



UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

“Diseño de un marco de trabajo para la gestión de riesgos de ingeniería social basado en los estándares ISO 27002 y NIST 800-50”

Realizado por:

Ing. Manuel Fernando Fernández Fernández.

Director del proyecto:

Ing. Verónica Elizabeth Rodríguez Arboleda, MBA.

Como requisito para la obtención del título de:

**MASTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON
MENCIÓN EN SEGURIDAD EN REDES Y COMUNICACIÓN**

Quito, 28 de febrero de 2019.

DECLARATORIA

El presente trabajo de investigación titulado:

“DISEÑO DE UN MARCO DE TRABAJO PARA LA GESTIÓN DE RIESGOS DE INGENIERÍA SOCIAL BASADO EN LOS ESTÁNDARES ISO 27002 Y NIST 800-50”

Realizado por:

MANUEL FERNANDO FERNÁNDEZ FERNÁNDEZ

ha sido dirigido por la docente:

ING. VERÓNICA RODRÍGUEZ, MBA

quien considera que constituye un trabajo original de su autor

Ing. Verónica Rodríguez Arboleda, MBA

DIRECTORA

LOS PROFESORES INFORMANTES

Los Profesores Informantes:

Msc. FABIÁN HURTADO

Msc. CHRISTIAN PAZMIÑO

Después de revisar el trabajo presentado,
lo han calificado como apto para su defensa oral ante el tribunal examinador

Msc. Fabián Hurtado

Msc. Christian Pazmiño

Quito, marzo del 2019

DECLARACIÓN JURAMENTADA

Yo, MANUEL FERNANDO FERNÁNDEZ FERNÁNDEZ, con cédula de identidad 0802913681, declara bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

Manuel Fernando Fernández Fernández
C.C. 080291681

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por permitirme terminar este proyecto satisfactoriamente y haberme dado la oportunidad de tomar esta maestría.

A mi esposa por su apoyo incondicional a lo largo de toda la carrera, por todos los momentos de clases, deberes, trasnochadas, etc., sin duda, contigo fueron más llevaderos.

A la Ing. Verónica Rodríguez por su acertada dirección y entrega, sin duda, este trabajo no hubiese salido adelante sin su gran aporte y enorme dedicación.

A mis amigos y compañeros: Andrés, Anita, Jean y Verito... gracias por los momentos y experiencias vividas en toda la carrera, sin Uds. no hubiera sido lo mismo.

Un especial agradecimiento a la Sra. Micaela, ya que sin su apoyo tan valioso no hubiese sido posible llevar a cabo este proyecto... ¡Que Dios la bendiga!

DEDICATORIA

Este trabajo lo dedico a mis motores: mi esposa y mis hijas, quienes son mi motivación e inspiración constante.

A mis padres, ya que, sin su aporte, sacrificio y dedicación en mis etapas iniciales, esto no hubiese sido posible.

RESUMEN

Cuando se habla de seguridad informática es muy común que las organizaciones se enfoquen en los diversos equipos tecnológicos que evitan accesos externos no deseados (por ej. Firewalls, IPS, UTM's, etc.), o es frecuente pensar que las pruebas de intrusión o pruebas de penetración sobre la infraestructura tecnológica va a mitigar todos los riesgos que atentan sobre la información; sin embargo, son pocas las organizaciones que visualizan de manera holística todos los componentes de riesgo de un ambiente tecnológico, incluyendo el factor humano.

El presente trabajo tiene como objetivo primario, desarrollar un marco de control para la mitigación de los riesgos que provoca el componente humano dentro de un esquema de seguridad de la información. Para llegar a desarrollar el modelo, se ha llevado a cabo un estudio y caracterización de algunos de los componentes de los ataques de ingeniería social, tales como: conductas o comportamientos naturales de los seres humanos, técnicas de ataques más usadas; además se ha realizado un repaso por los marcos de trabajo, metodologías y estándares de TI actuales, de donde se ha recabado lineamientos y buenas prácticas que han servido de base para el desarrollo de la propuesta, a la cual se la ha denominado MATIS (**Marco de Trabajo para los riesgos de Ingeniería Social**).

MATIS es un marco de trabajo que podría ser adoptada por los responsables de la gestión de riesgos de seguridad de la información de cualquier organización que requiera incorporar a sus estrategias de seguridad, un set de buenas prácticas y controles que permitirán minimizar la exposición a los ataques que buscan vulnerar el factor humano.

ABSTRACT

When talking about information security, it is very common to focus on technical solutions that intent to prevent unauthorized access (e.g. Firewalls, IPS, UTPs, etc.). In addition, it is common to think that intrusion or penetration tests will mitigate all the risks that threat the security information; However, there are few organizations who visualize holistically all the risks components of an IT environment, including the human factor.

The main objective of this project is to develop a framework for the mitigation of the risks caused by the human component within an information security environment. In order to develop the framework, a study and characterization of social engineering's components attacks has been carried out, such as: natural behaviors of human beings, most used attack techniques. In addition it has also been conducted a review of current IT frameworks, methodologies and standards, from which guidelines and good practices have been collected that have served as the basis for the development of the proposal, which has been called MATIS.

MATIS is a framework that could be adopted by those responsible for the management of information security of any organization (e.g. IT Security Officer) that requires incorporating into their security strategies, a set of good practices and controls that will minimize exposure to attacks that seek to harm the human factor.

Índice General

CAPÍTULO I.....	12
INTRODUCCIÓN	12
1 EL PROBLEMA DE LA INVESTIGACIÓN	12
1.1 PLANTEAMIENTO DEL PROBLEMA	12
1.1.1 Diagnóstico.	12
1.1.2 Pronóstico.....	15
1.1.4 Formulación del problema.	15
1.1.5 Objetivo general.	16
1.1.6 Objetivos específicos.....	16
1.1.7 Justificación.....	16
CAPÍTULO II	18
FUNDAMENTACIÓN TEÓRICA.....	18
2.1 MARCO TEÓRICO	18
2.1.1 Riesgo tecnológico	18
2.1.2 Ataque informático.....	18
2.1.3 Ingeniera Social.....	19
2.1.4 Psicología	19
2.1.5 La interacción social.....	20
2.1.6 El riesgo del factor humano	20
2.1.7 Categoría de ataques de Ingeniería Social.....	20
2.1.8 Técnicas de Ingeniera Social.....	21
2.1.9 Marco de trabajo (<i>Framework</i>)	26
2.1.10 Marcos de referencia de TI.....	28
2.1.11 Adopción de una perspectiva teórica	29
2.2 ESTADO DEL ARTE	30
CAPÍTULO III	39
ANÁLISIS SITUACIONAL.....	39

3.1	Análisis de los factores psicológicos	39
3.1.1	La psicología como factor incidente de la Ingeniería social	39
3.2	Análisis de las técnicas de ingeniería social	51
3.3	Análisis de las normas y marcos de referencia de TI	78
3.3.1	Análisis de COBIT	78
3.3.2	Análisis de ITIL	80
3.3.3	Análisis de ISO 27002	82
3.3.4	Análisis de NIST 800-50	84
CAPÍTULO IV		87
DESARROLLO DE LA PROPUESTA DE MARCO DE TRABAJO.....		87
4.1	Introducción	87
4.2	Diseño del Marco de Trabajo para los Riesgos de Ingeniería Social	88
4.3	Explicación del modelo del marco de referencia.....	92
4.4	Desarrollo de los componentes de MATIS.....	93
4.4.1	Componente 1: Personas.....	93
4.4.2	Componente 2: Política de Seguridad General	115
4.4.3	Componente 3: Controles	115
CAPÍTULO V		129
CONCLUSIONES Y TRABAJOS FUTUROS		129
BIBLIOGRAFÍA.....		131

Índice de figuras

Figura 1 - Cobertura y relación de los marcos de trabajo de TI.	26
Figura 2 - Mensaje de advertencia en Windows. Fuente:	31
Figura 3 - Clasificación de los ataques de ingeniería social de acuerdo a sus características.	32
Figura 4 - Características de la Ingeniería Social 2.0.	34
Figura 5 - Correo de phishing usando imagen del Banco Pichincha.	53
Figura 6 - Ejemplo de correo de Malware-phishing.	54
Figura 7 - Esquema de operación de un ataque phishing basado en DNS	54
Figura 8 - Ejemplo de ataque de tipo Content-Injection	55
Figura 9 - Ejemplo de ataque de Search Engine Phishing	56
Figura 10 - Ejemplo de uso de acortadores de URL	56
Figura 11 - Correo que descargaba malware haciendo uso del evento de un terremoto en Ecuador.	58
Figura 12 - Formulario donde se debía ingresar los datos de tarjeta de crédito para ser parte del ficticio sorteo.....	59
Figura 13 - Ejemplo de ataque Smishing.	62
Figura 14 - Ejemplo de información obtenida con Spokeo.....	69
Figura 15 - Visión general de los componentes definidos por la NIST 800-50.....	85
Figura 16 - Visión general del análisis de riesgos de los vectores de ataques de IS.....	87
Figura 17 - MATIS – Marco de trabajo de gestión de riesgos de ingeniería social	91

CAPÍTULO I

INTRODUCCIÓN

1 EL PROBLEMA DE LA INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Diagnóstico.

En la actualidad, el rol que desempeña las tecnologías de la información es cada vez más importante y transcendental en la sociedad. La tecnología ha ayudado a que uno de los recursos más importantes de las organizaciones, la información, pueda crearse, usarse, almacenarse, reportarse o destruirse de manera más eficiente.

Si bien los beneficios y bondades que brinda el uso de TI puede ayudar a las compañías a optimizar sus procesos, obtener ventaja competitiva e innovar, existen factores inherentes propios de la tecnología que generan riesgos que atentan sobre la integridad, confidencialidad y disponibilidad de la información.

Es por esto que, frecuentemente las organizaciones hacen grandes inversiones en implementaciones de software y hardware (cortafuegos, sistemas antivirus, sistema de detección de intrusos, etc.) que buscan minimizar los riesgos de TI, muchos de estos esfuerzos se enfocan en cerrar las brechas de seguridad existentes en la infraestructura tecnológica. Sin embargo, hay un componente de la ciberseguridad poco conocido y altamente riesgoso: los usuarios de tecnología.

Hoy en día, con todas las soluciones de seguridad existentes en el mercado, el usuario es el único componente del ambiente de tecnología que no puede protegerse. Precisamente, los ataques dirigidos a vulnerar a las personas y que tiene por objetivo obtener información privilegiada o confidencial se denomina Ingeniería Social.

Según estudios recientes realizados por Digital Guardian (2015) al menos el 97 % de los ataques informáticos usan información que ha sido obtenida mediante alguna técnica de ingeniería social. El mismo informe de Digital Guardian reveló que, por ejemplo, al menos el 91 % de las brechas de seguridad se originan debido a ataques de *phishing*, una de las técnicas de ingeniería social más explotadas.

Por otro lado, en los últimos años se han conocido un sinnúmero de ciberataques a nivel mundial realizados mediante técnicas de ingeniería social. A continuación, se describen algunos casos:

En febrero de 2016, un *hacker* reveló a la revista *Motherboard* que había comprometido la seguridad del Departamento de Justicia de los Estados Unidos mediante el uso de técnicas de ingeniería social, el cual tuvo como resultado el robo de más de 9 mil registros de empleados del Departamento de Seguridad Nacional estadounidense; además de revelar los datos de 20 mil empleados del FBI. Fuentes oficiales dieron a conocer que el ataque fue posible ya que el atacante logró comprometer una cuenta de correo de un empleado con la que después mediante un engaño telefónico, logró obtener acceso al portal web del Departamento de Justicia, desde donde mediante técnicas de *hacking*, logró acceder a la base de datos y así robar 200 GB de información confidencial (Motherboard, 2016).

Otro caso ocurrió en diciembre de 2015, en una región del este de Ucrania donde se suscitó una interrupción del servicio de energía eléctrica por alrededor de 6 horas, afectando a más de 80 mil personas. Esta falla eléctrica fue causada por un ataque informático, la cual fue lograda mediante un ataque de *phishing* que permitió a los atacantes ganar acceso al sistema de control central de operaciones, mediante un malware conocido como *BlanEnergy3*, el cual se encontraba escondido dentro de un archivo adjunto en formato Excel (Zetter, K., 2016).

Por otro lado, en marzo 2013, una de las cadenas de *retail* más grandes de Estados Unidos, *Target*, fue víctima de un ataque informático, el cual tuvo como resultado el robo de información de clientes y tarjetas de crédito de más de 70 millones de clientes. El robo fue posible mediante un ataque de *phishing*, en el cual los atacantes enviaron correo infectados con *malware* a uno de los proveedores de la cadena de *retail*, quien no contaba con sistemas robustos de seguridad, una vez dentro de los sistemas del proveedor, los atacantes aprovecharon la conexión de red existente con el sistema de facturación de *Target* para acceder al sistema de pagos de la cadena de *retail*, desde donde extrajeron la información de tarjetas de créditos de sus clientes (Krebs on Security, 2014).

Estos eventos invitan a que se cuestione sobre el enfoque de las estrategias de seguridad informática de las organizaciones y el nivel de consciencia que los líderes de las funciones de seguridad poseen sobre la necesidad de definir enfoques holísticos de prevención y monitoreo del ambiente de riesgos de TI, no solo a nivel de *hardware* y *software*, si no también considerando el riesgo que genera el factor humano.

Además, las herramientas, marcos de trabajo, metodologías y estándares para la mejora de entrega de servicios de TI, gobierno de TI, gestión de riesgos y gestión de TI existentes en la

industria (tales como, por ejemplo: ITIL, COBIT, ISO 27000) no abarcan con profundidad y detalle la gestión de riesgos derivados de ingeniería social.

1.1.2 Pronóstico.

El número de los delitos informáticos crece a diario a nivel mundial, la mayoría de estos ataques se logran con información que es obtenida mediante técnicas de ingeniería social, las cuales han evolucionado en los últimos tiempos. No adoptar políticas, procedimientos y normas de seguridad que minimicen los riesgos de ingeniería social podría generar que el número de ataques informáticos siga aumentando, provocando que los riesgos que atentan contra la seguridad de la información se materialicen, derivando en pérdidas económicas, robo de información confidencial o estratégica e inclusive afectación a la reputación a las organizaciones.

1.1.3 Control del pronóstico.

El número de delitos informáticos que se llevan a cabo mediante el uso de técnicas de ingeniería social puede minimizarse si las organizaciones implementan buenas prácticas, políticas y procedimientos de control sobre los riesgos que genera el factor humano dentro de un ambiente tecnológico y su información. El presente trabajo busca desarrollar un marco de trabajo que contenga dichas políticas y controles que puedan ser adoptadas por cualquier organización de cualquier tamaño y sector.

1.1.4 Formulación del problema.

Las normas y estándares de TI existentes, incluyendo las prácticas de gestión de riesgos de TI no poseen información específica y detallada que proponga normas, políticas y

procedimientos que puedan ser adoptadas por las organizaciones para la prevención y mitigación de los riesgos de ingeniería social.

1.1.5 Objetivo general.

Diseñar un marco de trabajo basado en los estándares ISO 27002 y NIST 800-50 mediante el estudio de los factores de la psicología humana, investigación de las técnicas de ataques y normas de TI existentes que permita la gestión de riesgos de ingeniería social.

1.1.6 Objetivos específicos.

- Determinar los factores de la psicología humana que generan los riesgos de ingeniería social mediante el análisis de artículos científicos, bibliografía y estudio de vectores de ataques existentes, para identificar las connotaciones de los seres humanos que son explotados en los ataques informáticos.
- Realizar un análisis sobre las buenas prácticas, estándares y normas de gestión de riesgos y gobierno de TI existentes mediante el estudio de los marcos de referencia y metodologías de TI globalmente aceptadas para definir la línea base de políticas y procedimientos de la guía a elaborar.
- Diseñar un marco de trabajo para la gestión de riesgos de ingeniería social tomando como base el estudio de los factores de riesgo de la psicología humana y la línea base de normas y estándares existentes.

1.1.7 Justificación.

1.1.7.1 Justificación técnica

Contar con marco de referencia dedicado a la gestión de riesgos de ingeniería social, basado en un estudio de los comportamientos psicológicos que originan los riesgos, con contenido

estructurado, técnicamente fundamentado, basado en buenas prácticas, estándares y marcos metodológicos existentes, justifica el desarrollo del presente trabajo.

1.1.7.2 Justificación metodológica

Parte fundamental de este proyecto, implica la definición de una línea base, la cual está compuesta por las buenas prácticas propuestas por los diversos estándares y metodologías existentes en la actualidad, entre ellos: COBIT, ISO 27002, NIST 800-50. El uso de estos marcos de referencia y estándares permitirán aprovechar conceptos ya estudiados, discutidos y probados, de modo que el modelo a proponer contará con conocimientos ya definidos que aportarán en la estandarización de términos y uso de un lenguaje integrado.

1.1.8 Alcance

A continuación, se delimita el alcance de este trabajo en sus tres componentes principales:

- i) **Factores psicológicos:** se han considerado los siguientes: solidaridad, reciprocidad, confianza, colectivismo, reconocimiento, obsecuencia, urgencia y consistencia.
- ii) **Vectores de ataques:** se han considerado los siguientes: *phishing*, *smishing*, *vishing*, *spear-phishing*, *whaling*, información de libre acceso, *trashing*, *Shoulder surfing*, *piggybacking* o *tailgaiting*, *sex appeal*, *baiting*, uso de redes Wifi abiertas y espionaje de oficina.
- iii) **Marcos de referencia o estándares:** para el análisis se ha considerado COBIT 5, ITIL, ISO 27002 y NIST 800-50, de los cuales, para el diseño del amrco de referencia se utilizaron los dos últimos.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1 MARCO TEÓRICO

2.1.1 Riesgo tecnológico

Se conoce como riesgo de tecnología de la información a la probabilidad de que los sistemas de información y sus componentes (*hardware*, *software*, usuarios y administradores) que son utilizados para registrar, procesar, almacenar, transmitir y reportar información fallen, originando que la información pueda ser modificada, borrada, divulgada o dañada, cuyas implicaciones pueden ser de diversas índoles, entre ellas: financiera, estratégica, operacionales, regulatorias y reputacionales (Areitio, 2008).

2.1.2 Ataque informático

Según Stu Sjouwerman (2011), un ataque informático o cibercrimen es un delito en el cual se involucra a una computadora, o un acto malicioso cometido mediante una conexión de Internet. Otras definiciones afirman que un ataque informático es un método ofensivo realizado por una o varias personas mediante el uso de un sistema informático u otros mecanismos, las cuales usualmente se aprovechan de vulnerabilidades o brechas de seguridad y cuyos motivantes pueden ser de índole social, económico o político (ACISSI, 2015).

2.1.3 Ingeniera Social

La ingeniería social es el conjunto de técnicas o estrategias psicológicas y habilidades sociales -tales como: la influencia, la persuasión y la sugestión- utilizadas de manera premeditada, con el fin de conseguir que otra persona haga algo por otro, donde en la mayoría de los casos el objetivo final es la obtención de información confidencial (ACISSI, 2015).

La ingeniería social no es un tema nuevo o un concepto que haya surgido con la informática, ya que es tan antigua como la existencia de los seres humanos. Sin embargo, las técnicas que usa la Ingeniería Social han evolucionado en los últimos años y con el crecimiento de la era digital, los atacantes se han adaptado y han tomado ventaja de las vulnerabilidades que generan el factor humano.

Entre otras definiciones de ingeniería social, se tiene:

Mitnick (2003) señaló: "La Ingeniería Social el arte de atacar al eslabón más débil, los seres humanos" (p. 90).

Samarai (2015) afirmó: "La aplicación deliberada de técnicas engañosas diseñadas para manipular a alguien con el fin de divulgar información o realizar acciones que pueden dar como resultado la publicación de esa información" (p.38).

2.1.4 Psicología

Según Rohrer (1998) la psicología es la ciencia que estudia los procesos y los estados consciente, así como sus orígenes y sus efectos. Esta definición se puede complementar con la enunciada por Moore (1996), en la que menciona que psicología es la ciencia que estudia la personalidad humana. Estos dos conceptos ayudarán a comprender

mejor los mecanismos que son usados por los atacantes informáticos en las diferentes técnicas de Ingeniería Social.

2.1.5 La interacción social

Es el enlace que existen entre las personas, que genera confianza, afecto, aprendizaje, y hermandad entre la sociedad. Es la esencia del subconsciente que busca imperativamente la aceptación social que brinda satisfacción personal (Edmond Marc, 1992).

2.1.6 El riesgo del factor humano

Tomando la definición de Mitnick (2003), quien manifestó que la ingeniería social usa la influencia y persuasión para engañar a la gente para convencerlos de que mediante acciones legítimas se brinde u otorgue información confidencial, se puede determinar que, la ingeniería social mezcla algunas disciplinas, entre ellas: psicología, sociología, antropología, ciencias sociales y tecnologías de la información.

Sin embargo, cuando se habla del factor humano, es importante comprender cuáles características psicológicas permiten que los atacantes sociales puedan sacar provecho de las mismas, en los siguientes párrafos se buscará entender las características de los seres humanos que son explotadas por los ciberdelincuentes.

2.1.7 Categoría de ataques de Ingeniería Social

Entrando un poco más en materia, es importante conocer las distintas variantes que puede tomar los ataques de Ingeniería Social, a continuación, se muestra la clasificación realizada por Areitio (2008):

Ataques Técnicos

En este tipo de ataque no existe contacto directo entre el *hacker* y la víctima, ya que generalmente se utilizan métodos informáticos, tales como: sitios de Internet, correos electrónicos, boletines informativos, etc., en este método, el atacante juega el papel de una entidad conocida y de mucha confianza.

Ataques Social

Este tipo de infiltraciones comúnmente usan aspectos socio-psicológico, como, por ejemplo: el ego, la vanidad, la empatía, etc. El objetivo de estos ataques es convencer a la víctima de que está realizando una acción legítima. Este es el tipo de ataques donde las víctimas tardan en darse cuenta que han sido vulneradas.

