social Engineering Framework: Understanding the Deception Approach to Human Element of Security. *International Journal of Computer Science Issues (IJCSI), XIX*(2), 8. doi:10.20943/01201702.816

Instituto Nacional de Estadísticas y Censos. (12 de 06 de 2017). *Ecuador en Cifras.* Obtenido de INEC - Estadísticas Sociales - Tecnologías de la Información y Comunicación 2016: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/170125.Presentacion_Tics_2016.pdf

International Organization for Standardization. (2017). *ISO/IEC JTC 1 - Information Technology.* Recuperado el 27 de junio de 2017, de https://www.iso.org/isoiec-jtc-1.html

Jaafor, O., & Birregah Babiga. (2015). Multi-layered graph-based model for social engineering vulnerability assessment. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 1480-1488.

Kaspersky Lab. (24 de Junio de 2017). *Internet Security Definitions | Kaspersky Lab US*. Obtenido de AO Kaspersky Lab: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kemp, S. (2017). *Digital in 2017, global overview. A collection of Internet, Social Media, and Mobile Data from around the world.* We Are Social.

Khan, G. F., Swar, B., & Lee, S. K. (Octubre de 2014). Social Media Risks and Benefits: A Public Sector Perspective. *Social Science Computer Review, XXXII*(606), 606-627. doi:10.1177/0894439314524701

Khan, Z. C., & Mashiane, T. (Agosto de 2014). An Analysis of Facebook's Graph Search. *Information Security for South Africa (ISSA), 2014*, (págs. 1-8). Johannesburgo. doi:10.1109/ISSA.2014.6950517

Kowalski, S. (2002). Value Based Risk Assessment: The Key to a Successful Security Target. *3rd International Common Criteria Conference (ICCC).* Otawa.

Malenkovich, S. (19 de Mayo de 2014). *Los Cinco Errores Más Graves Que Puedes Cometer en Facebook*. (Kaspersky Lab ) Obtenido de https://latam.kaspersky.com/blog/los-cinco-errores-mas-graves-que-puedes-cometer-en-facebook/3122/

McAffe Labs. (2016). *2017 Threats Predictions.* Santa Clara: Intel Security.

McAuley, J., & Leskovec, J. (2014). Discovering Social Circles in Ego Networks. *ACM Transactions on Knowledge Discovery from Data (TKDD) - Casin special issue, 8*(1), 1-28. doi:10.1145/2556612

McAuley, J., & Leskovec, J. (2014). Discovering Social Cirlces in Ego Networks. (ACM, Ed.) *ACM Transactions on Knowledge Discovery from Data (TKDD), VIII*(1). doi:10.1145/2556612

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, Indiana, Estados Unidos: John Wiley & Sons.

Mouton, F., Leenen, L., & Venter, H. S. (2015). Social Engineering Attack Detection Model: SEADMv2. *2015 International Conference on Cyberworlds (CW).* Visby: IEEE. doi:10.1109/CW.2015.52

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (Julio de 2014). Towards an Ontological Model Defining the Social Engineering Domain. (K. Kimppa, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka, Edits.) *ICT and Society - 11th IFIP TC 9 International Conference on Human Choice and Computers*, 266-279. doi:10.1007/978-3-662-44208-1

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social Engineering Attack Framework. *Information Security for South Africa (ISSA).* Johannesburg: IEEE. doi:10.1109/ISSA.2014.6950510

NaliniPriya, G., & Asswini, M. (2015). A survey on vulnerable attacks in online social networks. *2015 International Conference on Innovation Information in Computing Technologies (ICIICT).* Chennai: IEEE. doi:10.1109/ICIICT.2015.7396102

National Institute of Standards and Technology. (26 de Enero de 2017). *NIST Mission, Vision, Core Competencies, and Core Values*. (U.S. Department of Commerce) Obtenido de https://www.nist.gov/about-nist/our-organization/mission-vision-values

Nohlberg, M., & Kowalski, S. (2008). The Cycle of Deception - A Model of Social Engineering Attacks, Defences and Victims. *Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)* (págs. 1-11). Plymouth: University of Plymouth.