Ataques Físico

Los ataques físicos implican que al atacante debe realizar alguna actividad que implique presencia o contacto físico, ya sea de forma directa o indirecta, entre los principales ataques tenemos: escarbar en la basura, mirar por encima del hombro, *tailgaiting*, entre otros.

2.1.8 Técnicas de Ingeniería Social

Como consecuencia de las categorías de ataques de Ingeniería Social, existen métodos y técnicas que son usadas por los atacantes, entre ellas se encuentran las siguientes:

Phishing

Este término proviene del término anglosajón “pescar”, y en el mundo de la ciberseguridad se refiere al tipo de ataques en donde un usuario malintencionado intenta lograr

que la víctima “muerda el anzuelo”, lo cual va desde descargar algún virus, ingresar credenciales en un sitio falso, responder a un correo falso hasta instalar software que generan puertas traseras (Bisson, 2015).

Este tipo de ataques es el mecanismo de Ingeniería Social más usados en actualmente. Según Digital Guardian (2015), el 91 % de los ataques de seguridad están ligados a un ataque donde se ha utilizado algún tipo de *phishing*.

Uso de Información de libre acceso

Comúnmente, los atacantes suelen iniciar sus ofensivas mediante la recolección de datos de libre acceso, los cuales están disponibles en redes sociales, blogs, portales web, entre otros.

Sitios de Internet como LinkedIn, Facebook y Google+ suelen contener amplia información suficiente para que un hacker obtenga la información base sobre la cual dirigirá su ataque (NoticiasSeguridadInformatica, 2016).

Escarbar en la basura (*Trashing*)

Esta es una técnica que hace referencia a la obtención información confidencial mediante la búsqueda de documentos o papeles que han sido descartados, por ejemplo, en la basura. En algunas ocasiones, un atacante puede llegar a conseguir información sensitiva, tales como: anotaciones, instructivos, procedimientos e inclusive credenciales de acceso únicamente hurgando en el basurero o en el depósito de reciclaje (NoticiasSeguridadInformatica, 2016).

Infiltración en la vida real

En muchas de las tramas cinematográficas o series televisivas se ha observado como un individuo desempeña un rol falso con el fin de acercarse a un objetivo; pues esto no es menos real en el mundo de la ingeniería social. Existen casos conocidos de infiltraciones de espías gubernamentales en donde con un vasto estudio previo, el atacante se inserta en el ambiente cotidiano de la víctima. Esto puede ir desde el hacer compras en el mismo supermercado, acudir a la misma iglesia, o intencionalmente coincidir en un bar o fiesta, con el fin de ganar hacerse cercano y así obtener datos que de a poco otorguen mayor información al atacante (NoticiasSeguridadInformatica, 2016).

Espiar por encima del hombro (*Shoulder surfing*)

Este tipo de ataque consiste en entablar una conversación con la víctima con el fin de ir realizando notas mentales sobre lo que el objetivo introduce en el dispositivo, principalmente, las credenciales de accesos a los sistemas (Bisson, 2015).

Uso del *sex appeal*

Un o una atacante puede hacer uso de su apariencia y atractivo físico para conseguir que otra persona realice algo por él o ella. En algunos casos, los atacantes mantienen relaciones sentimentales de corto o mediano plazo para ganar la confianza de la víctima con el fin de obtener la mayor cantidad de información confidencial posible (NoticiasSeguridadInformatica, 2016).

Piggybacking o tailgating

Esta técnica no es exclusiva de la ingeniería social, ya que ha sido utilizada como método de infiltración a lo largo de la historia. Esta práctica consiste en obtener acceso

físico no autorizado a instalaciones o edificios restringidos simplemente caminando detrás de una persona autorizado. En ciertos casos más complejos, el atracador puede hacerse pasar por un empleado de una entidad de servicio público (por ej.: correo, plomería, teléfono, etc.), y con la excusa de tener las manos ocupadas (por ej., cargando un paquete), solicitará a una persona autorizada mantener la puerta abierta para poder ingresar (Bisson, 2015).

Pérdida delibera de dispositivos USB

Esto consiste en abandonar de manera intencional dispositivos de almacenamiento externo, como por ejemplo memorias flash o discos USB portátiles, en sitios públicos donde pueda ser fácilmente encontrado por la víctima para que apelando a su sentido de curiosidad, inserte el dispositivo en su equipo y así este infecte de código malicioso al equipo de la víctima, en algunos de los casos creando puertas traseras que luego son utilizadas por el *hacker* (Bisson, 2015).

Suplantación de identidad

Esta práctica no es nueva ni de uso exclusivo de los ataques informáticos, más bien, es un método ampliamente usado por *hackers* y consiste en jugar un rol, tales como: usuarios de soporte técnico, gerentes o altos mandos. Este tipo de técnicas comúnmente tienen mayor éxito en organizaciones con un alto número de empleados, debido a que es imposible conocer a todos, por lo que falsificar una credencial no es complicado (NoticiasSeguridadInformatica, 2016).

Espionaje de oficina

Es conocido que, en los últimos años, existen atacantes que emplean o reclutan a empleados internos de las organizaciones con el fin de que les provean información interna de la compañía. Eventos que podrían parecer no intencionales, como por ejemplo, dejar desbloqueado el computador o compartir las credenciales generan una amplia brecha de seguridad para que un usuario mal intencionado logre acceso a información sensible, evitando invertir amplios recursos en vulnerar una contraseña o atacando *Firewalls* y demás restricciones de seguridad (Bisson, 2015).

Ingeniería social inversa

Este es uno de los modos más avanzados de la ingeniería social, ya que el atacante crea un problema intencionalmente para poder intervenir como parte de la solución. Por ejemplo, un atacante podría generar una denegación de servicio sobre el sitio web de una organización, con la finalidad de hacer creer que la seguridad perimetral o la seguridad lógica de una organización está bajo amenaza. Dado este escenario, el atacante surge como un consultor de seguridad o un miembro del equipo de soporte con altos conocimientos sobre la solución donde ellos pueden demostrar su conocimientos y experiencia. Una vez contratados para resolver el problema que ellos mismos causaron, los atacantes están en la posibilidad de ejecutar actividades no autorizadas y robar información confidencial (Bisson, 2015).

Intimidación

En este tipo de ataques, el *hacker* simula ser un directivo importante de la organización y mediante el uso de su supuesta autoridad, logra hacer que la víctima realice

lo que le pida, lo cual puede ir desde el entregar sus credenciales, proporcionar informes que contengan información confidencial, entre otros.

Este tipo de ataques se aprovecha del sentir inherente del ser humano del de obedecer sin cuestionar a sus líderes o superiores, ya que pueden sentir temor de ser despedidos o multados.

2.1.9 Marco de trabajo (*Framework*)

Marco de referencia, marco de trabajo o *framework* es un conjunto estructurado de estándares, conceptos y buenas prácticas destinada a servir de soporte o guía para la construcción o elaboración de una solución que busca resolver una problemática en particular (Rodríguez, 2005).

De acuerdo a los trabajos de Roberto Soriano (Domenech, 2009) y Mark Thomas (Thomas, 2015), quienes toman como referencias las publicaciones de ISACA, consideran como marcos de trabajo (o *framework* en inglés) a: ITIL, ISO, COBIT, NIST, Price2, TOGAF, PMBOK, etc., tal como se muestra en la imagen siguiente:

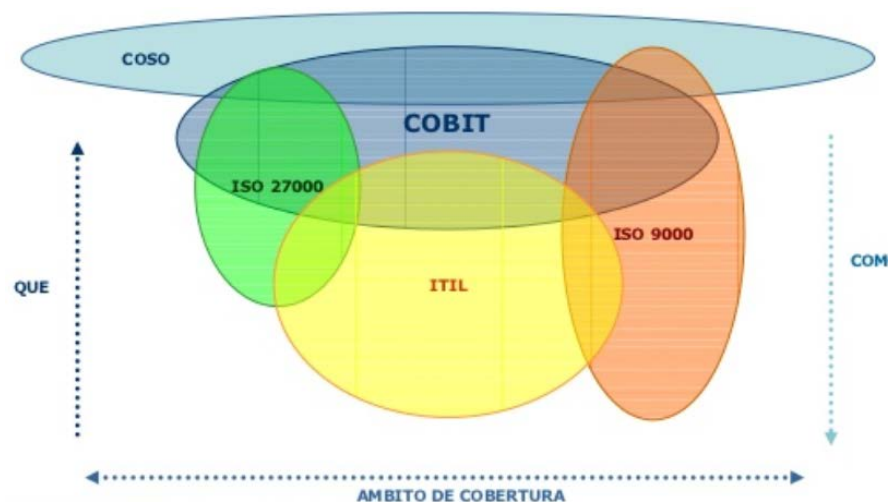


Figura 1 - Cobertura y relación de los marcos de trabajo de TI. **Fuente:** (ISACA, 2015)

Jennifer F. Alfafara autora del artículo “*Overview of Frameworks: Cobit, COSO ITIL ISO COSO, ITIL, ISO, and more*” (Alfafara, 2009) realiza una comparación entre los conceptos *frameworks* versus estándares, dando las siguientes definiciones de *framework*:

- i. Una estructura conceptual de ideas
- ii. Esqueleto o marco estructurado
- iii. Marco de referencia

Mientras que define a un estándar como una regla o principio que es usada para la base de un criterio. Además, este artículo menciona que los motivos por el cual se desarrollan marcos de trabajo o *framework* son: (i) falta de alineamiento entre el negocio y los procesos de tecnología, (ii) proveer guía la Administración de una compañía para asegurar el cumplimiento regulatorio.

Adicionalmente, Alfafara abarca el concepto de *framework* de control (o marco de control), los cuales se definen como un sistema reconocido de actividades de control que cubren los controles internos esperados en una organización, y, además, para ser más exactos, para que un *framework* sea reconocido como tal debe al menos:

- i. Proveer o favorecer al ambiente de control,
- ii. Proveer continuamente a la evaluación de riesgos,
- iii. Aportar para el diseño, implementación y mantenimiento de controles, políticas y procedimientos efectivos.
- iv. Aportar sobre la información y comunicación.

- v. Aportar en el monitoreo y seguimiento de la eficacia de las políticas y procedimientos, así como también la resolución de problemas identificados por los controles.

2.1.10 Marcos de referencia de TI

En la actualidad existen marcos de trabajo, normas, estándares y metodologías globalmente aceptadas relacionadas a la seguridad de la información, gestión de riesgos de TI, gobierno y gestión de TI, arquitectura empresarial de TI, etc. A continuación, se detallan las más importantes:

ITIL

Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información), frecuentemente abreviada ITIL, es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI (ITIL, 2016).

COBIT

Desarrollado y patrocinado por ISACA, COBIT es un marco de trabajo de gobierno empresarial de TI que ayuda a las Organizaciones a crear un valor óptimo a partir de la TI,

al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

COBIT, su versión más reciente (COBIT 5) permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas (ISACA, 2015).

ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (ISO/IEC, 2013).

2.1.11 Adopción de una perspectiva teórica

Para lograr construir el marco de trabajo, se tomará como base las metodologías, y estándares de TI existentes a nivel global. Esto permitirá definir un estado del arte que sirva de línea base para conocer los aspectos que estas metodologías abordan en relación a la gestión de riesgos de ingeniería social, de tal modo que este sea el insumo principal para el diseño del modelo a desarrollar.

2.2 ESTADO DEL ARTE

Parte fundamental del presente trabajo es el análisis sobre publicaciones de artículos científicos, proyectos de titulación y otros documentos que han aportado sobre la temática de ingeniería social. Se ha revisado algunos de estos documentos y se considera relevante mencionar los siguientes:

Del análisis realizado al trabajo de Sergio Arcos Sebastián, titulado “Ingeniería social, aplicada a la seguridad informática” (Sebastián, 2011), se puede concluir que la ingeniería social depende de dos grandes factores: la psicología del ser humano y el componente tecnológico. El autor llega a esta conclusión mediante una investigación de 5 casos suscitados en los últimos 18 años. A continuación, se realiza un análisis esquematizado de uno de estos casos donde se puede inferir la separación del componente técnico y el psicológico

Evento	Análisis técnico	Análisis Psicológico
<p><i>Virus “I Love You”</i></p> <p>Malware que en mayo de 2000 ocasionó el bloqueo de más de 2200 servidores a nivel global originando pérdidas de más de 3 millones de dólares</p>	<p>El virus fue escrito en <i>Visual Basic</i> de <i>Microsoft</i> y explotaba las siguientes vulnerabilidades:</p> <ul style="list-style-type: none"> - Brecha de seguridad en el sistema operativo: la configuración por defecto de <i>MS Windows</i> traía activada por defecto la opción que permitía interpretar scripts del lenguaje VBS. - Modificación de la extensión original: debido a que el sistema operativo leía los ficheros de derecha izquierda hasta encontrar el primer punto, se generaba la sensación de ser un archivo de texto, y debido a que, 	<p>Más allá del alto nivel de complejidad técnico del virus, el mismo no podría haber tenido éxito si no se explotaban los siguientes factores psicológicos:</p> <ul style="list-style-type: none"> - Falta de alertas visuales: el sistema operativo no mostraba ningún mensaje de alerta que prevenga la ejecución de ficheros que requieren privilegios de administrador. En la actualidad, los sistemas operativos de <i>Microsoft</i> despliegan un mensaje de advertencia, que, si bien no elimina el malware, reduce

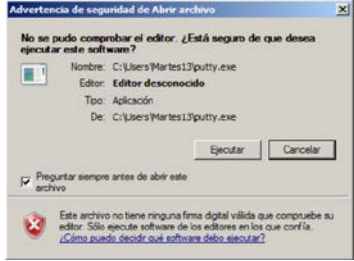
Evento	Análisis técnico	Análisis Psicológico
	<p>además, el ícono de un archivo de texto era el mismo que el de las extensiones .VBS, daba la sensación de ser un fichero de texto válido.</p> <ul style="list-style-type: none"> - Propagación de virus por Internet: parte del éxito de este <i>malware</i> estuvo en su rápida propagación mediante el uso de la función <i>spreadtoemail()</i>, la cual se encarga de leer la agenda de MS Outlook y enviar un correo con el virus a todos los contactos de la agenda. - Uso del registro del sistema: una de las funciones que hizo que el virus fuera difícil de erradicar, era el hecho de que el mismo se apoderaba del registro del sistema e iniciarse automáticamente cada vez que el equipo se reiniciaba. - Uso de scripts ActiveX: el malware creaba un fichero con la extensión HTM, el cual se enviaba por mIRC, aprovechando la activación de <i>ActiveX</i> en el navegador para poder ejecutar el código de <i>VBScript</i>, el cual contenía también el virus 	<p>considerablemente su propagación.</p>  <p>Figura 2 - Mensaje de advertencia en Windows. Fuente: (Sebastián, 2011)</p> <p>Además, el ícono que se usaba para identificar un fichero de <i>VisualBasic</i> era muy similar al de un fichero de texto.</p> <ul style="list-style-type: none"> - Uso de palabras amigables: el hecho de que el autor del virus haya usado palabras como “love”, “letter”, “you” ayudó a que los usuarios que recibieron el virus mediante e-mail, asocien a este correo con algo agradable, lo cual a su vez generó un estímulo positivo. - Remitente de confianza: el virus se propagó mediante el envío automático de correos a todos los contactos de las agendas de MS Outlook, lo cual tuvo como efecto que el nivel de propagación sea alto debido a que las personas que recibían el correo de parte de alguien conocido y de confianza.

Tabla 1: Análisis del virus “I love you”.
Fuente: (Sebastián, 2011). **Elaborado por:** Autor.

Por otro lado, se ha analizado el artículo científico de Katharina Krombholz, Heidelinde Hobel, Markus Huber y Edgar Weippl, denominado “Advanced Social Engineering Attacks” (Krombholz, Heidelinde , & Hube, 2016). Del análisis de este artículo se puede destacar la clasificación taxonómica de la ingeniería social, ya que, de acuerdo a los autores, estos ataques suelen ser multifacéticos. La clasificación se la puede realizar dependiendo de tres factores: (i) el tipo, (ii) el operador, (iii) el canal.

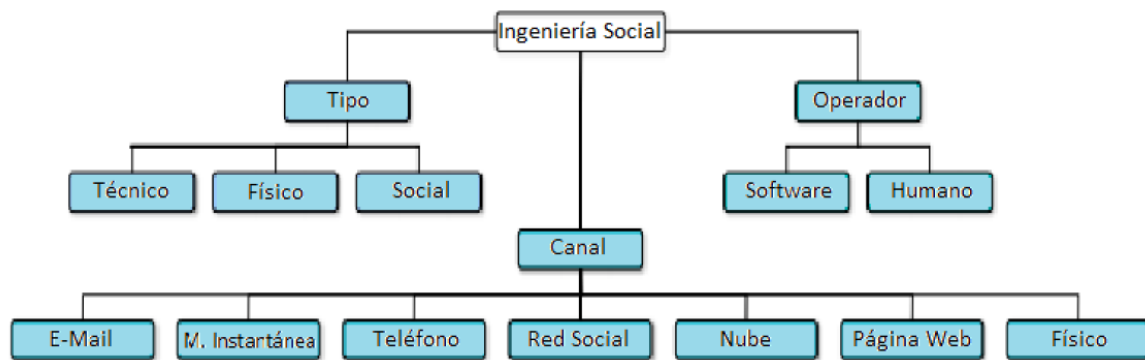


Figura 3 - Clasificación de los ataques de ingeniería social de acuerdo a sus características. **Fuente:** (Krombholz, Heidelinde, & Hube, 2016)

Adicionalmente, el artículo propone un mapeo entre la taxonomía de ingeniería social y los diversos tipos de ataques actuales (Ver tabla 2). Esta clasificación puede servir como referencia para el marco de trabajo a diseñar, ya que permite esquematizar de manera más estructurada las políticas, procedimientos y controles a elaborar. Por ejemplo, según la tabla 2, existen diferentes tipos de ataques asociados al canal físico, lo cual se relaciona con los vectores de ataques de: *phishing*, husmear por encima del hombro, escarbar en la basura, ingeniería social a la inversa y *baiting*. Estos ataques podrían evitarse o el riesgo asociado a

estos mitigarse, con la implementación de procedimientos o controles efectivos de seguridad física.

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Threat	Baiting
Channel	E-mail	✓			✓		✓	
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓	✓	✓

Tabla 2: mapeo entre la taxonomía de ingeniería social
Fuente: (Krombholz, Heidelinde , & Hube, 2016).

Otro de los artículos que se ha analizado es el *paper* “*Social Engineering 2.0: A Foundational Work*” (2017), escrito en colaboración por Davide Ariu, Enrico Frumento y Giorgio Fumera. El análisis realizado a este *paper* permite concluir que existen tres factores principales que han evolucionado en el ámbito de la ingeniería social en los últimos años, siendo estos:

- **Tecnología:** en la actualidad, la tecnología tiene mayor presencia en la sociedad a través de teléfonos inteligentes, *wereables*, redes sociales y demás, esto ha abierto la puerta para que nuevos riesgos aparezcan.

- **Sociedad:** la forma de interactuar de las personas también ha evolucionado de la mano de la tecnología. Cada vez existen más experiencias virtuales que físicas, y es más común que actividades “humanas” estén integradas a las redes sociales. Esto lleva a concluir que la tecnología está cambiando las maneras tradicionales que los seres humanos han conservado por mucho tiempo.
- **Ciber-crimen:** cada vez se habla más sobre la futura guerra cibernética, aquel conflicto cuyos protagonistas no serán soldados ni armas, si no, *hackers* y computadoras. Servicios emergentes como el “CaaS” (Ciber-crimen como servicio por sus siglas en inglés), invita a pensar que las organizaciones deben blindarse aún más, en todos los ámbitos, incluyendo a sus usuarios de tecnología.

La evolución de estos factores son los que han contribuido al surgimiento de lo que los autores denominan el fenómeno Ingeniería Social 2.0. La figura 4 muestra las principales características de la Ingeniería Social 2.0

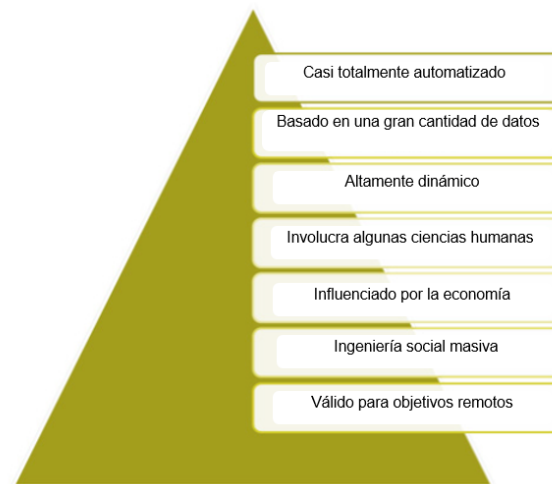


Figura 4 - Características de la Ingeniería Social 2.0. **Fuente:** (Hansen, 2017)

Se considera que lo expuesto en este artículo científico puede servir de referencia significativa para la elaboración del marco de trabajo de ingeniería social, debido a que brinda información de vectores de ataques actuales y sus características, lo cual permitirá incluir dentro del análisis, factores de riesgos emergentes y por ende, el framework a desarrollar podrá contar con una visión de procedimientos y controles a la vanguardia de la situación actual de la temática de ingeniería social.

Además, se ha seleccionado el trabajo denominado “Proyecto SAVE”, un estudio auspiciado por la Universidad Royal Danish Defence College y desarrollado por el Instituto Danés de Bomberos y Seguridad Informática de Dinamarca (DBI). Este estudio presenta los resultados de la aplicación de 185 vectores de ataque realizados de forma controlada a tres instituciones danesas definidas como objetivo, utilizando principalmente las técnicas de: *spear-phishing*, *whaling*, *phishing* convencional, *smishing*, ataques con archivos PDF y dispositivos USB.

Como punto de partida, el proyecto SAVE realiza una clasificación de los objetivos de sus ataques (targets) de acuerdo a lo detallado en la tabla 4.