O'Connell, R. (17 de Julio de 2003). *A typology of child cybersexploitation and online grooming practices.* Obtenido de http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf

Ollmann, G. (2007). *IBM Global Technology Services: The vishing guide.* IBM. Obtenido de http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf

Oriyano, S. P. (2016). *Certified Ethical Hacker Version 9: Study Guide.* (B. W. Mary, Ed.) Indianapolis, Indiana, Estados Unidos: SYBEX.

Osterman Research. (2016). *Prácticas y Prioridades de Pruebas de Seguridad, Reporte de Encuesta.* Trustwave.

Peng, J., Meng, Y., Xue, M., Hei, X., & Ross, K. W. (2015). Attacks and Defenses in Location-Based Social Networks: A Heuristic Number Theory Approach. *2015 International Symposium on Security and Privacy in Social Networks and Big Data.* Hangzhou: IEEE. doi:10.1109/SocialSec2015.19

PwC. (2017). *Key findings from The Global State of Information Security® Survey 2017.* PwC. Obtenido de https://www.pwc.com/gsiss

Ramos Varón, A. Á., Barbero Muñoz, C., Marugán Rodríguez, D., & González Durán, I. (2015). *Hacking con Ingeniería Social. Técnicas para hackear humanos.* (A. Gutiérrez M., Ed.) Bogotá, Colombia: Ediciones de la U.

Rapoport, A. (1957). Contribution to the theory of random and biased nets. *The bulletin of mathematical biophysics, XIX*(4), 257-277.

Reynolds, G. W. (2016). *Ética en la tecnología de la información* (5a ed.). (O. Martínez, Ed., & A. Zendejas Escandón, Trad.) México D.F., México: Cengage Learning.

Rouse, M. (junio de 2007). *TechTarget, Search Security - What is White Hat?* Recuperado el 26 de junio de 2017, de http://searchsecurity.techtarget.com/definition/white-hat

SANS. (2016). *SANS Institute: Information Security Resources*. Recuperado el 26 de Junio de 2017, de https://www.sans.org/information-security/

Servicio Ecuatoriano de Normalización INEN. (octubre de 2015). NTE INEN-ISO/IEC 27032:2015. *Norma Técnica Ecuatoriana INEN-ISO/IEC 27032:2015. Tecnologías de la Información - Técnicas de Seguridad - Directrices para ciberseguridad (ISO/IEC 27032:2012, IDT)*(3). Quito, Pichincha, Ecuador: Servicio Ecuatoriano de Normalización INEN.

Servicio Ecuatoriano de Normalización INEN. (2016). NTE INEN-ISO/IEC 27001:2016. *Norma Técnica Ecuatoriana. Tecnologías de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos.*

*(ISOIEC 27001:2013 + Cor 1:2014 + Cor 2:2015, IDT)*(2). Quito, Pichincha, Ecuador: Servicio Ecuatoriano de Normalización INEN. Obtenido de http://www.normalización.gob.ec

Servicio Ecuatoriano de Normalización INEN. (abril de 2017). NTE INEN-ISO/IEC 27002:2017. *Norma Técnica Ecuatoriana. Tecnologías de la información - Técnicas de Seguridad - Código de práctica para los controles de seguridad de la información (ISO/IEC 27002:2013 + Cor1.: 2014 + Cor.2: 2015, IDT)*(2). Quito, Pichincha, Ecuador: Servicio Ecuatoriano de Normalización INEN.

Stamos, A. (26 de Julio de 2017). *Preparing for the future of security requires focusing on defense and diversity - Black Hat USA 2017 - Facebook Security.* Obtenido de https://www.facebook.com/notes/facebook-security/preparing-for-the-future-of-security-requires-focusing-on-defense-and-diversity/10154629522900766/

Symantec. (2017). *Internet Security Threat Report.* Mountain View: Symantec Corporation.

Tukey, J. W. (1977). *Exploratory Data Analysis.* Middlesex: Addison-Wesley Publishing Co.