Núm.	Objetivo	Definición
1	Organización	Compañía, empresa, organización
2	Grupo	Oficina o departamento
3	Individuo	Empleado en específico

Tabla 4: Clasificación de objetivos de ataques. **Fuente:** (Hansen, 2017)

Los vectores de ataques realizados a los tres objetivos se repartieron de la siguiente

forma:

Vector de ataque	Objetivo 1	Objetivo 2	Objetivo 3	Descripción del ataque
<i>Spear-Phishing</i>	3	1	3	Son ataques de <i>phishing</i> con la característica de ser dirigidos y personalizados basados en la información obtenidos en la fase de reconocimiento
<i>Whaling</i>	1	1	1	Estos tipos de ataques se focalizan en individuos de alto rango (CEOs, CTO, etc.), es decir, personas con acceso a información altamente valiosa.
<i>Phishing</i> convencional	2	4	146	Son aquellos ataques que mediante el envío de un email que parece ser legítimo, los atacantes logran que la víctima comparta información confidencial (por ejemplo contraseñas)
<i>Smihing</i>	3	5	9	Es el tipo de <i>phishing</i> que se realiza mediante el uso de mensajes de texto (SMS)
Ataques vía USB	0	0	3	Consiste en deliberadamente abandonar un dispositivo USB para que la víctima lo inserte en su equipo mientras se ejecuta algún virus u otro proceso malicioso que busca robar información o bloquear el equipo.
Ataques vía archivos PDF	1	2	0	Se trata de que la víctima abra un archivo PDF que es enviado por correo electrónico, con el fin de que se ejecuten procesos que buscan ejecutar código malicioso.

Tabla 5: Resumen de los vectores de ataques usados en el proyecto SAVE,
Fuente: (Hansen, 2017). **Elaborado por:** Autor.

Este interesante estudio muestra los siguientes resultados, resumidos en la siguiente matriz:

Vector de ataque	Objetivo 1	Objetivo 2	Objetivo 3	Promedio
<i>Spear-Phishing</i>	0 %	100 %	100 %	67 %
<i>Whaling</i>	0 %	0 %	100 %	33 %
<i>Phishing</i> convencional	100 %	100 %	40 %	80 %
<i>Smishing</i>	100 %	80 %	89 %	90 %
Ataques vía USB	-	-	0 %	0 %
Ataques vía archivos PDF	100 %	50 %	-	50 %

Tabla 6: Resumen de los resultados de vectores de ataques analizados en SAVE,
Fuente: (Hansen, 2017). **Elaborado por:** Autor.

Este estudio muestra que el *smishing* fue el vector de ataque más explotado (90 %), seguido del *phishing* convencional (80 %) y el *spear-phishing* con el 67 %; es decir, los 3 tipos de ataques de *phishing* fueron los más exitosos; en su contrapartida, el ataque relacionado a una interacción física tuvo menor éxito.

El nivel de detalle de este estudio, mediante la aplicación de vectores de ataque en casos reales, permite identificar de mejor forma los riesgos que son explotados en los ataques de ingeniería social, principalmente para los vectores de ataque actuales. Se concluye que este análisis permitirá enfocar la atención de las políticas, procedimientos y controles con mayor énfasis en los casos que resultaron con mayor éxito.

Se puede resumir el aporte de los artículos científicos analizados en el estado del arte de la siguiente manera:

Título	Autor	Tipo	Aporte						
			Factores técnicos	Factores psicológicos	Estructura / Clasificación	Riesgos de IS Emergentes / Actuales	Aplicación en casos reales		
Ingeniería social, aplicada a la seguridad informática	Sergio Arcos Sebastián	Trabajo de titulación	✓	✓					
<i>Advanced Social Engineering Attacks</i>	Katharina Krombholz, Heidelinde Hobel, Markus Huber y Edgar Weippl	Artículo científico	✓	✓	✓				
<i>Social Engineering 2.0: A Foundational Work</i>	Davide Ariu, Enrico Frumento y Giorgio Fumera	Artículo científico	✓	✓		✓			
Proyecto SAVE	Universidad <i>Royal Danish Defence College</i> y desarrollado por el Instituto Danés de Bomberos y Seguridad Informática de Dinamarca (DBI).	Estudio aplicado	✓	✓		✓	✓		

Tabla 7: Resumen de aporte de los artículos analizados. **Elaborado por:** Autor.

CAPÍTULO III

ANÁLISIS SITUACIONAL

En el presente capítulo se realizará un análisis situacional de los tres principales componentes de este trabajo: es decir: análisis de los factores psicológicos, análisis de técnicas de ingeniería social y análisis de los marcos de referencia de TI. Los resultados serán la base del marco de trabajo a desarrollar.

3.1 Análisis de los factores psicológicos

Como ya se ha mencionado, tanto en el marco teórico como en el estado del arte, es importante identificar aquellas características, conductas y comportamientos propios del ser humano que son explotadas en los ataques de ingeniería social. Esto se realizará mediante análisis de diferentes vectores de ataque, así como también de eventos suscitados.

3.1.1 La psicología como factor incidente de la ingeniería social

Kevin Mitnick, reconocido *hacker* a nivel mundial, por sus infiltraciones conocidas en diferentes organizaciones, más que ser un experto informático es considerado un experto ingeniero social. Precisamente, Mitnick (2008) enunció los cuatro principios de la ingeniería social:

- Todos queremos ayudar
- El primer sentimiento siempre es de confianza hacia los demás.
- No nos gusta decir “No”

- Todos queremos ser alabados.

Se procederá a tomar como pilares los cuatro factores enunciado por Mitnick para entender las connotaciones de los seres humanos que generan los riesgos de ingeniería social.

Todos queremos ayudar (Solidaridad)

Charles Chaplin (1951) manifestó: “Todos queremos ayudar el uno al otro. Los seres humanos son así. Queremos vivir de la felicidad de los demás, no de la miseria de los demás.”.

Esta cita invita a reflexionar sobre el hecho de que el ser humano por naturaleza posee ese instinto de ayudar a los demás y probablemente se deba a que biológicamente nuestro cuerpo genera un sentimiento de bienestar y alivio cuando ayuda a otra persona más, es decir, ayudar genera en el ser humano un sentimiento de satisfacción.

Por otro lado, el ser humano desde su génesis buscó estar siempre acompañado, nuestros aborígenes vivían en colonias y siempre procuraban interactuar con la comunidad, ya que, como es conocido, el ser humano no es una entidad perfecta y no posee todas las habilidades que le permiten hacer todo lo que desee, por lo que siempre existe alguna situación en la que requiere la habilidad que alguien más posee.; es decir, la capacidad y predisposición de ayudar del ser humano nació con el ser humano mismo, sin importar el ámbito en el que se desenvuelva.

Esta característica de ayudar a los demás inclusive ha sido objeto de investigaciones científicas, ya que, por ejemplo, en una de las últimas obras de Springer, llamada *Rigins of*

Altruism and Cooperation (2014), el autor concluye que los seres humanos somos altruistas y cooperativos por naturaleza, al contrario de lo que se creía: egoístas, violentos u hostiles.

Por definición, la capacidad de ayudar a los demás de manera desinteresada se conoce como solidaridad. Según la organización sin fines de lucro *InspirAction* (2012), la solidaridad puede clasificarse en dos grupos:

- **Solidaridad circunstancial:** es cuando se da algo material como dinero, alimentos o materiales para un fin en particular. Por ejemplo, cuando ocurre alguna catástrofe natural, las personas suelen emprender campañas de recolección de víveres, medicinas, entre otros.
- **Solidaridad de compromiso:** este tipo de solidaridad se presenta cuando una persona se compromete a sacrificar su vida y su tiempo a ayudar a otras personas. Los casos más conocidos son el de las monjas, voluntarios de bomberos, cruz roja, entre otros.

Esta capacidad de ayudar a los demás no es solo cosa de los seres humanos, ya que, por ejemplo, en agosto de 1996, un gorila rescató y protegió a un niño de tres años que había caído desde la zona de visitantes de un zoológico en Estados Unidos. El gorila tomó al niño y lo entregó a los encargados del zoológico sano y salvo (La Vanguardia, 2016).

Todo esto invita a reflexionar que el comportamiento de ayudar a los demás es una conducta propia de la humanidad por naturaleza, quien inclusive muchas veces no es consciente de que lo es o está haciendo.

Análisis del factor Solidaridad

El *tailgating* es uno de los tipos de ataque de ingeniería social que se aprovecha de la predisposición de las personas a ayudar a los demás, ya que usualmente los *hackers* propician situaciones en las que se presentan de tal forma que avocan ayuda de alguien más -por ejemplo, con las manos ocupadas con alguna caja pesada- para que de esta forma alguien más abra la puerta por ellos y así ganar acceso a un lugar inicialmente no autorizado.

Uno de los casos de ataque social que usó la técnica de *tailgating* ocurrió en el Reino Unido, en donde un consultor de seguridad de Siemens logró obtener acceso físico a las instalaciones de uno de sus clientes donde después de alocarse en una sala por varios días, se hizo pasar por un analista de soporte de TI para obtener las credenciales de acceso (usuario y contraseña) de al menos 17 empleados, consiguiendo así acceso a información confidencial. Según lo manifestado por el consultor Creenless en el artículo de *Computerworld UK* (2017), bastó con esperar a que una persona abra la puerta por él al verlo con las manos ocupadas con dos tazas de café.

Otro ejemplo de ataques que toman ventaja de la solidaridad se presenta posterior a eventos catastróficos, tal es el caso suscitado en 2015, donde posterior al terremoto de Nepal, los *hackers* enviaron múltiples ataques de *phishing* que estaban camuflados en correos que solicitaban donaciones para organizaciones ficticias, cuando realmente contenían archivos adjuntos o *links* maliciosos.

El primer sentimiento es de confianza (Confianza)

Según Jack Gibb (1978). “la confianza es un término difícil de definir, ya que es una vivencia que se siente y no se piensa, es algo parecido al amor, es una experiencia que se

da libremente” Este autor es uno de los más reconocidos en esta temática, llegando a manifestar en su libro *Trust* lo siguiente: “La confianza implica un sentimiento instintivo, una creencia incuestionable en algo o alguien, es libremente otorgada, es similar al amor y su presencia o ausencia puede producir grandes diferentes en nuestras vidas.” (Gibb ,1978).

Los seres humanos tendemos a confiar, antes de inclusive razonar; esto se debe a que las personas buscan en primer lugar mantener relaciones intrapersonales importantes (amistades, compañeros de trabajo, familia). Según Mario Morales Vergara (2000), reconocido psicólogo, los seres humanos, desde que nacemos buscamos sentir confianza, ya sea en ámbito social como personal, ya que la confianza –al igual que la desconfianza– son sentimientos elementales para el desarrollo del ser humano

Análisis del factor Confianza

Como se ha mencionado, es innato del ser humano la predisposición a confiar en los demás, lo que genera una vulnerabilidad que podría minimizar cualquier esfuerzo enfocado a proteger la información. Esto se puede observar en ataques que usan la imagen de instituciones reconocidas o de instituciones de renombres, tales como: bancos, instituciones privadas o gubernamentales, etc., De acuerdo con un estudio de Kaspersky Labs (2017), uno de cada tres ataques de *phishing* son dirigidos a bancos, los cuales principalmente hacen uso de las instituciones financieras de mayor reputación en sus sectores, tomando ventaja de la imagen de confianza que generan estas instituciones.

No nos gusta decir “No” (Colectivismo)

En Tailandia, también conocida como la “tierra de las sonrisas” no existe la palabra “No” (BBC, 2017) y es que probablemente la población de ese país sea la muestra más

fehaciente de que los seres humanos nos desarrollamos bajo una consigna de colectivismo, amabilidad y orientación al servicio.

Para entender mejor esta connotación, se debe comprender que el evitar dar una respuesta negativa ante un requerimiento de alguien más, puede estar dado por las razones siguientes enunciadas por Francisco Sáez, fundador de la *start-up*, *FacileThings* (2017)

- **Queremos ayudar**

Como se mencionó anteriormente, los seres humanos hemos sido históricamente solidarios, ya que ayudar nos hace parecer ser más empáticos, amables y generosos, por el contrario, no ayudar nos hace ver como egoístas.

- **Tememos al rechazo**

Los seres humanos tenemos el instinto de querer caer bien a los demás, buscando siempre su aprobación. Esto se debe a que históricamente los seres humanos evitan ser marginados, ya que compartir con otras personas genera mayores beneficios que el estar solos.

- **Respeto a los demás**

Muchas personas simplemente pueden llegar a creer que no ayudar a otro va en contra de sus principios y educación, y en ciertos modos, esto genera sensaciones de incomodidad o insatisfacción personal.

- **Temor a los enfrentamientos**

Los seres humanos desde sus inicios tuvieron que luchar y confrontarse con animales, bestias e inclusive con otros seres humanos para poder subsistir; sin

embargo, con el paso del tiempo, los recursos eran cada vez más accesibles y los hombres se acostumbraron a dejar de luchar, a su vez que vivieron los beneficios del evitar confrontaciones. Esta tendencia a evitar conflictos se reforzó con el paso de los tiempos y hoy en día es evidenciable cada vez más.

- **Sentimiento de culpabilidad o miedo**

El sentirse culpable genera inquietud en las personas, por eso, para encontrar tranquilidad, las personas a menudo evitan decir “no” para evadir esta incómoda sensación

- **Temor a perder oportunidades**

Cuando las personas se rehúsan a ayudar, se genera una percepción de que en el futuro las situaciones pueden revertirse y en caso de que nosotros seamos quienes requiramos la ayuda, no vamos a poder contar con ella.

Análisis del factor Colectivismo

Ya sea porque los seres humanos tenemos la predisposición de ayudar, tenemos miedo al rechazo o evitamos confrontaciones, el colectivismo resume algunos de los comportamientos más explotados por los ataques sociales,

Todos queremos ser alabados (Reconocimiento)

Según la RAE, la palabra reconocimiento está conformada por tres vocablos derivados del latín: “re” que equivale a “repetición”; “cognoscere” equivalente a “conocer”; y, el sufijo “mento” que significa instrumento, por lo tanto, reconocimiento es la acción y efecto de reconocer o reconocerse.

Todo ser humano quiere ser reconocido, los elogios causan sensaciones de bienestar y es motivación que se traduce en energías y ganas de seguir haciendo las cosas bien. El reconocimiento es fundamental en el desarrollo de la autoestima desde niños; es motivación para los empleados en una empresa y es vital en las relaciones intrapersonales, o, dicho en otras palabras, la necesidad de reconocimiento está presente en todos los ámbitos de la vida independientemente de la etapa en la que se encuentre una persona.

Análisis del factor Reconocimiento

Buscar reconocimiento de los demás puede llevar a las personas a compartir información personal en sitios de Internet, por ej. redes sociales. Muchos atacantes escarban en la Web con el objetivo de obtener datos que puedan servir para preparar un ataque más grande. Registrar una visita en *Facebook*, recibir una etiqueta en una foto de *Instagram*, incluir la ubicación en un tuit, etc., son claros ejemplos de lo que hoy en día son hechos frecuentes que generan riesgos que pueden ser usados por ingenieros sociales.

Además de los cuatro principios de la ingeniería social enunciados por Mitnick, existen otros aspectos de la psicología que son enunciados por otros autores y que son válidos para el análisis que se está realizando, por ejemplo, El Dr. Robert Cialdini en su libro *Influence: The Psychology of Persuasion* (1984), describe los siguientes motivadores claves:

Reciprocidad

Un estudio realizado por el profesor Kunz (2017) de la Universidad Brigham Young concluyó que los seres humanos tienden a devolver favores, pagar las deudas y dar el mismo trato que reciben de otros. Por otro lado, un profesor de la Universidad de Cornell convocó

a un grupo de personas a una supuesta evaluación de arte, en la misma, obsequió una botella de Coca Cola al primer de los dos grupos. Luego pidió a ambos grupos la colaboración con la adquisición de boletos para una rifa. Teniendo como resultado que los del primer grupo compraron más papeletas que los del grupo que no recibieron Coca Cola.

La reciprocidad es, por lo tanto, un principio presente en los seres humanos, la cual obliga a devolver los favores que otra persona realiza. Probablemente este principio se desarrolló en las épocas primitivas con el fin de intercambio social; muestra de esto, son las actividades de trueque que favoreció al desarrollo societario de la época.

Esta regla elemental de interacción de los humanos en la mayoría de las ocasiones es instintiva y se realiza de manera inconsciente en las personas, inclusive funciona cuando el valor de lo recibido no es igual al valor de lo dado. Por esto, es altamente probable que una persona que recibió un regalo de cumpleaños también entregue un presente a cambio. Esta regla de interacción de los seres humano es innata e inclusive trasciende aspectos como la cultura. Es que, no ser recíproco puede llegar a ser mal visto y condenado por la sociedad, ya que las personas ingratas o desagradecidas generan desconfianza.

Análisis del factor Reciprocidad

Servicios en línea que ofrecen la posibilidad de descargar juegos, música o convertir formatos de archivos a cambio de información, es un claro ejemplo del uso del factor reciprocidad. Otros casos conocidos se han suscitado cuando ingenieros sociales establecen como objetivo a miembros de alto mando donde juegan un rol falso que les permite compartir información supuestamente confidencial, la cual realmente es falsa, por lo que es altamente probable que la víctima entregue información confidencial a cambio.

Consistencia / Compromiso

Esta conducta humana se refiere al hecho de que las personas de buena salud mental generalmente tienen comportamientos con un sentido de coherencia y con formas de actuar congruentes y similares. No actuar de una misma forma ante escenarios similares puede llegar a ser mal visto por las demás personas, generando así un sentimiento de desconfianza

Análisis del factor Consistencia

Actuar de manera consistente es utilizado por los ingenieros sociales, ya que, mediante el estudio de los hábitos y comportamiento de una persona objetivo, es posible predecir sus acciones futuras y así, conjuntamente con el uso de otras técnicas, puede conseguir que la víctima realice algo por él.

Obsecuencia / Autoridad

La obsecuencia se define como la sumisión, extrema amabilidad o alta predisposición a obedecer a la autoridad. Esta característica no es innata del ser humano, ya que lo normal es que cada uno busque hacer lo que desee; sin embargo, las diferentes sociedades y agrupaciones de las que el ser humano ha formado parte (por ejemplo: tribus, familia, colegio, trabajos) se ha encargado de inculcar este comportamiento. El temor a sanciones, castigos u otra consecuencia negativa hace que esta conducta se presente en determinados escenarios.

Hoy en día, las empresas, compañías y cualquier tipo de organización cuentan con estructuras jerárquicas en diferentes niveles; es decir, siempre existe una figura de autoridad, sobre la cual se genera un sentido de respeto y obsecuencia. Ser un buen empleado puede tener algunas connotaciones, de las cuales, el ser obediente y no refutar la

voluntad de los superiores es un comportamiento propio de un empleado que busca inspirar confianza para ser tomado en cuenta y así obtener algún tipo de reconocimiento

Análisis del factor Obsecuencia

Jugar el rol de una persona de alto rango es una técnica común utilizada por los ingenieros sociales para obtener acceso a información confidencial. Otro claro ejemplo de obsecuencia frecuentemente usado, se da cuando un supuesto analista de mesa de servicio solicita las credenciales de acceso a un determinado usuario para poder solventar algún problema ficticio que el mismo *hacker* pudo haber creado.

A más de los aportes de Mitnick y Cialdini, otros autores han identificado otras conductas psicológicas como aspectos incidentes en los riesgos de ingeniería social, entre ellos:

Principio de urgencia o escasez

Este factor se refiere al comportamiento que puede llegar a tener un ser humano ante una situación que genera presión por realizar o conseguir algo. Este principio también conocido como principio de escasez, actúa como un acelerador en la toma de decisiones de las personas, haciendo que muchas veces no se consideren todos los factores o variantes de una determinada situación. Ejemplos puntuales de este principio son los avisos de “últimos boletos disponibles”, “alguien más también está interesado en tu artículo”, “descuento válido solo por hoy”.

Análisis del factor urgencia

Anuncios de correos electrónicos como “Reclame su premio solo por hoy”, o “Microsoft cerrará su cuenta de Outlook si no completas tu información inmediatamente”

son claros ejemplos de ataques de ingeniería social que buscan aprovecharse del sentido de urgencia que se puede llegar a causar en las personas.

Similitud / Caer bien

Nacer en la misma ciudad, atender a la misma iglesia, apoyar al mismo equipo de fútbol o compartir los mismos gustos musicales son ejemplos de similitud de comportamientos en los seres humanos. Cuando se presentan estas situaciones, las partes involucradas generan un lazo común que conlleva a que las personas mantengan un trato especial y favorable.

Análisis del Factor de Similitud

Según Robert Cialdinin (2015), es mucho más probable que seamos más accesibles y demos mayores facilidades a las personas con las que compartimos algún tipo de gusto, ya que tener similitud con otra persona generalmente se traduce en “caer bien”, lo cual puede ser usado por ingenieros sociales para llevar a cabo tareas maliciosas.

Prueba social / Consenso

El hecho de que los seres humanos, ante situaciones de duda, nos guiemos basados en lo que hacen los demás puede conllevar a que se realicen acciones diferentes a las que la persona realmente desea. Comprar un producto porque alguien más lo hizo, visitar un restaurante porque tiene buenas referencias o votar por el candidato con mayores probabilidades de ganar, son claros ejemplos la prueba social.

Análisis del factor prueba social

En Internet existen sitios de Internet falsos, los cuales invitan a unírnos o visitar determinados sitios *Web* que poseen buenas referencias o un alto número de visitantes, llegando a ser en algunos casos, sitios *Web* con referencias al número de “likes”. Por ejemplo, un *hacker* puede aparentar tener muchos amigos en Facebook para conseguir la confianza de la víctima y así obtener información valiosa para un ataque informático.

3.2 Análisis de las técnicas de ingeniería social

La matriz siguiente, resume el análisis de las técnicas de ingeniería social desde la perspectiva de los factores de riesgos psicológicos y los componentes de categorías de ataques informáticos. Se ha considerado las siguientes características a ser analizadas:

Categoría de ataque: tomando lo analizado en el estado del arte, se plantea considera las categorías de técnico, físico y social. Se ha considerado definir al nivel de relevancia de categoría en dos formas: Primario y Secundario.

Factor psicológico asociado: se considerará los factores identificados en el análisis anterior, siendo estos: solidaridad, reciprocidad, confianza, colectivismo, reconocimiento, obsecuencia, urgencia y consistencia.

Canal: se refiere al mecanismo que podría ser usado para explotar una vulnerabilidad de ingeniería social, siendo estos: e-mail, mensajería instantánea, redes sociales, *cloud*, sitios *web*, físico

Operador del ataque: hace referencia a la entidad que lleva cabo el ataque de ingeniería social, pudiendo ser: humano o computador.

Nivel de automatización: de acuerdo al análisis a realizar, se la podrá categorizar en:
alto, medio y bajo

Objetivos: en este apartado se incluirá a qué o quién está dirigido el ataque, pudiendo ser:
una persona común, un grupo de personas o una organización (empresa, compañía, etc.).

Vector de ataque	Características		Análisis
<i>Phishing</i>	Categorías de ataques informáticos	Técnico	<p>S</p> <p>Dependiendo del ataque, un hacker puede hacer uso de las siguientes técnicas de <i>phishing</i>:</p> <ul style="list-style-type: none"> • Deceptive Phishing: esta técnica es probablemente la más usada en el <i>phishing</i>. En este caso, los hackers roban la identidad de alguna institución reconocida y envían correos a sus clientes con el fin de obtener cualquier información confidencial, como, por ejemplo: credenciales de accesos, información de tarjetas de crédito, etc.
		Físico	
		Social	

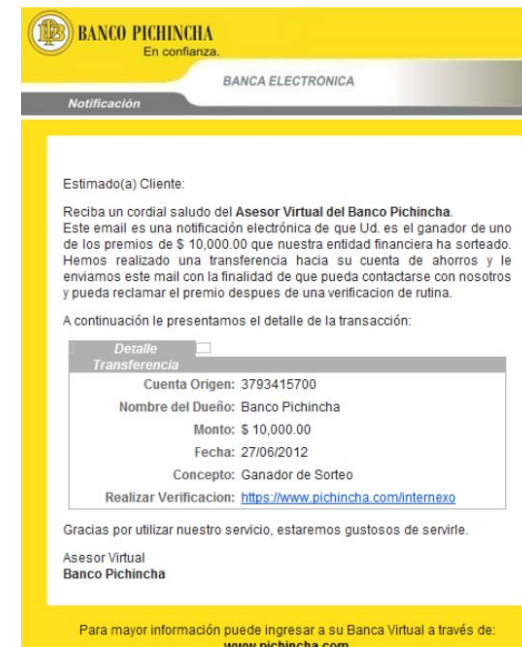


Figura 5 - Correo de phishing usando imagen del Banco Pichincha. **Fuente:** (Journalistika 2.0, 2011)

Vector de ataque	Características	Análisis
------------------	-----------------	----------

- **Malware-Based Phishing:** en este tipo de ataques, se busca que la víctima ejecute algún software malicioso, el cual puede venir como archivo adjunto en un correo o archivo descargable de un sitio web.

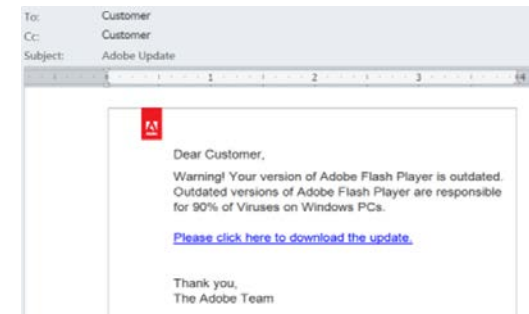


Figura 6 - Ejemplo de correo de Malware-phishing. **Fuente:** (Experian, 2015)

- **DNS-Based Phishing:** esta técnica también conocida como *pharming* se trata de que los cibercriminales manipulan los archivos del sistema de nombres de dominio (DNS) de una empresa para que, de este modo, las solicitudes de direcciones URL sean redirigidas a un sitio web falso.

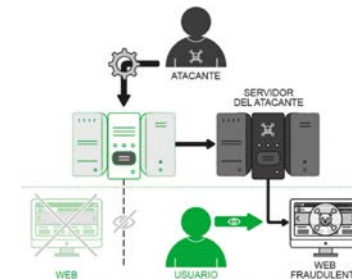


Figura 7 - Esquema de operación de un ataque phishing basado en DNS. **Fuente:** (Corchado, 2017)

Vector de ataque	Características	Análisis
------------------	-----------------	----------

- **Content-Injection Phishing:** en estos ataques, los *hackers* reemplazan parcialmente el contenido de un sitio web verdadero por componentes falsos con el fin de engañar al usuario para que entregue información sensible.



Figura 8 - Ejemplo de ataque de tipo Content-Injection. **Fuente:** (Experian, 2015)

- **Search Engine Phishing:** en este caso, los atacantes crean sitios web de búsquedas para redireccionar al usuario a sitios web falsos. Uno de los casos recientes más conocidos, fue el de Banco español Sadabell, donde los atacantes lograron introducir una página falsa mediante el servicio de GoogleAdwards, haciendo que el sitio web malicioso aparezca por encima del oficial en las búsquedas de Google, de este modo, lograron que muchos de sus clientes entreguen credenciales a los hackers (Falero, 2015).

Vector de ataque	Características	Análisis
------------------	-----------------	----------

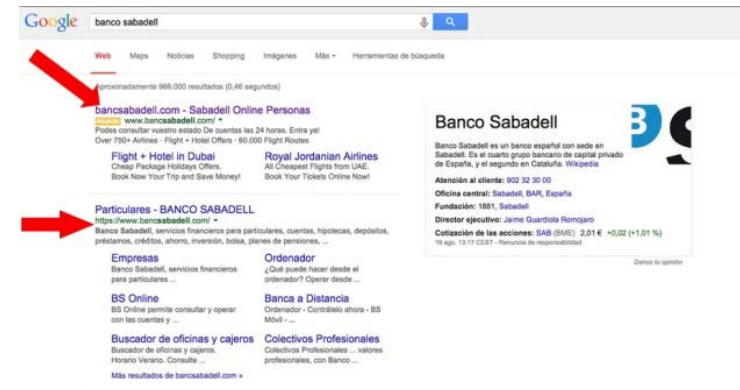


Figura 9 - Ejemplo de ataque de Search Engine Phishing. **Fuente:** (Falero, 2015)

Según un estudio de ESET las principales técnicas que los hackers utilizan para realizar ataques de phishing son (Paus, 2015):

- **Acortadores o modificadores de URLS:** los ciberdelincuentes tratan de usar un dominio similar al original, con la diferencia de la ubicación del punto (“.”).



Figura 10 - Ejemplo de uso de acortadores de URL. **Fuente:** (Paus, 2015)

Vector de ataque	Características	Análisis
		<ul style="list-style-type: none"> - Inyección de Iframes: los Iframes son líneas de código fuente que permite colocar un elemento HTML dentro de otro objeto HTML principal. Desde la perspectiva del usuario, esta se visualiza como una ventana dentro de la ventana principal del navegador Web (Pérez, 2015). Esto podría permitir a los atacantes modificar el código fuente de un sitio web, de forma que al usuario se le presente un Iframe dentro del sitio real y así engañar a la víctima - Uso de técnicas ligadas a los marcos de código HTML: En este tipo de ataques permiten modificar partes de código fuente con el fin de introducir códigos HTML que puede ser usado para capturar datos ingresados o alterar vínculos para redirigir a sitios web maliciosos (Pérez, 2015).
Factor psicológico asociado	Solidaridad	✓
	Reciprocidad	✓
	Confianza	✓
	Colectivismo	✓
	Reconocimiento	✓
	Obsecuencia	✓
	Urgencia	✓
		<p>Dependiendo del objetivo o víctima, cuando se refiere a <i>Phishing</i>, el atacante puede aprovechar prácticamente cualquiera de los factores psicológicos incluidos en el presente trabajo. Según la Oficina de Seguridad de Internauta (2014), los principales motivos pueden ser:</p> <ul style="list-style-type: none"> - Problemas de carácter técnico - Nuevas recomendaciones de seguridad para prevención del fraude - Cambios en la política de seguridad - Promoción de productos, premios o regalos - Inminente desactivación del servicio - Falsas ofertas de empleo - Notificación de ser el ganador de algún premio - Solicitud de ayuda social - Envío de documentos de un contacto conocido - Órdenes dictadas por el Jefe o dueño de la compañía.


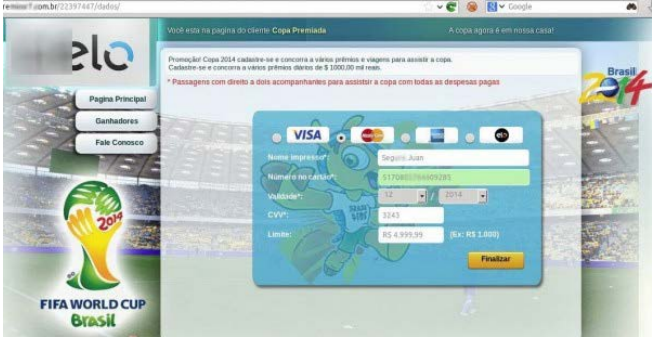
Vector de ataque	Características	Análisis
	Consistencia ✓	<p>Los correos conocidos como <i>spam</i> o correos basura son una muestra de ataques de <i>phishing</i>. Por ejemplo, los e-mails que notifican ser el ganador de premios o ser el beneficiario de una herencia son casos de phishing que buscan aprovecharse del sentido de urgencia y de la consistencia de las personas.</p> <p>De igual manera, los atacantes suelen aprovecharse de los eventos más conocidos o los que son tendencia para llevar a cabo este tipo de ataques. Tal es el caso de que, en septiembre de 2010 un correo electrónico era distribuido entre miles de personas el cual prometía dar acceso a imágenes satelitales de las zonas afectadas por un terremoto en Ecuador (Bortnik, 2010). Los usuarios que hacían clic en el enlace del correo obtenían el archivo “epicentro_terremoto.exe”, el cual era un malware.</p> 

Figura 11 - Correo que descargaba malware haciendo uso del evento de un terremoto en Ecuador.
Fuente: (Bortnik, 2010)

Vector de ataque	Características	Análisis
		<p>Otro caso de <i>phishing</i> que buscaba aprovecharse de la confianza y curiosidad de las personas, se presentó en Brasil previo al Mundial de Fútbol del 2014 . El correo prometía boletos para ver un partido de fútbol a cambio de datos personales y financieros (claves de tarjeta de crédito). Lo llamativo de este caso es que el sitio real sí estaba sorteando entradas a los partidos del Mundial, lo cual fue aprovechado por los hackers para engañar de manera más fácil a los usuarios (Charkiewicz, 2014).</p> 
Canal	E-mail	✓
	Mensajería instantánea	✓
	Redes sociales	✓
	Cloud	✓
		<p>Según un estudio de McAfee Labs, el correo electrónico es el principal mecanismo utilizado por los <i>hackers</i> para llevar a cabo técnicas de ingeniería social Dicho estudio muestra que el número de correos de spam supera 2 y 3 veces al número de correos legítimos (Samani & McFarland, Hacking the Human Operating System, 2015).</p> <p>Si bien el principal canal de ataque es el correo electrónico, existen otros casos en los que se utilizan otros canales, por ejemplo:</p>

Vector de ataque	Características	Análisis
	Sitios Web	✓
	Físico	-
		<ul style="list-style-type: none"> - Uso de redes sociales: se han presentado casos, en los cuales los hackers contactan a las víctimas por redes sociales o mensajerías instantánea, intentado persuadir a sus víctimas para que accedan a un link (por eje. link para hacer video llamadas) y así lograr que la víctima instale un malware - Uso de <i>cloud</i>: en este caso, los ciberdelicuentes suben archivos maliciosos a sitios <i>cloud</i> (Google Drive, Dropbox), los cuales son compartidos en sitios abiertos tales como: foros, chats, etc. Por ejemplo, un foro de video juegos puede incluir links a archivos malicioso en vez de permitir la descarga del videojuego.
Operador del ataque	Humano	✓
	Computador	✓
		<p>Los ataques de phishing son realizados en su mayoría por una persona con la ayuda de computadoras o equipos tecnológicos, con proporciones particulares dependiendo del tipo de ataque.</p> <p>El componente Computador brinda ciertos indicios que permitirían identificar un ataque, por ejemplo:</p> <ul style="list-style-type: none"> - El destinatario de correo - El tipo de certificado que usa - Uso de portal de <i>scams</i> - Sitios falsos de Internet.
Nivel de automatización	Alto	✓
	Medio	-
	Bajo	-
		<p>El nivel de automatización de un ataque de <i>phishing</i> puede llegar a ser alto, dependiendo de la sofisticación de los equipos tecnológicos, por ejemplo, un atacante puede hacer uso de herramientas de envío masivo de correo, así como también puede llevar a dirigir un ataque al servidor de nombres de una organización (DNS).</p>
Objetivos	Organización	P

Vector de ataque	Características		Análisis
	Grupo	S	Según un estudio de Panda Security (2017) los ataques <i>phishing</i> han estado dirigidos a organizaciones, siendo las instituciones bancarias uno de los sectores más vulnerados.
	Individuo	S	

Vector de ataque	Características			Análisis
Smishing	Categorías de ataques informáticos	Técnico	S	Si bien hoy en día los <i>smartphones</i> con sus aplicaciones y sistemas de mensajería instantánea (por eje. <i>Whatsapp</i> , <i>Telegram</i> , <i>Messenger</i>) prácticamente dominan el mundo de la comunicación, los viejos y conocidos mensajes de texto no dejan de ser un mecanismo habitual de comunicación para instituciones como bancos u otras Entidades. Esto ha sido aprovechado por los hackers para llevar a cabo ataques de ingeniería social. Este tipo de ataques principalmente se aprovecha de las brechas de seguridad de índole social, ya que aparentemente, para los usuarios, los mensajes de texto son más confiables que los e-mails, por lo que es menos probable que una víctima sospeche que está siendo parte de un ataque. Técnicamente hablando, no se requiere de grandes herramientas o complejos algoritmos para llevar a cabo este tipo de ataques, ya que es suficiente con el hecho de contar con una aplicación que permita enviar SMS de manera masiva.
		Físico	-	
		Social	P	
	Factor psicológico asociado	Solidaridad	✓	Debido que el <i>Smishing</i> es un subtipo de <i>phishing</i> , los factores de riesgo psicológicos que pueden ser vulnerados son exactamente los mismos que los analizados en la matriz anterior.
		Reciprocidad	✓	
		Confianza	✓	

	Colectivismo	✓	De acuerdo a un artículo de la BBC, el <i>smishing</i> se vale del sentido de urgencia que se encuentra inmerso en los mensajes SMS (Tecnología, 2017).
	Reconocimiento	✓	
	Obsecuencia	✓	
	Urgencia	✓	
	Consistencia	✓	
Canal	E-mail		Particularmente el <i>Smishing</i> únicamente se vale del canal de mensajería, el cual es ampliamente usado por las instituciones financieras para la autenticación de dos pasos; además, este es un método de comunicación aún es usado por aquella generación que no dispone de un <i>Smartphones</i> pero igual precisan acceder a datos o consultas de estados de cuentas de sus bancos, etc. Asimismo, los atacantes utilizan esta técnica para engañar a las víctimas, de modo que estas hagan clic sobre el enlace y así se logre redireccionar a sitios ilegales o se descargue algún malware.
	Mensaj. Inst.	✓	
	Redes sociales		
	Cloud		
	Sitios Web		
	Físico		



Figura 13 - Ejemplo de ataque *Smishing*. **Fuente:** (Cluley, 2016)

Operador del ataque	Humano	✓	Los ataques de <i>Smishing</i> pueden ser realizados por una persona (humano) o con la ayuda de equipos informáticos. Hoy en día, aplicaciones como MDirector, SMS UP, Altiria, Mensatek, etc., permiten enviar SMS masivos a grupos de usuarios, de modo que se puede dirigir un ataque de IS.
	Computador	✓	
Nivel de automatización	Alto		Este tipo de ataques no necesitan de un alto mayor de automatización para llevarlo a cabo, ya que puede bastar con un simple celular con paquete de SMS o simples herramientas de envío masivos de SMS.
	Medio	✓	
	Bajo		
Objetivos	Organización	P	Los objetivos que principalmente buscan los ataques de <i>smishing</i> son las organizaciones, luego, le siguen los grupos y finalmente a nivel de individuo.
	Grupo	S	
	Individuo	S	

Vector de ataque		Características		Análisis
Vishing	Categorías de ataques informáticos	Técnico	S	Esta técnica es una derivación del phishing tradicional y se basa en el engaño mediante llamadas telefónicas. En estos ataques, el <i>hacker</i> busca obtener información de la víctima mediante la persuasión e influencia, valiéndose de herramientas que falsean u ocultan la información del atacante. Solo en 2012, más de 2.4 millones de personas habían sido víctimas de este tipo de ataques (López Grande & Guadrón, 2015)
		Físico	-	
		Social	P	
				Uno de los ataques más conocidos llevado a cabo mediante <i>vishing</i> , es el que en el cual, la víctima que toma la llamada falsa, escucha una grabación donde se advierte sobre algún peligro con su tarjeta de crédito y solicita que se llame a un número

			falso para que sea cambiada; una vez que la víctima cae en la trampa, los datos son recabados por el atacante para luego ser utilizados con fines fraudulentos
			En tal sentido, el componente social juega un papel fundamental en este tipo de ataques y posiblemente, el componente técnico sea uno de los menos complejos de utilizar.
Factor psicológico asociado	Solidaridad	✓	En el año 2017, medios locales reportaron que personas malintencionadas se aprovecharon de una campaña de recolección de fondos para niños sin hogar para recibir donaciones de manera ilegal, en Chile (Paus, 2015).
	Reciprocidad	✓	
	Confianza	✓	
	Colectivismo	✓	Un ejemplo del uso de <i>vishing</i> que explota el factor humano de obsecuencia podría ser cuando un nuevo empleado es solicitado de compartir su <i>password</i> por un atacante que finge ser un tipo del área de seguridad y que precisa verificar que sus nuevas contraseñas cumplen con la política interna. Después el <i>hacker</i> da algunas recomendaciones a la víctima, de modo que pueda tener la posibilidad de adivinar el patrón de sus futuras contraseñas.
	Reconocimiento	✓	
	Obsecuencia	✓	
	Urgencia	✓	Este factor psicológico y más factores están presentes en los diferentes vectores de ataques, ya que al ser un ataque
	Consistencia	✓	
Canal	E-mail		De acuerdo a un estudio de McAfee realizado en 2014, el teléfono fue uno de los canales de comunicación usados por los atacantes para llevar a cabo ataques de Ingeniería Social, el cual es el principal medio de uso de este tipo de <i>phishing</i> .
	Mensaj. Inst.		
	Redes sociales		
	Cloud		
	Teléfono	✓	
	Físico		
Operador del ataque	Humano	✓	Este tipo de ataque puede ser ejecutado por una persona o por un computador. Por ejemplo, en febrero de 2017, un atacante logró obtener información personal de
	Computador	✓	

			más de 9000 empleados del FBI mediante una llamada telefónica (Motherboard, 2016) .
			Por otro lado, existen ataques que se apoyan de máquinas contestadoras con mensajes pregrabados que amenazan a los usuarios con dejar de prever un determinado servicio si no se entrega alguna información confidencial.
Nivel de automatización	Alto		Debido a la no complejidad de los factores que inciden en este tipo de ataques, no se identifican niveles de automatización alto.
	Medio	✓	
	Bajo		
Objetivos	Organización	✓	Los ataques de <i>vishing</i> están dirigidos principalmente a organizaciones, especialmente aquellas con un alto número de empleados donde es imposible que todos los empleados se conozcan entre sí, haciendo que el hacerse pasar por alguien más sea algo menos complejo.
	Grupo		
	Individuo		

Vector de ataque		Características		Análisis
<i>Spear-Phishing</i>	Categorías de ataques informáticos	Técnico	S	La principal diferencia entre el <i>spear-phishing</i> y el <i>phishing</i> tradicional, es que el primero de estos es un ataque mucho más elaborado y personalizado en su contenido.
		Físico	-	
		Social	P	
Factor psicológico asociado	Factor psicológico asociado	Solidaridad	✓	Dado que el <i>spear-phishing</i> es una derivación del phishing, los factores psicológicos que explotan estos ataques son exactamente iguales a los del <i>phishing</i> .
		Reciprocidad	✓	
		Confianza	✓	
		Colectivismo	✓	
		Reconocimiento	✓	
		Obsecuencia	✓	
		Urgencia	✓	
		Consistencia	✓	

Canal	E-mail	✓	El canal por el cual se llevan a cabo los <i>spear-phishing</i> pueden ser: email, servicios de mensajería instantánea, uso de redes sociales, uso de servicios <i>cloud</i> y sitios web; en todos los casos, el principal objetivo radica en que las víctimas accedan a link que puede contener <i>malware</i> , por lo que el canal del correo electrónico es el más usado en este tipo de ataques.
	Mensaj. Inst.	✓	
	Redes sociales	✓	
	Cloud	✓	
	Sitios Web	✓	
	Físico	-	
Operador del ataque	Humano	✓	Ambos componentes son necesarios para llevar a cabo un ataque de <i>spear-phishing</i> ; in embargo, el uso de herramientas computadorizadas es ampliamente necesario, ya que al ser un ataque altamente customizado se requiere de aplicaciones que permitan copiar o imitar sitios web, falsear correos electrónicos, entre otros.
	Computador	✓	
Nivel de automatización	Alto		Se considera que el nivel de automatización es bajo, dado que difícilmente va a ser posible llevar a cabo estos ataques sin la creatividad y nivel de personalización que una persona pueda darle.
	Medio		
	Bajo	✓	
Objetivos	Organización	✓	Al ser ataques altamente personalizados, estos son dirigidos especialmente a personas específicas dentro de una organización o fuera de ellas.
	Grupo		
	Individuo	✓	