US-CERT Publications. (24 de junio de 2017). *Avoiding Social Engineering and Phishing Attacks (ST04-014)*. Obtenido de United States Computer Emergency Readiness Team: https://www.us-cert.gov/ncas/tips/ST04-014

Wasserman, S., & Faust, K. (1994). Social Network Analysis in the Social and Behavioral Sciences. En S. Wasserman, *Social Network Analysis: Methods and Applications* (págs. 3-27). Cambridge University Press. doi:10.1017/CBO9780511815478.002

Webber, A., Li, C., & Szymanski, J. (2012). *Guarding the Social Gates: The Imperative for Social Media Risk Management.* San Mateo: Altimeter Group.

Zhang, W. (2010). Integrated Security Framework for Secure Web Services. *Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI)* (págs. 178-183). Jinggangshan: IEEE. doi:10.1109/IITSI.2010.8

Žitnik, S. (2012). *Lovro Šubelj - Publications & talks.* Obtenido de http://wwwlovre.appspot.com/resources/research/networks/ssd/slavko.net

# ANEXO 1

**Políticas de Seguridad de la Información para el uso de Redes Sociales**

1. Las páginas de la organización deberán administrarlos cada persona mediante su cuenta personal de Facebook, la misma que deberá constar el nombre completo, así como una foto de identificación, de este modo quedará registrado las acciones que realicen a nombre de la página de la organización.
2. La administración total de cada página la realizarán un máximo de 3 personas de confianza designados y en acuerdo con la entidad superior de la organización; los demás usuarios tendrán únicamente permiso de Editores o inferiores.
3. No se dará autorización a aplicaciones a los perfiles de Facebook sin la autorización de personal de Seguridad de la Información.
4. No se debe publicar ni vincular información laboral como el correo electrónico del trabajo en redes sociales.
5. Cuando un funcionario se desvincule de la organización, deberá entregar todas las credenciales que posea y el administrador deberá revocar todos los permisos de publicación y administración de las cuentas. Cuando los permisos sean otorgados a funcionarios de la organización, y los permisos revocados, se deberá cambiar las contraseñas a las cuales tenía acceso el funcionario, así como los correos de notificación y los números de teléfono celular vinculados a la cuenta en el caso de que hayan pertenecido al funcionario desvinculado.
6. Las contraseñas se las cambiará una vez cada 2 meses, o cuando así se lo disponga realizarlo.
7. Las contraseñas deberán tener más de 8 dígitos, además debe incluir: mayúsculas, minúsculas, números y caracteres especiales.
8. Se debe usar una contraseña distinta para cada perfil para cada red, y deberá ser distinta a otras usadas en los sistemas de la organización.
9. Las credenciales no serán compartidas por ningún motivo por medios escritos o digitales, únicamente a las personas autorizadas y de confianza.
10. No deberán abrir enlaces recibidos en perfiles, páginas o correos de notificaciones de redes sociales que no haya sido antes verificado su integridad y veracidad, en el caso de hacerlo, deberá ser en un equipo con protección contra virus, malware y phishing.

11. Verificar siempre al ingresar las credenciales, que la dirección sea la página correcta y que sea segura (https).
12. Se deberán habilitar todas las configuraciones de seguridad y privacidad necesarias como: notificaciones de inicio de sesión, registro de dirección IP y utilización de 2FA.
13. Cada jefatura organizacional establecerá el uso de redes sociales mediante un control de mando que permita a sus subalternos el uso o no de una u otra red social. Este control de mando será configurado y dispuesto por los respectivos administradores de red.
14. Cada dispositivo utilizado por los funcionarios deberá estar equipado con soluciones de seguridad anti-phishing.
15. Se dictarán capacitaciones semestrales sobre el uso adecuado de redes sociales por parte de personal de seguridad de la información a todos los funcionarios.
16. Se realizarán evaluaciones controladas de seguridad de la información en perfiles de redes sociales de los funcionarios.
17. Se sugiere la utilización de equipos virtuales configurados y controlados específicamente para gestión de redes sociales.