Vector de ataque		Características		Análisis
Whaling	Categorías de ataques informáticos	Técnico	S	Este es un ataque derivado del <i>phishing</i> que tiene como principal objetivo el atacar a personal de rango alto (CEOS, Directores Ejecutivos, etc.), ya que son personas que muy probablemente poseen acceso a información confidencial.
		Físico	-	
		Social	P	
Factor psicológico asociado	Factor psicológico asociado	Solidaridad		Dado que el <i>whaling</i> es una derivación del <i>phishing</i> , los factores psicológicos que explotan estos ataques son exactamente iguales a los del <i>phishing</i> pero con especial énfasis en los factores de consistencia y obsecuencia, ya que por ejemplo, un atacante puede aprovecharse de los comportamientos usuales y predictivos de los altos mandos para vulnerar su cuenta de correo y con esto aprovecharse de su posición para solicitar información a subordinados o exigir que se realicen actividades que favorezcan al atacante.
		Reciprocidad		
		Confianza		
		Colectivismo		
		Reconocimiento		
		Obsecuencia	✓	

Canal	Urgencia		Al ser un tipo especial de <i>phishing</i> , los canales que pueden ser usados por el <i>whaling</i> son los mismos que los del <i>phishing</i> , con especial énfasis en aquellos que los altos directivos suelen usar (E-mail, Internet)
	Consistencia	✓	
	E-mail	✓	
	Mensaj. Inst.	✓	
	Redes sociales	✓	
	Cloud	✓	
	Sitios Web	✓	
Operador del ataque	Físico	-	Los ataques de <i>whaling</i> usualmente son llevados a cabo por personas mediante el uso de computadoras o herramientas informáticas.
	Humano	✓	
Nivel de automatización	Computador	✓	Se considera que el nivel de automatización es bajo, dado que difícilmente va a ser posible llevar a cabo estos ataques sin la interacción de una persona.
	Alto		
	Medio		
Objetivos	Bajo	✓	Los ataques de <i>whaling</i> usualmente están dirigidos a altos funcionarios de organizaciones cuando lo que buscan es información particular de una empresa; también pueden darse ataques enfocados a individuos cuando lo que se busca es obtener beneficios de alguna figura pública, ya sean estos económicos o de reconocimiento.
	Organización	S	
	Grupo	S	
	Individuo	P	

Vector de ataque		Características		Análisis
Información de libre acceso	Categorías de ataques informáticos	Técnico	S	Hoy en día, la información disponible en Internet es sumamente significativa.
		Físico	-	Las redes sociales, tales como Facebook, Instagram o LinkedIn han creado un mundo en donde la información es cada vez más fácil de obtener.
		Social	P	
		Solidaridad		Estos ataques principalmente se aprovechan de los factores siguientes:
		Reciprocidad		

Factor psicológico asociado	Confianza	✓	<ul style="list-style-type: none"> - Confianza, ya que las personas suelen subir su información a las redes sociales, confiando plenamente en que su información se encuentra segura. - Reconocimiento: otro factor relevante que incide es el reconocimiento o validación social, ya que muchas personas que suben su información a Internet, lo hacen con el fin de buscar reconocimiento de su círculo social.
	Colectivismo		
	Reconocimiento	✓	
	Obsecuencia		
	Urgencia		
	Consistencia		
Canal	E-mail		<p>Los canales que pueden ser aprovechados por los atacantes de manera principal son:</p> <ul style="list-style-type: none"> - Redes sociales: ya que, dependiendo del nivel de configuración, es posible que allí exista información altamente valiosa. Por ejemplo, <i>Facebook</i> dispone de algunas funcionalidades que facilitan la compartición de información sensitiva, por ej. la funcionalidad “Amigos cerca” permite conocer la ubicación de personas que se encuentran en un determinado rango de distancia. “Estoy aquí” es la funcionalidad de <i>Facebook</i> que permite a sus usuarios indicar dónde se encuentran exactamente. De igual manera, Twitter permite a los usuarios indicar desde donde escriben un tuit. - Sitios Web: los portales de Internet son un buen repositorio en la cual el atacante puede obtener información pública. - Físico: información impresa o escrita en papel que en muchas ocasiones no es correctamente almacenada (por ej. documentos de escritorios en las oficinas). <p>Herramientas como Pipl, WebMii, Yasni, PeekYou, Spokeo permiten que cualquier persona pueda obtener información de alguien más únicamente conociendo sus nombre o dirección de correo.</p>
	Mensaj. Inst.		
	Redes sociales	✓	
	Cloud		
	Sitios Web	✓	
	Físico	✓	

Dirección domiciliaria, cuentas de redes sociales, número de teléfono son algunos ejemplos de los datos que pueden ser obtenidos en estos sitios

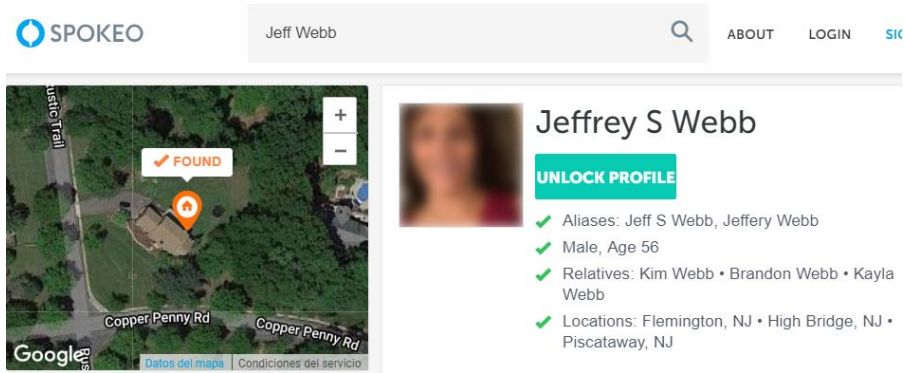


Figura 14 - Ejemplo de información obtenida con Spokeo. Fuente: Spokeo¹

Los operadores y comandos de Google son también una buena herramienta de libre acceso que permitiría escarbar por la red y conseguir información valiosa.

Operador del ataque	Humano	✓	La información de libre acceso puede ser recabada por personas o mediante el uso de software que automatizan la colección de datos.
	Computador	✓	
Nivel de automatización	Alto		Considerando las técnicas avanzadas de búsqueda, se puede considerar el nivel de automatización como medio, en relación a los demás vectores de ataque de Ingeniería Social
	Medio	✓	
	Bajo		
Objetivo	Organización	✓	

¹ Spokeo; <https://www.spokeo.com/>

		Grupo	✓	Este tipo de ataques puede ser dirigido a organizaciones, grupos de personas o individuos en particular, dependiendo de lo que el hacker busca obtener.
		Individuo	✓	
Vector de ataque		Características		Análisis
Escarbar en basura / Trashing	Categorías de ataques informáticos	Técnico		Este tipo de ataque es netamente físico, ya que requiere de la intervención de una persona que se encargue de hurgar en la basura para poder obtener algún tipo de información confidencial o información útil para preparar un ataque mayor. Procedimientos documentados, contraseñas, credenciales de acceso, agendas, anotaciones, reportes, discos duros o memorias USB, son algunos de los ejemplos de las cosas que pueden encontrarse en la basura de las organizaciones
		Físico	P	
		Social	S	
	Factor psicológico asociado	Solidaridad		Confiar en que en los desechos no existe información valiosa o en que nadie va a intentar buscar en ella, es el principal factor social que influye para que este tipo de ataques tenga éxito.
		Reciprocidad		
		Confianza	✓	Además, el comportamiento consistente de las personas permite que se puedan dar este tipo de ataques, ya que, la rutina básica de poner la basura en su lugar, recolectar internamente y ubicarla en el punto de recogida para ser enviada en los camiones recolectores, puede llegar a ser una rutina muy predecible que puede facilitar el trabajo a los atacantes.
		Colectivismo		
		Reconocimiento		
		Obsecuencia		
		Urgencia		
		Consistencia	✓	
	Canal	E-mail		El <i>trashing</i> es un vector de ataque que requiere ser realizado en su totalidad por una persona, es decir, es un ataque físico.
		Mensaj. Inst.		

Vector de ataque	Características		Análisis
		Redes sociales	
		Cloud	
		Sitios Web	
		Físico	
	Operador del ataque	Humano	Al ser un ataque cien por ciento físico, el operador del ataque en todos los casos es una persona.
		Computador	
	Nivel de automatización	Alto	Este tipo de ataques no suelen tener procedimientos automatizados
		Medio	
		Bajo	
	Objetivos	Organización	Este tipo de ataques principalmente están orientados a organizaciones, las cuales están conformadas por un alto número de empleados, haciendo que la probabilidad de que alguien deseche información confidencial, sea alta
		Grupo	
		Individuo	

Vector de ataque	Características		Análisis
Piggybacking o tailgaiting	Categorías de ataques informáticos	Técnico	El <i>piggybacking</i> o el <i>tailgaiting</i> es un tipo de ataque físico porque requiere de la acción de una persona de manera presencial; también se considera social porque suele aprovecharse del comportamiento amable o cortés de las personas.
		Físico	
		Social	
			En algunos casos los atacantes se aprovechan del descuido o desatención de las personas para colarse en zonas no autorizadas; mientras que, en otras ocasiones, el

			atacante puede interactuar con las personas para ganarse la confianza y hacerles creer que es un empleado de la compañía y que olvidó su credencial. También, es posible que el atacante se presente con las manos ocupadas y apele al sentido de cordialidad de un usuario autorizado para que este sostenga la puerta por él.
Factor psicológico asociado	Solidaridad	✓	Los factores psicológicos que son vulnerados en este tipo de ataques son: - Solidaridad: las personas tienden a ser amables y ayudar los demás, lo cual puede ir desde mantener la puerta abierta hasta habilitar el ascensor a alguien más. - Confianza: como se mencionó anteriormente, las personas tienden a confiar primero antes que desconfiar; sobre todo cuando el atacante juega un rol de una persona amigable y con buena presencia.
	Reciprocidad		
	Confianza	✓	
	Colectivismo		
	Reconocimiento		
	Obsecuencia		
	Urgencia		
	Consistencia		
Canal	E-mail		El canal que habilita este ataque es cien por ciento físico.
	Mensaj. Inst.		
	Redes sociales		
	Cloud		
	Sitios Web		
	Físico	✓	
Operador del ataque	Humano	✓	Este es un tipo de ataque netamente físico.
	Computador		
	Alto		

	Nivel de automatización	Medio		Al ser un ataque netamente físico, no existe nivel de automatización.
		Bajo	✓	
	Objetivos	Organización	✓	Este tipo de ataques están dirigidos principalmente a organizaciones, sobre todo aquellas donde existe un alto número de empleados.
		Grupo		
		Individuo		
Vector de ataque		Características		Análisis
Sex appeal	Categorías de ataques informáticos	Técnico		El uso del <i>sex appeal</i> es primariamente una técnica social que puede llegar a ser física.
		Físico	S	
		Social	P	Uno de los casos de ingeniería social más conocidos que se basó en el uso de <i>sex appeal</i> fue el experimento “Robin Sage”
		Solidaridad		Apelar al atractivo físico sin duda es una forma de ataque social que busca vulnerar comportamientos humanos básicos como el de fraternizar o tener
		Reciprocidad	✓	

Factor psicológico asociado	Confianza	✓	<p>relaciones sentimentales, lo cual se relaciona con los factores psicológicos de reciprocidad, confianza y reconocimiento, de la siguiente manera:</p> <ul style="list-style-type: none"> • Reciprocidad: Robin Sage aparentaba ser amable y compartía falsos secretos de estado a cambio de confesiones de sus contactos reales. • Confianza: muchos de las víctimas confiaron en la buena apariencia de Sage, así como también en los datos falsos que ella publicó en sus redes sociales. En algunos de los casos donde no tuvo éxito, las víctimas se tomaron la molestia de verificar su información y corroborar que se trataba de un perfil falso. • Reconocimiento: parte del comportamiento de Robin Sage fue el de hacer cumplidos a sus víctimas, así como también destacar las intachables trayectorias de sus víctimas.
	Colectivismo		
	Reconocimiento	✓	
	Obsecuencia		
	Urgencia		
	Consistencia		
Canal	E-mail	✓	El uso de sex appeal puede realizarse principalmente por canales electrónicos, ya que no exponen directamente al atacante; siendo los canales más usados las redes sociales y los servicios de mensajería instantánea.
	Mensaj. Inst.	✓	
	Redes sociales	✓	
	Cloud		El canal físico si bien es menormente utilizado, no deja de ser una vía para este tipo de ataques, ya que, por ejemplo, una atacante puede persuadir a su víctima en algún evento social haciendo uso de su atractivo físico.
	Sitios Web		
	Físico	✓	
Operador del ataque	Humano	✓	Debido al nivel de sofisticación de este tipo de ataques, el operador es, en la mayoría de los casos, una persona. Sin embargo, se han identificado ataques que inician mediante correo electrónicos que son enviados por máquinas.
	Computador	✓	
Nivel de automatización	Alto		El nivel de automatización de estos ataques puede variar dependiendo de la estrategia del atacante, ya que puede ir desde mecanismos cien por
	Medio	✓	

		Bajo		ciento físicos y que dependen de una persona, hasta el uso de software de envío de correos masivos.
Objetivos		Organización	✓	Este tipo de ataques puede estar dirigido a un individuo o a un empleado de la compañía, dependiendo del objetivo del atacante.
		Grupo	✓	
		Individuo	✓	
Vector de ataque		Características		Análisis
Espionaje de oficina	Categorías de ataques informáticos	Técnico		Este tipo de ataque tiene un componente social amplio, ya que requiere de que una persona se prepare con anticipación para poder infiltrarse en la vida real, por lo que debe tener mucho cuidado, ya que su identidad es conocida y puede verse comprometida.
		Físico	S	
		Social	P	
	Factor psicológico asociado	Solidaridad		Este vector se aprovecha de la confianza que se genera dentro de un ámbito de trabajo, ya que es completamente normal generar confianza con las personas con las que se comparte en la oficina, lo cual se refiere a un comportamiento esperado en las personas, es decir, se es consistente.
		Reciprocidad		
		Confianza	✓	
		Colectivismo		
		Reconocimiento		
		Obsecuencia		
		Urgencia		
		Consistencia	✓	
Canal		E-mail		El canal que habilita este ataque es cien por ciento físico.
		Mensaj. Inst.		

	Redes sociales		
	Cloud		
	Sitios Web		
	Físico / Otro	✓	
Operador del ataque	Humano	✓	Este tipo de ataques son llevado a cabo por personas de manera presencial
	Computador		
Nivel de automatización	Alto		Al ser ataques físicos y presenciales, no se considera posible automatizar estos tipos de ingeniería social.
	Medio		
	Bajo	✓	
Objetivos	Organización	✓	Los ataques de espionaje de oficina, tal y como su nombre lo indica, está orientado netamente a organizaciones, principalmente aquellas con un alto número de empleados, ya que vuelve más complejo el detectar este tipo de infiltraciones.
	Grupo	✓	

En la matriz siguiente, se resume el análisis realizado a cada vector de ataque. Se ha marcado con un tono rojizo (tono más fuerte = relevancia primaria, tono más leve = relevancia secundaria) aquellos puntos donde ya sea la categoría, el factor psicológico, el canal, el operador de ataque, el nivel de automatización o el objetivo de ataque es relevante para cada vector de ataque. Desde la perspectiva de riesgos, se puede determinar que los cuadros marcados de tono rojizo representan un riesgo asociado a las características del vector de ataque que requiere atención.

Vector de ataque	Categoría			Factor psicológico								Canal							Operd		Automatiz,			Objetivo		
	Técnico	Físico	Social	Solidaridad	Reciprocidad	Confianza	Colectivismo	Reconocimiento	Obsecuencia	Urgencia	Consistencia	E-mail	Mensaj. Inst.	Redes sociales	Cloud	Teléfono	Sitios Web	Físico / Otro	Humano	Computador	Alto	Medio	Bajo	Organización	Grupo	Individuo
Phishing																										
Smishing																										
Vishing																										
Spear-Phishing																										
Whaling																										
Info de libre acceso																										
Trashing																										
Shoulder surfing																										
Piggybacking o tailgaiting																										
Sex appeal																										
Baiting																										
Uso de redes WiFi																										
Espionaje de oficina																										

3.3 Análisis de las normas y marcos de referencia de TI

Un componente fundamental del presente trabajo es el definir una línea base, la cual tomará como referencia a los marcos de referencia globalmente aceptados en el ámbito de tecnologías de la información. La idea es identificar si estos poseen información, tales como lineamientos o buenas prácticas que puedan ser tomados como base para el diseño del modelo a proponer.

Como se analizó en el capítulo dos, las metodologías a considerar son: COBIT, ITIL, ISO 27002, NIST 800-50.

3.3.1 Análisis de COBIT 5

El Modelo de referencia de COBIT 5 considera 5 dominios y un total de 37 procesos. A continuación, resumimos el propósito y objetivo con el fin de identificar si existen conceptos que aporten a la gestión de riesgos de ingeniería social (ISACA, 2015):

Evaluar, Orientar y Supervisar (EDM): este es el dominio de COBIT que aborda los conceptos de gobierno de TI. Tiene como principal meta, asegurar que los objetivos de empresa se logren mediante la evaluación y atención de las necesidades de las partes interesadas.

Alinear, Planear, Organizar (APO): este dominio de gestión de COBIT contempla la definición de estrategias y tácticas, identificando las formas en el que mediante el uso de las TI puede ayudar a que el negocio logre sus objetivos estratégicos.

Construir, Adquirir e Implementar (BAI): en este dominio se encuentran los procesos de gestión enfocados a que los proyectos tecnológicos se traduzcan en obtención de beneficios para los *stakeholders*, de acuerdo al presupuesto y tiempos, teniendo en cuenta las actividades de mantenimiento y operaciones posteriores.

Entregar, Dar Servicio y Soporte (DSS): abarca todo lo relacionado a la entrega de servicios tecnológicos, considerando las prioridades de la empresa, optimización de costos, operaciones eficientes y seguras alcanzando los criterios de seguridad de la información.

Supervisar, Evaluar y Valorar (MEA): obtiene, valida y evalúa el cumplimiento de los objetivos del negocio mediante el uso de métricas con el fin de reportar de manera estructurada el nivel de apoyo de los objetivos de TI hacia la empresa.

Resumen de análisis COBIT 5

En la siguiente matriz se resume el aporte de los diferentes dominios de COBIT a la temática de Ingeniería Social:

Dominio	Aporte	Observaciones
Evaluar, Orientar y Supervisar	No	El proceso EDM04. Asegurar la optimización de recursos, aborda el concepto de recursos humanos desde una perspectiva de disponibilidad y uso eficiente de las personas y demás recursos tecnológicos. <i>Conclusión:</i> Por lo expuesto en el párrafo anterior, se considera que este proceso no aporta a la gestión de riesgos de ingeniería social.
Alinear, Planear, Organizar	No	El proceso APO07. Gestionar los Recursos Humanos se enfoca principalmente a garantizar que exista una estructura definida y clara, con responsabilidades y capacidades de decisión y niveles de autoridad claramente definidos y comunicados <i>Conclusión:</i>

Dominio	Aporte	Observaciones
		Por lo expuesto en el párrafo anterior, se considera que este proceso no aporta a la gestión de riesgos de ingeniería social.
Construir, Adquirir e Implementar	No	El proceso BAI08. Gestionar el Conocimiento se enfoca en la provisión de conocimiento al personal a cargo de actividades relacionadas a TI con el fin de facilitar la toma de decisiones. Conclusión: Por lo expuesto en el párrafo anterior, se considera que este proceso no aporta a la gestión de riesgos de ingeniería social.
Entregar, Dar Servicio y Soporte	No	En este dominio no existen conceptos relacionados a la ingeniería social o al factor humano.
Supervisar, Evaluar y Valorar	No	En este dominio no existen conceptos relacionados a la ingeniería social o al factor humano.

Tabla 8: Análisis de la aplicabilidad los dominios COBIT 5. **Elaborado por:** Autor.

En conclusión, COBIT 5 es un marco de referencia enfocado al gobierno y gestión de las TI en la empresa, de la cual no se ha identificado procesos o actividades que sirvan de referencia para el marco de gestión que pretende desarrollar este trabajo.

3.3.2 Análisis de ITIL

Recordando la definición de ITIL, es un conjunto de buenas prácticas para la gestión de servicios de TI, permite anticipar que esta metodología posee un enfoque muy claro: los servicios de TI. Esto se puede corroborar al realizar un breve repaso por las diferentes etapas que contiene esta librería (ITIL, 2016):

Estrategia del servicio: esta etapa busca alinear la estrategia de TI con los objetivos de la organización, de modo que las diferentes decisiones generen valor en el negocio.

Diseño del servicio: en esta etapa se busca asegurar que los servicios de TI a ofrecer dentro de la organización posean características que consideren aspectos como costos, desempeño y funcionalidades, siempre alineado y procurando alcanzar los objetivos de la organización.

Transición del servicio: esta fase procura asegurar que los servicios de TI, ya sean nuevos o existentes, atiendan a necesidades explícitas de la empresa, manteniendo un control adecuado sobre todas las actividades de mantenimiento y cambios.

Operación del servicio: esta etapa se refiere específicamente a la forma en la que el servicio es llevado a cabo, buscando mantener criterios de seguridad y confiabilidad en concordancia con los objetivos de la organización.

Mejora continua del servicio: se refiere en adoptar buenas prácticas orientadas a mejorar la calidad del servicio de manera constante procurando la eficiencia y optimización de costos.

Resumen de análisis ITIL

En la siguiente matriz se resume el aporte de las diferentes etapas de ITIL a la temática de Ingeniería Social:

Dominio	Aporte	Observaciones
Estrategia del servicio	No	De acuerdo al análisis individual de cada una de las etapas de ITIL, se puede concluir que el enfoque de ITIL es enteramente orientado a los servicios de
Diseño del servicio	No	
Transición del servicio	No	
Operación del servicio	No	
Mejora continua del servicio	No	

TI, y no aborda prácticas asociadas a la gestión de riesgos de ingeniería social

Tabla 9: Análisis de aplicabilidad de los dominios ITIL. **Elaborado por:** Autor.

En conclusión, ITIL es un marco de referencia enfocado al servicio de TI por lo que se considera que no existen procesos o actividades que sirvan de referencia para el marco de gestión que pretende desarrollar este trabajo.

3.3.3 Análisis de ISO 27002

Este estándar contiene 14 dominios, 25 objetivos de control y 114 controles propuestos por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La siguiente matriz resume el análisis realizado sobre los 14 dominios e incluye el aporte que se planea sea tomado como controles base que serán parte del diseño del marco de gestión de riesgos de ingeniería social.

Dominio ISO 27002	Aplicable	Controles a considerar
Políticas de seguridad de la información	Si	5.1 Directrices de la Dirección en seguridad de la información. 5.1.1 Conjunto de políticas para la seguridad de la información.
Organización de la seguridad de la información	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo

Dominio ISO 27002	Aplicable	Controles a considerar
Seguridad relativa a los recursos humanos	Si	7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la información. 7.2.3 Proceso disciplinario. 7.3 Cese o cambio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo
Gestión de activos	Si	8.3 Manejo de los soportes de almacenamiento. 8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes.
Control de acceso	Si	9.2 Gestión de acceso de usuario. 9.2.4 Gestión de información confidencial de autenticación de usuarios 9.4 Control de acceso a sistemas y aplicaciones. 9.4.3 Gestión de contraseñas de usuario
Criptografía	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo
Seguridad física y del entorno	Si	11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos 11.1.6 Áreas de acceso público, carga y descarga.
Seguridad de las operaciones	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo
Seguridad de las comunicaciones	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo
Adquisición, desarrollo y mantenimiento de los sistemas de información	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo
Relación con proveedores	Si	15.1 Seguridad de la información en las relaciones con suministradores. 15.1.1 Política de seguridad de la información para suministradores.

Dominio ISO 27002	Aplicable	Controles a considerar
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
Gestión de incidentes de seguridad de la información	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo
Cumplimiento	No	Se considera que no existen controles relevantes que puedan aportar al diseño del marco de trabajo

Tabla 10: Análisis de aplicabilidad de los procesos ISO 27003. **Elaborado por:** Autor.

3.3.4 Análisis de NIST 800-50

El Instituto Nacional de Estandarización y Tecnología (NIST por sus siglas en inglés) es una agencia del departamento de Comercio de los Estados Unidos de América que tiene como responsabilidad el desarrollo de estándares técnicos, físicos, administrativos y de gestión con el objeto de garantizar la efectividad de seguridad y privacidad de los datos que se almacenan o transmiten mediante equipos de tecnología. Este Instituto ha publicado una serie de informes relacionados a la Tecnologías de la Información mediante la serie 800.

Precisamente, la publicación 800-50, contiene un programa denominado “Construyendo un programa de concientización y entrenamiento sobre la seguridad de la información” el cual busca ser una guía enfocada a atender tres conceptos claves sobre la seguridad de la información: la concientización, el entrenamiento y la educación.

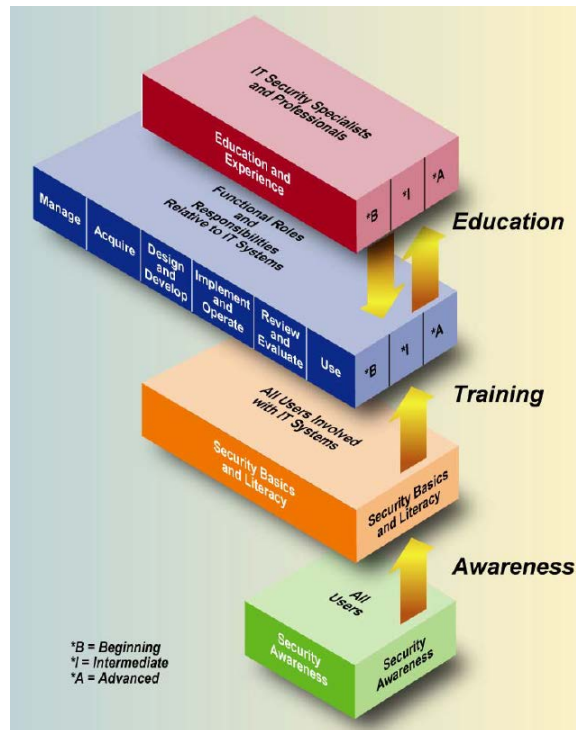


Figura 15 - Visión general de los componentes definidos por la NIST 800-50. **Fuente:** NIST 800-50

Concientizar

Este término puede ser confundido con “entrenar”; sin embargo, según NIST son dos conceptos diferentes, ya que el principal propósito de la concientización es el lograr que las personas pongan la atención requerida en el concepto de “seguridad”, en otras palabras, es lograr que un usuario común incluya esta palabra en su mente y logre pensar en seguridad en cada una de las actividades que realiza. Por ende, este componente implica a todos los usuarios de una organización, incluyendo proveedores.

Entrenar

Según NIST, entrenar se refiere a crear o desarrollar habilidades y competencias enfocadas a las personas que desempeñan una función ligada a la seguridad de la información (gerentes de TI, desarrolladores, auditorías, operadores, etc.); es decir, entrenar significa enseñar a alguien más una determinada habilidad que pueda usar en sus

funciones diarias. Considerando el modelo propuesto por NIST, para llegar a una fase de entrenamiento se debe contar con la etapa base, es decir, concientización

Educación

Este componente integra habilidades y competencias relacionadas a la seguridad asociadas a diversas especialidades funcionales dentro de un cuerpo común de conocimiento, incluyendo conceptos multidisciplinarios. Dicho en otras palabras, la seguridad de la información, si bien está altamente ligada a las computadoras no solo implica que se debe ser experto en temas de seguridad sobre las computadoras, sino también en áreas relacionadas, por ejemplo, psicología.

Estos tres componentes claves propuestos por la NIST 800-50 son abordados en un esquema de ciclo de vida, considerando las etapas de: diseño, desarrollo, implementación y post-implementación, lo cual busca mediante una secuencia ordenada, la implementación de un programa efectivo que aporte a la seguridad de la información.

La siguiente matriz resume los marcos de referencia o estándares analizados y el uso que se les va a dar en este trabajo.

Marco de referencia / Estándar	Uso a dar
COBIT	No se usará este marco de referencia
ITIL	No se usará este marco de referencia
ISO 27002	Se usarán 16 controles de 5 dominios diferentes
NIST 800-50	Se usarán los componentes: concientizar, entrenar y educar en la fase de diseño

Tabla 11: Resumen de los marcos de referencia a adoptar. **Elaborado por:** Autor.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA DE MARCO DE TRABAJO

4.1 Introducción

A continuación, se desarrollará la propuesta de marco de trabajo para la mitigación de riesgos de ingeniería social, para lo cual se diseñará un modelo estructurado que contendrá lineamientos adoptados de los estándares analizados, así como buenas prácticas, políticas de seguridad y controles, los cuales pueden servir de guía que permitan mitigar los riesgos de ingeniería social.

Se tomará como base, el análisis realizado en el apartado 3.2, (Ver bosquejo en la figura 15), en la cual se llegó a determinar los riesgos que existen por cada vector de ataque para cada una de sus características, ya sea: la categoría, los factores psicológicos, el canal, el operador, el nivel de automatización y el objetivo.

	Categoría			Factor psicológico							Canal					Operd	Automatiz.			Objetivo						
Vector de ataque	Técnico	Físico	Social	Solidaridad	Reciprocidad	Confianza	Colectivismo	Reconocimiento	Obscurencia	Urgencia	Consistencia	E-mail	Mensaj. Inst.	Redes sociales	Cloud	Teléfono	Sitios Web	Físico / Otro	Humano	Computador	Alto	Medio	Bajo	Organización	Grupo	Individuo
Phishing																										
Smishing																										
Vishing																										
Spear-Phishing																										
Whaling																										
Info de libre acceso																										
Trashing																										
Shoulder surfing																										
Piggybacking o tailgaiting																										
Sex appeal																										
Baiting																										
Uso de redes WiFi																										
Espionaje de oficina																										

Figura 16 - Visión general del análisis de riesgos de los vectores de ataques de IS. **Fuente:** Autor

4.2 Diseño del Marco de Trabajo para los Riesgos de Ingeniería Social

A partir del análisis realizado en el párrafo anterior, la presente propuesta de marco de referencia busca plantear contramedidas que permitan mitigar los riesgos de ingeniería social identificados (cuadros con tonos rojizos).

Las contramedidas a proponer corresponden a políticas, controles y buenas prácticas que han sido tomadas como referencia a partir de los estándares analizados, es decir, ISO 27002 y NIST-800-50 y adaptadas a los riesgos identificados en este trabajo, además de otros controles identificados como parte de la investigación. Se propone lo siguiente:

Código	Color	Nombre	Marco de referencia / Estándar
CT		Controles técnicos	- Controles de ISO 27002 - Controles identificados en la investigación
CF		Controles físicos	- Controles de ISO 27002 - Controles identificados en la investigación
PS		Política General de Seguridad	- Controles de ISO 27002
PC		Programa de Concientización	- Marco de referencia de NIST 800-50
PE		Programa de Entrenamiento	- Marco de referencia de NIST 800-50

Tabla 12: Bosquejo de los controles y políticas del modelo propuesto. **Elaborado por:** Autor.

Por lo tanto, se infiere que los controles, políticas y programas propuestos ayudarían a mitigar los ataques de ingeniería social, según lo detallado en la tabla 12, adjunta a continuación:

	Categoría				Factor psicológico								Canal				Operd		Automatiz,			Objetivo				
Vector de ataque	Técnico	Físico	Social	Solidaridad	Reciprocidad	Confianza	Colectivismo	Reconocimiento	Obsecuencia	Urgencia	Consistencia	E-mail	Mensaje. Inst.	Redes sociales	Cloud	Teléfono	Sitios Web	Físico / Otro	Humano	Computador	Alto	Medio	Bajo	Organización	Grupo	Individuo
Phishing																										
Smishing																										
Vishing																										
Spear-Phishing																										
Whaling																										
Info de libre acceso																										
Trashing																										
Shoulder surfing																										
Piggybacking o tailgaiting																										
Sex appeal																										
Baiting																										

	Categoría				Factor psicológico								Canal				Operd		Automatiz,			Objetivo				
Vector de ataque	Técnico	Físico	Social	Solidaridad	Reciprocidad	Confianza	Colectivismo	Reconocimiento	Obsecuencia	Urgencia	Consistencia	E-mail	Mensaje. Inst.	Redes sociales	Cloud	Teléfono	Sitios Web	Físico / Otro	Humano	Computador	Alto	Medio	Bajo	Organización	Grupo	Individuo
Uso de redes Wifi																										
Espionaje de oficina																										

Tabla 12: Detalle de los controles y políticas por cada vector de ataque. **Elaborado por:** Autor.

Con el fin de esquematizar los programas, la política y los controles propuestos han sido agrupados en 3 componentes: Personas, Políticas y Controles, la cual se ha representado en un solo modelo consolidado para poder brindar una visión holística del marco de trabajo. La imagen siguiente muestra de manera gráfica el resultado del modelo propuesto, al cual se ha denominado MATIS (**M**arco de **T**rabajo para la **M**itigación de **R**iesgos de **I**ngeniería **S**ocial)

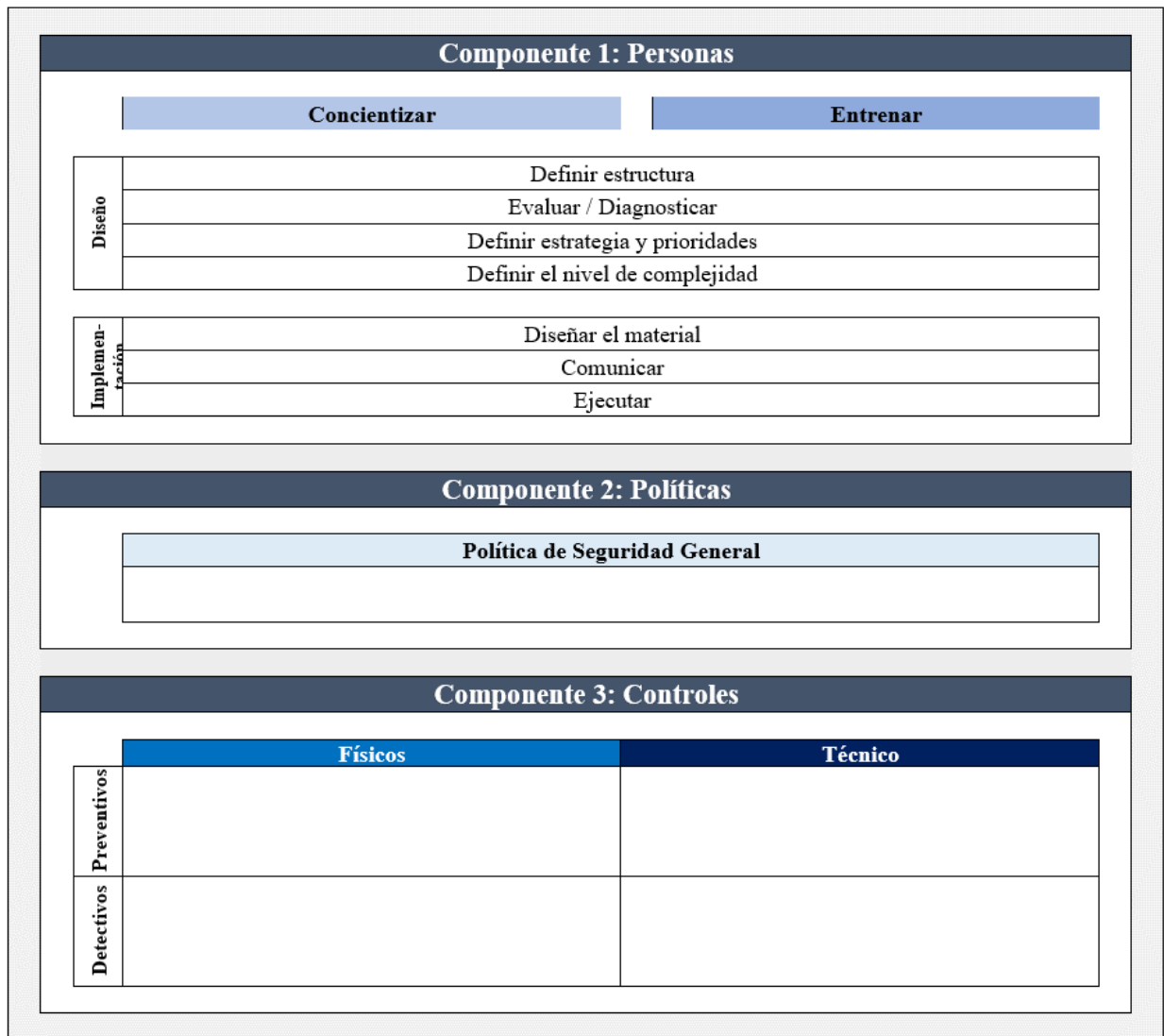


Figura 17 - MATIS – Marco de trabajo de gestión de riesgos de ingeniería social. **Fuente:** Autor.

4.3 Explicación del modelo del marco de referencia.

El modelo del marco de trabajo propuesto está conformado por 3 componentes: el programa de concientización y capacitación, las políticas de seguridad y el set de controles.

El componente **Concientizar y Entrenar** contiene los pasos que deben seguirse para diseñar y llevar a cabo un programa de concientización y entrenamiento dirigido a los empleados de manera estructurada.

El componente **Políticas** es básicamente un compendio de políticas de seguridad mínimas que se recomienda incorporar o confirmar que existan dentro de la política corporativa de seguridad. Esto permitirá complementar el marco de control y las campañas de concientización del *framework*.

Finalmente, el componente **Controles**, propone un set de controles técnicos, controles físicos y controles operativos que, de ser implementados, permitirán reducir los riesgos asociados a la ingeniería social,

4.4 Desarrollo de los componentes de MATIS

4.4.1 Componente 1: Personas

Este macro proceso abarca todos aquellos esfuerzos que se deben enfocar para mitigar los riesgos de ingeniería social que están directamente ligados a las actividades que se deben realizar sobre las personas, o en este caso, los empleados de una compañía. Como se ha analizado previamente, muchos de los riesgos de ingeniería social pueden ser contrarrestados si se aplican contramedidas sobre las personas. Dichas contramedidas se resumen en los procesos de: concientizar y entrenar, los cuales serán abordados a continuación:

Concientizar y Entrenar

Tomando como referencia el estándar NIST 800-50, ambas instancias – concientizar y entrenar – pueden ser abordadas como un solo proceso, ya que, prácticamente las actividades que se realizan en ambas son comunes, donde la diferencia es el enfoque que se les da a cada una de ellas.

De acuerdo al modelo propuesto, el proceso Concientizar y Entrenar está conformado por los subprocesos de diseño e implementación. A continuación, se desglosa cada una de ellas:

Diseño

Acorde al modelo propuesto, el subproceso de diseño considera los siguientes cuatro pasos a seguir para bosquejar un modelo de concientización y entrenamiento, en este caso, acoplado a los riesgos de ingeniería social.



Paso 1. Definir estructura

El estándar NIST 800-50 propone 3 modelos de estructura, de acuerdo a las necesidades de la organización, siendo estos:

- **Modelo 1:** Política, estrategia e implementación centralizada;
- **Modelo 2:** Política y estrategia centralizadas, implementación distribuida; y
- **Modelo 3:** Política centralizada, estrategia e implementación distribuida.

La definición del modelo de estructura básicamente dependerá de:

- El tamaño y dispersión geográfica de la organización (compañía local o multinacional)
- Funciones y responsabilidades organizativas definidas; y
- Asignaciones presupuestarias y autoridad.

La siguiente tabla muestra algunas características que deben ser tomadas en cuenta para la selección del modelo de estructura:

Modelo 1: Centralización total	Modelo 2: Política y estrategia centralizadas, implementación distribuida	Modelo 3: Política centralizada, estrategia e implementación distribuida
Este modelo es recomendable para organizaciones que:	Este modelo es recomendable para organizaciones que:	Este modelo es recomendable para organizaciones que:
<ul style="list-style-type: none"> - Son relativamente pequeñas o tienen un alto grado de estructura y administración central de la mayoría de las funciones de TI - Tienen una Casa Matriz con los recursos necesarios, la experiencia y el conocimiento de la (s) misión (es) y operaciones a nivel de unidad (sucursales); - Tienen un alto grado de similitud en la misión y los objetivos operativos en todos sus componentes. 	<ul style="list-style-type: none"> - Son relativamente grandes o tienen una estructura bastante descentralizada con responsabilidades claras asignadas tanto a la sede central (Matriz) como a los niveles de unidad (sucursales) - Tienen funciones que se extienden sobre un área geográfica amplia (por ej. región); o - Tienen unidades organizativas con diversas misiones, por lo que los programas de concientización y capacitación pueden diferir significativamente, según las necesidades específicas de cada sucursal. 	<ul style="list-style-type: none"> - Son relativamente grandes - Tienen una estructura muy descentralizada con responsabilidades generales asignadas a la Casa Matriz y responsabilidades específicas asignadas a los niveles de unidad (sucursales) - Tienen funciones que se extienden sobre un área geográfica amplia (por ej.: región) - Tienen sucursales semi-autónomas con misiones separadas y distintas, de modo que los programas de concientización y capacitación pueden diferir mucho.

Tabla 14: Modelo de estructuras. **Fuente:** NIST 800-50.

El modelo que se adopte regirá la gestión de los programas de concientización y entrenamientos de manera general para los tópicos de seguridad de la información y no específicamente para la gestión de riesgos de ingeniería social.

Paso 2. Evaluar o diagnosticar

Antes de iniciar cualquier programa de concientización o entrenamiento es imperativo determinar las necesidades reales de la organización con el fin de identificar el *gap* entre el nivel de cobertura existente versus las necesidades de la organización. Es altamente recomendable que personal clave dentro de la organización se involucre en este proceso, tales como: altos ejecutivos, personal de seguridad, propietarios de datos, administradores de sistemas, gerentes de negocio y usuarios claves.

Algunas de las técnicas sugeridas para la evaluación son:

- Entrevistas con personal clave y grupos
- Encuestas dirigidas o personalizadas.
- Revisión de programas y materiales de concientización y entrenamiento existentes relativos a ingeniería social.
- Revisión de datos o indicadores relacionadas a los programas de entrenamiento y concientización existentes, como, por ejemplo: número de asistentes versus números de convocados, calificación promedio de las últimas evaluaciones, etc.), relativos a ataques de ingeniería social.
- Revisión de usuarios con derechos de accesos sobre sistemas de información que podrían estar expuestos a ataques de ingeniería social.
- Revisión de observaciones y recomendaciones realizadas por terceros (auditores, entes reguladores, etc.) ligados a aspectos de ingeniería social.
- Indagaciones con gerentes funcionales, administradores de sistemas y demás personal con una alta dependencia en el uso de TI

- Revisión y análisis de eventos relacionados a seguridad que se hayan suscitados en el último año y que hayan sido llevados a cabo con técnicas de ingeniería social.
- Entendimiento y evaluación de las tendencias de la industria y aplicación de medidas recién adoptadas por otros, incluyendo nuevas técnicas o vectores de ataque de ingeniería social.

El resultado de la realización de la fase de diagnóstico debe aportar con respuestas a las siguientes preguntas:

- a. ¿Cuáles son las necesidades de concientización, entrenamiento o educación requeridas en la organización actualmente relacionadas a ingeniería social?
- b. ¿Qué se está realizando actualmente en la organización en materia de concientización y entrenamiento para alcanzar los objetivos de seguridad propuestos ligados a la ingeniería social?
- c. ¿Cuál es el estado actual de las acciones tomadas para atender las necesidades de la organización relativas a concientización o entrenamientos?
- d. ¿Cuáles son las brechas existentes entre las necesidades y qué se está haciendo al respecto?
- e. ¿Cuáles son las necesidades más críticas o prioritarias en la organización? ¿Se incluyen acciones a tomar sobre ataques de ingeniería social?

Paso 3. Desarrollar un plan y definir prioridades

Una vez concluida la fase de diagnóstico, se está en la capacidad de desarrollar una estrategia para el desarrollo del programa de concientización y entrenamiento, considerando

que el plan se refiere al documento que contiene el detalle de las actividades para llevar a cabo la estrategia.

Los factores listados a continuación pueden ayudar a definir el plan:

- Regulaciones o leyes locales existentes que requieran la realización de programas de concientización y capacitación que requieran adoptar enfoques relacionados a la ingeniería social.
- Alcance del programa de concientización y formación.
- Funciones y responsabilidades del personal de la organización que debe diseñar, desarrollar, implementar y mantener el material de concientización y capacitación, y que debe garantizar que los usuarios apropiados asistan o vean el material aplicable.
- Metas a cumplir para cada aspecto del programa (por ejemplo, concientización, capacitación, educación, desarrollo profesional [certificación]);
- Audiencias objetivo para cada aspecto del programa;
- Cursos o material obligatorio (y, si aplica, opcional) para cada público objetivo;
- Objetivos de aprendizaje para cada aspecto del programa;
- Temas a tratar en cada sesión o curso específicos para los riesgos de ingeniería social.
- Métodos de implementación que se utilizarán para cada aspecto del programa;
- Documentación, retroalimentación y evidencia de aprendizaje para cada aspecto del programa;
- Evaluación y actualización de material para cada aspecto del programa; y
- Frecuencia con la que cada público objetivo debe obtener el material.

Una vez definido el plan, es importante definir las prioridades que regirán las actividades del programa de concientización y entrenamiento, considerando:

- **Disponibilidad de material o recursos:** si se dispone fácilmente de material de concientización y capacitación y los recursos necesarios, las iniciativas clave en el plan se pueden programar con anticipación. Sin embargo, si el material del curso debe desarrollarse y / o los instructores deben identificarse y programarse, estos requisitos deben considerarse al establecer las prioridades.
- **Rol e impacto organizacional:** es muy común abordar la prioridad en términos del rol y de la organización y sus riesgos. Las iniciativas de concientización que se relacionan con los aspectos mandatorios de la organización pueden recibir una alta prioridad ya que las buenas prácticas de seguridad pueden ser apalancadas mediante la fuerza laboral de manera rápida. Además, enfocarse en los altos mandos o puestos de riesgos (por ej. administradores de sistemas y seguridad) puede ser una prioridad.
- **Nivel de cumplimiento actual:** otra forma de definir prioridad, puede ser mediante la identificación de las brechas en el programa de concientización. Para poder enfocarse en áreas con deficiencias.
- **Nuevos proyectos críticos:** si existen proyectos críticos, en los que las actividades de capacitación en seguridad es un hito importante para la implementación de un determinado proyecto, esto puede ser considerado un criterio de priorización

Paso 4. Definir el nivel de complejidad

En esta etapa se debe definir el nivel de complejidad del contenido del curso de concientización y entrenamientos, considerando los siguientes criterios:

- La(s) posición(es) del público objetivo dentro de la organización
- Nivel de conocimiento y habilidades relativas a seguridad requeridas en la posición

Distinguir los niveles de entrenamiento permitirán definir el nivel de complejidad de los entrenamientos. Se puede distinguir los siguientes:

Alto: en este nivel se encuentran las personas que deberían estar esperando ataques de ingeniería social y/o tienen privilegios sobre recursos de TI (por ej. la red local). Un analista de *helpdesk* es un claro ejemplo de esto, ya que parte de sus funciones es ayudar a los usuarios todo el día, al mismo tiempo que posee ciertos privilegios de administración, como, por ejemplo: crear usuarios, resetear contraseñas.

Medio: en este nivel se encuentran las personas que tienen contacto con los usuarios en general y/o pueden tener algún nivel de acceso a la red. Es posible que estas personas no tengan la autorización para realizar cambios en la red, pero ciertamente podrían ejecutar comandos o ir a otra computadora y hacer varias cosas desde allí. Los entrenamientos deben hacer énfasis en la necesidad de tener que confirmar la identidad de una persona antes de proporcionar información o hacer algo por alguien más.

Bajo: este nivel incluye a las personas que tienen poco o ningún acceso a la red o sistemas informáticos. Esto incluye guardias de seguridad y conserjes; sin embargo, las capacitaciones en este nivel deben incluir tácticas de ingeniería social que podrían estar dirigidas a ellos, incluyendo el evitar el ingreso a las instalaciones fuera del horario laboral (cuando sea posible). Las capacitaciones en este nivel pueden omitir ciertas tácticas que pueden no ser aplicables a todos.

Implementación

El subproceso de implementación consta de tres fases, resumida en la siguiente imagen:



Paso 1. Desarrollar material

Este paso es posiblemente la más importante de la fase de implementación, ya que en esta se definirán los tópicos a ser dictados en los programas de concientización. Un punto de partida previo al inicio del desarrollo del material es tomar como base las siguientes preguntas:

- ¿Qué comportamiento se desea reforzar? – Concientización
- ¿Qué habilidades se desea desarrollar sobre los participantes para que sean aplicados?
 - Entrenamiento

Es importante que se desarrolle material adaptado para la audiencia, de modo que los participantes sientan el nivel de personalización adecuado para ellos, evitando generar falta de interés o atención por compromiso.

De igual forma, el material debe ser actual y debe ser interesante para la audiencia; además, los mensajes a comunicar deben ser cortos y simples, ya sea que se aborden temas individuales o múltiples.

Selección de temas de Concientización

A continuación, se muestra un número de temas propuestos por la NIST 800-50, los cuales pueden ser tomados como referencia para la elaboración del material de los cursos o entrenamientos. A estos temas, se les ha incluido un mapeo contra los vectores de ataques de ingeniería social, de modo que se pueda adaptar el material en base a un tipo de ataque en particular (en caso de ser requerido).

Temas propuestos por NIST 800-50	Vectores de ataque												
	Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy. o tailg.	Sex appeal	Pérdida deliberada de	Uso de redes WiFi	Espi. de of.
Uso y administración de contraseñas, incluida las características de su composición y la frecuencia de los cambios.							✓	✓					
Protección contra virus, gusanos, troyanos y otros códigos maliciosos, incluyendo el uso del software (escaneo y análisis de amenazas).	✓	✓		✓	✓						✓	✓	
Política de seguridad, incluyendo las implicaciones del incumplimiento	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Correo electrónicos desconocidos y archivos adjuntos	✓	✓		✓	✓								
Uso de Internet, lo que está permitido vs lo prohibido, incluyendo el monitoreo de la actividad del usuario	✓			✓	✓	✓							
Correo no deseado (Spam)	✓			✓	✓								
Respaldo de información y almacenamiento de datos - enfoque centralizado o descentralizado													
Ingeniería social	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Respuesta a incidentes de seguridad ¿a quién se debe contactar? ¿qué se debe hacer?	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Seguridad en el ingreso de información sensitiva								✓					

Temas propuestos por NIST 800-50	Vectores de ataque												
	Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy. o tailg.	Sex appeal	Pérdida deliberada de	Uso de redes WiFi	Espi. de of.
Cambios en el ambiente de sistemas y cómo esto aumenta los riesgos sobre las aplicaciones y los datos (por ejemplo, agua, fuego, polvo o suciedad, acceso físico)													
Uso personal de tecnología y mecanismos de trabajo desde casa													
Los riesgos de seguridad de dispositivos móviles, tanto físicos como inalámbricos		✓	✓									✓	
Cifrado y transmisión de información confidencial, incluyendo el uso de Internet: política de la agencia de direcciones, procedimientos y contacto técnico para asistencia	✓	✓	✓	✓	✓								
Seguridad de los equipos portátiles en viajes								✓				✓	
Uso de software de propiedad personal en el trabajo													
Aplicación oportuna de parches de seguridad													
Software admitido / permitido en sistemas de organización	✓												
Problemas de control de acceso, principio del menor privilegio y la separación de funciones													
Responsabilidad individual (Accountability)													
Declaraciones de confirmación: contraseñas, acceso a sistemas y datos, información de uso personal													
Control de visitantes y acceso físico a áreas restringidas: discusión sobre la política de seguridad física aplicable y los procedimientos.							✓	✓	✓	✓	✓		✓
Seguridad en el escritorio: discusión sobre el uso de protectores de pantalla y la restricción de los visitantes a ver la pantalla								✓	✓				✓

Temas propuestos por NIST 800-50	Vectores de ataque												
	Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy. o tailg.	Sex appeal	Pérdida deliberada de	Uso de redes WiFi	Espi. de of.
Protección de la información confidencial, ya sea en sistemas, documentos físicos, en dispositivos de respaldos, etc., durante todo su ciclo de vida, hasta su destrucción.							✓		✓				✓
Uso apropiado de correo electrónico - archivos adjuntos y otras reglas.	✓			✓	✓								

Tabla 15: Mapeo de temas de entrenamiento vs vectores de ataque de IS. **Fuente:** NIST 800-50 **Mapeo elaborado por:** Autor.

Según el modelo propuesto por NIST, la concientización está enfocada a todos los usuarios de TI de una organización, ya que esto forma la línea base que se requiere para todos los empleados de una organización, indistinto de su cargo o función; sin embargo, cuando se habla de entrenamiento y educación, esto se debe realizar de manera personalizada y selectiva basado en las responsabilidades y necesidades del empleado. De manera más específica, el entrenamiento debe estar enfocado de acuerdo a las funciones o cargo del empleado; mientras que la educación está orientada a especialistas de seguridad de la información más allá del entrenamiento basado en sus funciones. En la matriz siguiente se resumen las categorías funciones que pueden ser consideradas para personalizar los entrenamientos:

Función	Descripción
Gerente o Administrador	Esta categoría se refiere a las personas encargadas de administrar las funciones de TI en una organización. Por ej. Director de TI
Comprador	Esta categoría se refiere a aquellas personas que participan en la adquisición de productos y / o servicios de TI (por ejemplo, forman parte de una junta para evaluar las propuestas de los proveedores de sistemas de TI). Esto es especialmente importante para aquellos que se desempeñan como representantes técnicos de los contratistas
Diseño y desarrollo de sistemas	Esta categoría abarca a aquellas personas que diseñan y desarrollan sistemas y aplicaciones.
Operadores	Esta categoría se refiere a aquellas personas que operan (administran) sistemas de TI (por ejemplo, servidores web, servidores de correo electrónico, servidores de archivos, LAN, WAN).
Revisores o auditores	esta categoría abarca a las personas que revisan y evalúan (auditan) las funciones de TI como parte del programa de controles internos de una organización, revisión interna o un programa de auditoría externa (por ejemplo, auditores externos).
Usuarios	esta categoría abarca a las personas que acceden a los recursos de TI y / o usan la TI para hacer su trabajo diario.

Tabla 16: Análisis de funciones claves para los entrenamientos **Elaborado por:** Autor.

Asimismo, los temas a desarrollar en los entrenamientos pueden ser personalizados dependiendo de las funciones o cargos de los asistentes, a continuación, se mencionan algunos tópicos que deberían considerarse de acuerdo a los cargos:

Función o cargo	Descripción	Vectores de ataque											
		Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy . o tailg.	Sex appeal	Baiting	Uso de redes WiFi
Helpdesk	<p>Los analistas de mesa de servicio deben ser entrenados para frustrar los intentos de ingeniería social con especial énfasis, ya que usualmente son personas muy ocupadas que reciben peticiones de soporte o servicios por diferentes canales (llamadas, correo, en persona) y, en cualquier momento.</p> <p>Un ingeniero social puede intentar convencerlos de que son usuarios legítimos y que necesitan algún tipo de asistencia, y dado que el objetivo principal de un servicio de asistencia es ayudar, eso es lo que exactamente buscará un atacante. Las funciones de mesa de ayuda deben estar capacitadas para ser amigable y, al mismo tiempo, utilizar el buen juicio y el escepticismo profesional antes de realizar alguna actividad como creación de cuentas de usuarios o reseteo de contraseñas, debe preguntarse y validar si el usuario es quien dice ser y si requiere o está autorizado para recibir lo que está solicitando.</p>	✓											
Administrador de TI	Si bien los administradores de TI pueden no recibir tantas llamadas telefónicas como los analistas de <i>Help Desk</i> , puede ser un objetivo porque posee altos privilegios sobre diversos componentes de tecnología (por ej. sistemas, bases de datos, redes, etc.), por lo que un ingeniero social puede apuntar a estas personas para ganar tiempo en tener que escalar privilegios.	✓				✓							✓

Función o cargo	Descripción	Vectores de ataque											
		Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulde surf.	Piggy. o tailg.	Sex appeal	Baiting	Uso de redes WiFi
	Los administradores de TI generalmente son más conscientes de los riesgos de tecnología a los que pueden estar expuestos, sin embargo, muchas veces su enfoque puede llegar a ser muy técnico (conocimiento de controles sobre plataformas tecnológicas, firewalls, DNS, etc.) y podrían no ser conscientes de otras técnicas de ingeniería social, sobre todo aquellas que se enfocan mayoritariamente en explotar algún comportamiento psicológico (tal y como se lo menciono anteriormente en el estudio del caso de Robin Sage, mediante el uso de sex appeal).												
Recepcionista	Las responsabilidades de una recepcionista pueden llegar a significar diferentes cosas en diferentes organizaciones (desde únicamente contestar llamadas hasta ser la mano derecha de altos ejecutivos), por lo cual se debe hacer especial énfasis al momento de armar un plan de concientización y capacitación dependiendo de las funciones reales que cumpla. Por ejemplo, si una recepcionista es responsable de contestar llamadas, se debe incluir dentro del programa de capacitación, ejemplos explícitos del uso de la persuasión que suelen llevar a cabo los ingenieros sociales mediante técnicas como el <i>vishing</i> .	✓		✓	✓								✓

Función o cargo	Descripción	Vectores de ataque											
		Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy. o tailg.	Sex appeal	Baiting	Uso de redes WiFi
	Por otro lado, si además de ser recepcionistas son secretarias de altos ejecutivos, se las debe instruir sobre la sensibilidad de la información al que ellas tienen acceso, marcando diferencias sobre qué se considera confidencial o no (por ejemplo, los nombres de un socio podría no ser confidencial, a diferencia de su dirección domiciliaria) y cómo un atacante podría persuadirla para que entregue información confidencial												
Teletrabajador	Los teletrabajadores presentan un riesgo especial, ya que pueden representar una brecha de seguridad al ser conexiones externas hacia las redes corporativas, permitiendo a un atacante comprometer primero su red local para luego escalar a la red de la organización, pudiendo presentarse conexiones indeseadas que pueden permanecer abiertas sin ser detectadas oportunamente.	✓			✓				✓				
Funciones de RRHH	El departamento de Recursos Humanos por su naturaleza, tiene acceso a información personal de todos los empleados de la organización, la cual es usualmente un activo altamente buscado por los atacantes, más allá de todas las implicaciones relativas a las regulaciones de protección de datos personales.	✓		✓	✓								

Función o cargo	Descripción	Vectores de ataque											
		Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy. o tailg.	Sex appeal	Baiting	Uso de redes WiFi
	<p>Esto es suficiente motivo para considerar a las personas que trabajan en este departamento para elaborar planes de concientización y entrenamiento personalizados que generen conciencia y acciones que eviten cualquier ataque dirigido. Además, al ser la función dentro de la organización responsable de las personas como tal, puede ser una buena idea apalancar en ellos la implementación de planes o campañas de concientización sobre todos los empleados de la compañía</p> <p>Asimismo, este departamento usualmente está en contacto con diversas áreas en la organización y a menudo solicita o entrega información de diferentes índoles, es por esto, que también se debe hacer énfasis en que previo a la entrega de cualquier información confidencial, ellos deben verificar la identidad del solicitante.</p>												
Departamento de Investigación y desarrollo	<p>Si bien un departamento de Investigación y Desarrollo no tendrá como actividad primera el responder llamadas telefónicas o responder correos electrónicos, puede llegar a ser un objetivo primario de ingenieros sociales, ya que estas personas tienen acceso a información sensible (como, por ejemplo: información de nuevos proyectos de la organización), lo cual es considerado información confidencial y estratégica.</p> <p>Es por esto, que, las organizaciones que tengan este departamento, deberán incluir dentro de sus programas de entrenamiento y concientización, actividades específicas para sus miembros.</p>	✓			✓								✓

Función o cargo	Descripción	Vectores de ataque												
		Phishing	Smishing	Vishing	Spear-Phishing	Whaling	Inf. Libre acc.	Trashing	Shoulder surf.	Piggy. o tailg.	Sex appeal	Baiting	Uso de redes WiFi	Espi. de of.
Altos ejecutivos (Niveles C)	<p>Los altos ejecutivos de una organización (por ej. CEOs o accionistas) generalmente tienen información altamente confidencial, por lo que sobre ellos se deben armar programas de concientización y entrenamientos altamente personalizados.</p> <p>Llegar a ellos puede ser un reto, mucho más poder concientizar sobre los riesgos a los que están expuestos, ya que por su índole de alto mando, no están acostumbrados a recibir instrucciones y podrían minimizar la situaciones</p> <p>Además, es muy frecuente que este tipo de usuarios soliciten excepciones a las reglas de seguridad de la compañía, pudiendo en algunas ocasiones, tener perfiles privilegiados de acceso a Internet, o excepciones sobre políticas de contraseñas (contraseñas menos fuertes) e inclusive privilegios de acceso remoto.</p>					✓								

Tabla 17: Consideraciones a tener en los entrenamientos de algunas funciones claves en la organización **Elaborado por:** Autor.

Paso 2. Comunicar e Implementar

Esta etapa tiene como objetivo dar a conocer el plan de entrenamiento a la organización con el fin de obtener el apoyo y compromiso de los recursos necesarios. Parte de la explicación comprende un extracto de las expectativas de las gerencias del negocio y un acercamiento del apoyo del personal de la compañía, haciendo énfasis en los beneficios que el programa traerá consigo. Además, se debe explicar cómo se fondearán los programas de concientización y entrenamiento, aclarando que los costos correrán por cuenta del área de seguridad de la información. Asimismo, esta etapa debe servir para dejar en claro los roles y responsabilidades de las partes involucradas.

Las actividades de comunicación dependerán del tipo de estructura definida en el paso uno de la etapa del diseño, tal y como se muestra en la tabla 18:

Modelo 1: Centralización total	Modelo 2: Política y estrategia centralizadas, implementación distribuida	Modelo 3: Política centralizada, estrategia e implementación distribuida
En este modelo, el Oficial de Seguridad está a cargo del desarrollo e implementación de todo el programa para todas las subsidiarias o sucursales. En este caso, el CIO o el Oficial de Seguridad deben ponerse en contacto con los administradores de las sucursales de la compañía para que con su ayuda se lleve a cabo las tareas de comunicación y coordinación de los aspectos logísticos del entrenamiento (coordinar con los asistentes, distribuir el material, etc.)	En este modelo el Oficial de Seguridad desarrolla todo el programa y las evaluaciones. El presupuesto es responsabilidad de cada sucursal, así como también la ejecución del programa en su unidad de negocio. Al mismo tiempo que tienen como responsabilidad el emitir reportes al Oficial de Seguridad Corporativo.	En este modelo el Oficial de seguridad determina la política y expectativas con respecto al programa de entrenamiento y concientización. La ejecución del programa es responsabilidad de cada sucursal, desde el diagnóstico, definición del plan y determinación de la estrategia; así como también el desarrollo del material, coordinación de aspectos logísticos y ejecución del programa. De igual manera, las sucursales deben

Modelo 1: Centralización total	Modelo 2: Política y estrategia centralizadas, implementación distribuida	Modelo 3: Política centralizada, estrategia e implementación distribuida
		emitir reportes al Oficial de Seguridad Corporativo.

Tabla 18: Responsabilidades de comunicación de acuerdo a la estructura definida de aplicabilidad de los dominios ITIL. **Fuente:** NIST 800-50 **Maapeo elaborado por:** Autor.

Existen diversos mecanismos de compartir los mensajes que se desean transmitir con los programas, los mismos dependen de los temas seleccionados y de los recursos disponibles. A continuación, se listan algunas técnicas que pueden ser usadas:

- Mensajes de concienciación en artículos variados de uso diario (por ejemplo, pendrives, esferos, llaveros, post-it, libretas, kits de primeros auxilios, kits de limpieza, CDs, marcadores, pelotas anti-stress, etc.)
- Posters vistosos ubicados en zonas estratégicas de las instalaciones con mensajes de las cosas que se pueden hacer y las cosas que no.
- Mensajes en *wallpapers* de los equipos de oficina.
- Mensajes en boletines internos
- Mensajes personalizados enviados por correo electrónico
- Mensajes multimedia (videos, animaciones)
- Sesiones por vía conferencia
- *Workshops* - sesiones dirigidas por un instructor.
- Implementación del “Día de la seguridad de la información” o eventos similares.
- Crucigramas, sopas de letras, etc.
- Concursos con recompensas

Los entrenamientos pueden ser ejecutados de varias formas, se enumeran algunas de estas:

Técnica	Descripción
Videos o aplicaciones interactivas	Esta es una de técnica de aprendizaje a distancia disponibles para entregar material de capacitación. Esta tecnología es compatible con instrucciones interactivas de audio y video de dos vías. La característica interactiva hace que la técnica sea más efectiva; sin embargo, suele ser costosa.
Capacitaciones basadas en aplicaciones Web	Esta técnica es una de las más usadas cuando se tiene sucursales o agencias distribuidas. Los participantes de estas sesiones pueden aprender de forma independiente y de acuerdo a su disponibilidad. En este tipo de capacitaciones, se puede incorporar test o evaluaciones calificadas que son recolectadas y analizadas de manera centralizada.
Entrenamientos presenciales	Probablemente esta es la técnica más antigua y conocida, en la cual, existe un instructor conocedor del tema quien se encarga de impartir el material y resolver las inquietudes que puedan surgir de la audiencia, en otras palabras, es la técnica más interactiva que existe; sin embargo, esta técnica podría no ser aplicable en grandes organizaciones donde coordinar las sesiones puede ser una tarea complicada o consumidora de recursos.

Tabla 19: Tipos de entrenamientos sugeridos por NIST 800-50. **Elaborado por:** Autor.

4.4.2 Componente 2: Política de Seguridad General

Política General de Seguridad

El objetivo de esta sección del marco de trabajo es aportar con un set de políticas de seguridad de aplicabilidad general, que pueden ser incorporadas dentro de la política de seguridad principal de la organización. Estas políticas incluidas como Anexo A, permitirían contar con lineamientos que deben ser seguidos por los empleados de una organización y que debe ayudar a minimizar la exposición al riesgo del factor humano.

4.4.3 Componente 3: Controles

La matriz que se incluye a continuación contiene los controles diseñados para la mitigación de riesgos de ingeniería social. Se ha tomado como referencia los controles de la ISO 27002 definidos en la Tabla 20, y se ha complementado con buenas prácticas y recomendaciones de seguridad en base al análisis realizado en el capítulo 2

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. o tailgating	Sex appeal	Baiting	Open Wifi	Espi. de of.
C-001	Investigación de antecedentes previo a la contratación	Se llevan a cabo actividades de verificación de la autenticidad de los datos curriculares, tales como: datos de identificación, información académica, información judicial, estatus crediticio, etc. El grado de verificaciones que se lleva a cabo depende del nivel de acceso a información que tendrá el candidato	Operativo	Preventivo	ISO 27002 7.1								✓	✓	✓	✓		✓
C-002	Investigación de antecedentes previo a la contratación - funciones sensitivas	Existen procedimientos enfocados a asegurar que el candidato cumple con las competencias técnicas para desempeñar el cargo y que certifica confiabilidad, especialmente para funciones relativas a la administración de seguridad	Operativo	Preventivo	ISO 27002								✓	✓	✓	✓		✓
C-003	Términos y condiciones en la contratación	Existen procedimientos que aseguran la inclusión de roles y responsabilidades relativas a seguridad, así como también la adhesión a las políticas de seguridad para los nuevos empleados, incluyendo la firma de un acuerdo de confidencialidad y no divulgación de información previo al inicio de cualquier actividad que implique el uso de información. Todo incumplimiento es penalizado o sancionado de acuerdo a la política de la organización	Operativo	Preventivo	ISO 27002	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. 0 authentication	Sex appeal	Baiting	Open Wifi	Espi. de of.
C-004	Concienciación, educación y capacitación en seguridad de la información	Se ha definido e implementado programas de concientización sobre los roles y responsabilidades de los colaboradores en cuanto a la seguridad de la información. Asimismo, se diseñan y ejecutan programas de entrenamiento y educación sobre seguridad de la información de acuerdo al nivel de responsabilidad de uso de información de los empleados.	Operativo	Preventivo	ISO 27002	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C-005	Después de la contratación	Se ha implementado procedimientos sobre la salida del empleado que aseguren la comunicación oportuna a las áreas relevantes en la compañía, así como también procedimientos de entrega del cargo, tales como: entrega de información en poder del empleado, retiro de accesos críticos y revisión de últimas transacciones realizadas	Operativo	Preventivo	ISO 27002									✓				✓

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-baiting	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. banking	Sex appeal	Baiting	Open Wifi	Espi. de of.
C-006	Manejo de los soportes de almacenamiento.	Existen procedimientos enfocados a asegurar el manejo adecuado de dispositivos de almacenamiento externos de acuerdo al esquema de clasificación de la información, considerando lo siguiente: i) De acuerdo al nivel de información que almacene el dispositivo, se ha implementado mecanismos de encriptación, principalmente para dispositivos extraíbles (pendrives) ii) Los dispositivos que almacenen información confidencial que sean dados de baja, son destruidos físicamente (por ej. incinerados). iii) Aquellos dispositivos que son trasladados entre sitios, son trasladados por <i>courries</i> autorizados y de confiabilidad probada, al mismo tiempo que se usan mecanismos de protección del dispositivo que impiden el acceso físico al mismo.	Operativo Físico Técnico	Preventivo	ISO 27002								✓			✓		
C-007	Gestión de información confidencial de autenticación de usuarios.	Se solicita la firma de una declaración de no divulgación de información de autenticación a todos los usuarios con acceso a información. Asimismo, existen mecanismos que permiten la identificación de un usuario previo a la provisión o	Operativo	Preventivo	ISO 27002	✓	✓	✓	✓	✓								

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. o tailgating	Sex appeal	Baiting	Open Wifi	Espi. de of.
		modificación de credenciales de acceso a un empleado.																
C-008	Uso de información confidencial para la autenticación	Existen procedimientos implementados que aseguran el uso contraseñas con características seguras (longitud, uso de caracteres especiales, cambio al primer ingreso, etc.) Además, las contraseñas son almacenadas de forma segura (encriptadas) y no son visibles para los administradores	Técnico	Preventivo	ISO 27002	✓	✓	✓	✓	✓								

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. o tailgating	Sex appeal	Baiting	Open Wifi	Espi. de of.	
C-009	Acceso a áreas restringidas	<p>Se han definido perímetros de seguridad de acuerdo al nivel de criticidad de los activos y su calificación de riesgo, considerando:</p> <p>i) Las áreas seguras son aseguradas mediante componentes físicos (paredes de concreto, puertas y techos sólidos, ventanas cerradas, etc.).</p> <p>ii) Los perímetros de seguridad cuentan con un área de recepción, la cual impide accesos no autorizados a las instalaciones.</p> <p>iii) Existen mecanismos de identificación de intrusos, el cual cubre todos los accesos existentes en el perímetro de seguridad (puertas, ventanas), incluyendo alertas o alarmas que se activan ante ingresos no autorizados.</p> <p>iv) Se registra y custodia apropiadamente la información de los ingresos a las áreas protegidas (fecha, hora, nombres)</p> <p>iv) El ingreso de visitantes a áreas seguras se realiza únicamente con la supervisión de una persona apropiada y autorizada.</p> <p>v) Se han implementado mecanismos de doble autenticación a las áreas que almacenan información confidencial</p>	Físico	Preventivo	ISO 27002								✓		✓				

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. bank	Sex appeal	Baiting	Open Wifi	Espi. de of.
-------------	----------------	-------------------------	--------------	-------------------	-----	----------	----------	---------	----------------	---------	------------	----------	------------------	-------------	------------	---------	-----------	--------------

vi) Existen mecanismos que permiten reportar oportunamente la identificación de personal no autorizado o no identificado.

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. o tailgating	Sex appeal	Baiting	Open Wifi	Espi. de of.
C-010	Seguridad de oficinas, despachos y recursos	Existen mecanismos de control apropiados sobre las oficinas, cuartos y demás instalaciones de la organización que contienen información sensitiva, considerando: i) Se restringe el acceso público no autorizado ii) No se incluyen etiquetas que identifiquen las diferentes áreas de la organización (por ej. datacenters, cuarto de archivos, etc. iii) Información de directorios o extensiones telefónicas no son visibles ni accesibles para personal no autorizado.	Físico	Preventivo	ISO 27002							✓	✓	✓		✓		✓
C-011	Áreas de acceso público, carga y descarga.	Existen procedimientos que restringen el acceso no autorizado a las áreas de carga y descarga y demás puntos relevantes, considerando al menos lo siguiente: i) Existen áreas separadas para la carga/ descarga de aquellas áreas que almacenan o procesan información. ii) El acceso a las áreas sensitivas es restringido a personal no autorizado y únicamente se debe permitir acceso a personal identificado.	Físico	Preventivo	ISO 27002							✓	✓	✓		✓		✓

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. o tailgating	Sex appeal	Baiting	Open Wifi	Espi. de of.
C-012	Salida de activos fuera de las dependencias de la empresa.	Existen procedimientos que restringen la salida de equipos de cómputo, software o información sin las autorizaciones respectivas, o al mismo tiempo, las personas autorizadas para permitir la salida de equipos están claramente identificadas. Los equipos de cómputo que requieren salir de las instalaciones de la organización (por ej. por mantenimiento) cuentan con autorización y su salida e ingreso son registrados en una bitácora	Operativo	Preventivo	ISO 27002				✓			✓		✓				
C-013	Reutilización o retirada segura de dispositivos de almacenamiento.	Todos los equipos de cómputo o demás dispositivos que contienen medios de almacenamiento son revisados para asegurar que la información sensitiva ha sido eliminada o sobrescrita de manera correcta previo al reúso o desecho. Para el caso de equipos que contienen dispositivos de almacenamiento que requieren mecanismos de destrucción más sofisticados, estos han sido identificados y llevados a cabo apropiadamente	Operativo	Detectivo	ISO 27002							✓						

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. o tailgating	Sex appeal	Baiting	Open Wifi	Espi. de of.
C-014	Equipo informático de usuario desatendido.	<p>Se han implementado procedimientos para garantizar que todos los usuarios de sistemas informáticos conocen y están conscientes de los requerimientos de seguridad en las estaciones de trabajo, de modo que se protegen los equipos desatendidos, considerando lo siguiente:</p> <ul style="list-style-type: none"> i) Las sesiones de usuarios se cierran al finalizar las actividades, ii) Los usuarios bloquean sus equipos por contraseña iii) Los usuarios cierran las aplicaciones o conexiones de red cuando no se están usando. iv) Los equipos móviles, como tabletas o smartphones también están protegidos con bloqueo de pantalla y contraseña. 	Operativo	Preventivo	ISO 27002								✓	✓				✓
C-015	Política de puesto de trabajo despejado y bloqueo de pantalla.	<p>La organización ha adoptado políticas de escritorio limpio, tanto para documentos físicos como para dispositivos de almacenamiento y pantallas de computadoras considerando la política de clasificación de la información, se tiene en cuenta:</p> <ul style="list-style-type: none"> i) Documentos físicos con información sensible son almacenados en gabinetes u otro 	Físico	Preventivo	ISO 27002							✓	✓	✓				✓

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-fishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. bank	Sex appeal	Baiting	Open Wifi	Espi. de of.
		<p>tipo de muebles que poseen sistemas de bloqueo (por ej. llaves)</p> <p>ii) Los equipos de cómputo y demás dispositivos son bloqueados con contraseña cuando no están en uso.</p> <p>iii) El uso no autorizado de fotocopadoras se restringe mediante el uso de contraseñas.</p>																
C-016	Seguridad de la información en las relaciones con suministradores	<p>Se han definido e implementado controles de seguridad sobre las actividades que están bajo la responsabilidad de proveedores, incluyendo:</p> <p>i) Identificación de proveedores y el tipo de servicio que provee.</p> <p>ii) Se ha definido el tipo de acceso que los proveedores deben poseer, el mismo que es controlado y monitoreado.</p> <p>iii) Se han definido acuerdos de requerimientos de seguridad mínimos que los proveedores deben cumplir.</p> <p>iv) Se han definido políticas del uso aceptable y no aceptable sobre la información de la organización a cargo del proveedor</p> <p>v) Se llevan a cabo programas de concientización y entrenamientos sobre las políticas de seguridad de la organización.</p>	Operativo	Preventivo	ISO 27002				✓			✓	✓	✓		✓		✓

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. bank	Sex appeal	Baiting	Open Wifi	Espi. de of.
		vi) Se ha definido un acuerdo de adhesión a las políticas, el cual es firmado por los proveedores que poseen relación con la organización																
C-017	Dstrucción de información	Se han implementado técnicas adecuadas de destrucción de la documentación, (por ej. destructoras de papel, depósitos de papel que garantizan que no se puede acceder a ellos y, posteriormente, se destruirá su contenido por empresas especializadas).	Físico	Preventivo							✓	✓	✓	✓				✓
C-018	Acceso físico a instalaciones	Se han implementado mecanismos de control físico de acceso a las instalaciones, tales como: i) Tornos giratorios, los cuales únicamente habilitan el acceso autenticado (por ej. mediante el uso de tarjetas de aproximación) ii) Puertas dobles o Mantrap, las cuales actúan de tal forma que la segunda puerta se abre únicamente cuando la primera puerta se ha cerrado y no se detecta más que una persona en el habitáculo intermedio iii) Guardias de seguridad, consiste en personal especializado que mediante observación impiden acceso a personal no autorizado	Físico	Preventivo										✓				

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. 0	Sex appeal	Baiting	Open Wifi	Espi. de of.
		iv) Existen mecanismos de control biométrico para el acceso a zonas restringidas, pudiendo estos ser: huella dactilar, escáner de iris, geometría de la palma de la mano, reconocimiento facial																
C-019	Antivirus	Se han implementado soluciones antivirus en los equipos de cómputo de la organización	Técnico	Preventivo		✓			✓	✓								
C-020	Proxys falsos	Se ha implementado mecanismos de servicio de detección de proxys transparentes	Técnico	Preventivo		✓			✓	✓								
C-021	Prevención de DNS Poisoning	Se ha definido apropiadamente la configuración y parchado de servidor DNS.	Técnico	Preventivo		✓												
C-022	Browser Proxy Configuration	Se mantienen como “prohibido” la configuración de proxy de los navegadores del dominio de la organización. Cualquier modificación a este parámetro es identificado y resuelto oportunamente.	Técnico	Preventivo		✓			✓	✓								
C-023	URL Obfuscation	Se han implementado herramientas de ofuscamiento de direcciones URL, mediante la definición de no confianza de URL provistos por defecto	Técnico	Preventivo		✓			✓	✓								
	URLS cortos	Se han implementado herramientas que permiten pre visualizar el URL	Técnico	Preventivo	Otro	✓			✓	✓								

Ref Control	Nombre Control	Descripción del control	Tipo (O/F/T)	Oportunidad (P/D)	Ref	Phishing	Smishing	Vishing	Spear-phishing	Whaling	Inf. Libre	Trashing	Shoulder surfing	Piggy. bank	Sex appeal	Baiting	Open Wifi	Espi. de of.
		completo en navegadores y operan apropiadamente																
C-024	Host Name Obfuscation	The defense against host name obfuscation is to set a policy to not use obfuscated host names. This is similar to never using bad domain names. A user should always type in the common FQDN.																
C-025	Controles de prevención de scripting cross-Site	Se han implementado y ejecutado análisis de código fuente de sitios web publicados, los cuales podrían prevenir ataques XSS. O a su vez, se realizan monitoreos periódicos de identificación de ataques de inyección de XSS	Técnico	Detectivo	Otro	✓			✓	✓								

Tabla 20: Matriz de controles propuestos por MATIS. **Elaborado por:** Autor.

CAPÍTULO V

CONCLUSIONES Y TRABAJOS FUTUROS

CONCLUSIONES

Al término del presente trabajo, se puede concluir lo siguiente:

- Llevar a cabo un estudio de los factores de la psicología humana, representados en conductas y comportamientos fue de gran ayuda, ya que permitió identificar de manera específica las vulnerabilidades de las personas que son explotadas por los ciberdelincuentes en los ataques de ingeniería social.
- Se realizó un estudio de los vectores de ataques, mediante la lectura de eventos reales que sirvieron para determinar los diferentes componentes de un ataque de ingeniería social, que, a más de tener un componente social, tiene componentes físicos o técnicos y pueden ser llevados a cabo mediante canales diversos. Este análisis sirvió como referencia para determinar los controles y políticas a diseñar en el marco de trabajo propuesto.
- Se analizó los marcos de referencia actuales COBIT, ITIL; sin embargo, en los estándares ISO 27002 y NIST 800-50 se encontró información referencial que permitió definir el modelo de gestión de riesgos de ingeniería social, identificando controles, políticas y programas que permitieron cubrir los riesgos identificados por cada vector de ataque
- Con los insumos de los puntos anteriores, se desarrolló MATIS, el marco de trabajo para la gestión de riesgos de ingeniería social. MATIS es un modelo propuesto que contiene tres componentes que considera los programas de concientización y capacitación, las políticas

y los controles de seguridad, los cuales ayudarían a mitigar esquematizadamente los riesgos de ingeniería social en cualquier organización que lo requiera.

RECOMENDACIONES

Además, se proponen las siguientes recomendaciones:

- Como trabajos futuros, se recomienda que el modelo diseñado en este trabajo, pueda ser adoptado y aplicado por cualquier profesional de la rama de Seguridad de la Información en un ambiente real (organización), o a su vez, pueda ser adoptado por algún tesista que disponga de los recursos y apertura para poder probarlo. El objetivo final sería validar la aplicabilidad de MATIS y medir la eficacia en un ambiente de riesgo real.
- Dada la velocidad con la que la tecnología evoluciona, es recomendable estar atento de las nuevas técnicas o vectores de ataque de ingeniería social, de modo que se consideren los factores de riesgos emergentes y actuales, dependiendo del momento en el que se desee aplicar el *framework*.

BIBLIOGRAFÍA

- ACISSI. (2015). Seguridad Informática Hacking Ético. In ACISSI, *Seguridad Informática Hacking Ético*. Barcelona: Ediciones ENI.
- Alfafara, J. F. (2009). *Resources Global Professionals*. Retrieved from <https://www.resourcenter.net/images/AHIA/Files/2009/AnnMtg/Handouts/C3.pdf>
- Areitio, J. (2008). Seguridad de la Información . In J. Areitio, *Seguridad de la Información* . Madrid.
- BBC. (2017). Retrieved from <https://www.bbc.com/mundo/vert-tra-38803395>
- Bisson, D. (2015). *Tripwire*. Retrieved from Tripwire: <https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>
- Bortnik, S. (2010). *ESE*. Retrieved from WeLiveSecurity: <https://www.welivesecurity.com/la-es/2010/09/01/falsa-alerta-de-terremoto-en-ecuador-propaga-malware/>
- Charkiewicz, G. (2014). *ESE*. Retrieved from WeLiveSecurity: <https://www.welivesecurity.com/la-es/2014/04/14/se-acerca-mundial-brasil-2014-nuevos-casos-fraude/>
- Cluley, G. (2016). Retrieved from <https://www.welivesecurity.com/la-es/2016/11/11/engano-por-sms-apple-id/>
- Corchado, B. (2017). *GoDaddy*. Retrieved from <https://es.godaddy.com/blog/que-es-el-phishing-y-que-tipos-existen/>
- Digital Guardian. (2015). *Digital Guardian*. Retrieved from Digital Guardian: <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack>
- Domenech, R. S. (2009). *LinkedIn*. Retrieved from <https://es.slideshare.net/rsoriano/cobit-itol-iso-27000-marcos-de-gobierno>
- Edmond Marc, D. P. (1992). La interacción social: cultura, instituciones y comunicación. In D. P. Edmond Marc, *La interacción social: cultura, instituciones y comunicación*.
- Experian. (2015). *Experian Information Solutions*. Retrieved from <https://www.edq.com/blog/hook-line-and-sinker/>

- Falero, L. (2015). *Top Position* . Retrieved from <https://t-position.com/3-tipos-de-phishing-mas-utilizados-por-ciberdelincuentes/>
- Hadnagy, C. (2011). Ingeniería social. El arte del hacking personal. In C. Hadnagy, *Ingeniería social. El arte del hacking personal*. Anaya Multimedia.
- Hansen, D. (2017). *Social Vulnerability & Assessment Framework*. Copenhagen: Royal Danish Defence College.
- Inspiration. (n.d.). *Inspiration: Por un mundo libre de pobreza*. Retrieved from <https://www.inspiration.org/justicia-economica/definicion-de-solidaridad>
- Journalistika 2.0. (2011). *ournalistika 2.0*. Retrieved from <http://journalistika.blogspot.com/2011/05/casos-de-phishing.html>
- Krebs on Security. (2014). *Krebs on Security*. Retrieved from <https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/#more-24313>
- Krombholz, K., Heidelinde , H., & Hube, M. (2016). *Advanced Social Engineering Attacks*. Viena.
- La Vanguardia. (2016). Retrieved from <https://www.lavanguardia.com/vida/20160202/301844337516/gorila-protege-nino-zoo.html>
- López Grande, C., & Guadrón, R. (2015). *Ingeniería Social: El Ataque Silencioso*.
- Mitnick, K. (2003). The Art of Deception. In W. L. Kevin D. Mitnick, *The Art of Deception*.
- Mitnick, K. D. (2003). The Art of Deception - Controlling the Human Element of Security. In K. D. Mitnick, *The Art of Deception - Controlling the Human Element of Security*. Indiana: Wiley Publishing.
- Motherboard. (2016). *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/qkjbwd/doj-hacker-also-accessed-forensic-reports-and-state-department-emails
- NoticiasSeguridadInformatica. (2016). *NoticiasSeguridadInformatica*. Retrieved from <http://noticiasseguridad.com/importantes/diversas-metodologias-y-tipos-de-ataques-de-ingenieria-social/>
- Panda Security. (2017). Retrieved from <https://www.pandasecurity.com/spain/mediacenter/seguridad/top-10-de-asuntos-de-emails-de-phishing-en-empresas/>
- Paus, L. (2015). *ESET*. Retrieved from <https://www.welivesecurity.com/la-es/2015/04/13/alerta-phishing-entidad-financiera-chile/>

- Pérez, I. (2015). Retrieved from <https://www.welivesecurity.com/la-es/2015/05/07/como-funciona-un-iframe/>
- Rodriguez, E. (2005). Metodología de la Investigación. In E. Rodriguez, *Metodología de la Investigación*. Juarez.
- Samani, R. (2015). *Hacking the Human Operating System*. Intel Security.
- Samani, R., & McFarland, C. (2015). *Hacking the Human Operating System*.
- Santelices, A. C. (2006). Introducción a la Psicología Social . In A. C. Santelices, *Introducción a la Psicología Social* . San José: Euened.
- Sebastián, S. A. (2011). *Ingeniería social: Psicología aplicada a la seguridad*.
- Sjouwerman, S. (2011). *Cyberheist: The biggest financial threat facing American businesses since the meltdown of 2008*. KnowBe4.
- Tecnología, B. M. (2017). Retrieved from <https://www.bbc.com/mundo/noticias-40802167>
- Thomas, M. (2015). Avoid Framework Overload Use COBIT5 to Leverage Multiple Best Practices. *ISACA South Africa Chapter*, (p. 36).
- Vergara, M. M. (2000). *Confianza y Desarrollo del Potencial Humano* .
- Zetter, K. (2016). Retrieved from Wired: <http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>
- (2014). Retrieved from <https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen>