OFICINA DE POSGRADO

Tema:

DISEÑO DE UNA GUIA PARA CAMPAÑAS DE INGENIERÍA SOCIAL AL INTERIOR DE UNA INSTITUCIÓN FINANCIERA

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la información

Autor:

Ing. Daniel Roberto Peña Pérez

Director:

Ing. Galo Mauricio López Sevilla, MSc.

Ambato – Ecuador

Marzo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

DISEÑO DE UNA GUÍA PARA CAMPAÑAS DE INGENIERÍA SOCIAL AL INTERIOR DE UNA INSTITUCIÓN FINANCIERA

Líneas de Investigación:

Seguridad de la información

Autor:

Ing. Daniel Roberto Peña Pérez

Galo Mauricio López Sevilla, MSc. f. _____

CALIFICADOR

Darío Javier Robayo Jacome, MSc. f. _____

CALIFICADOR

José Marcelo Balseca Manzano, MSc. f. _____

CALIFICADOR

Juan Carlos Acosta Teneda, P, PhD. f. _____

DIRECTOR UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villarroel, Dr. f. _____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Marzo 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **DANIEL ROBERTO PEÑA PÉREZ,** con CC. **180422681-7** autor del trabajo de graduación intitulado: "DISEÑO DE UNA GUÍA PARA CAMPAÑAS DE INGENIERÍA SOCIAL AL INTERIOR DE UNA INSTITUCIÍN FINANCIERA", previa a la obtención del título profesional de **MAGISTER EN CIBERSRGURIDAD**, en la **OFICINA DE POSGRADOS**.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, marzo 2022

Daniel Roberto Peña Pérez

CC. 180422681-7

AGRADECIMIENTO

Quiero empezar por agradecer a Dios por permitirme culminar esta etapa de mi vida, por ser la luz y sabiduría en mi camino. A la Pontificia Universidad Católica del Ecuador Sede Ambato que me permitió crecer como persona y profesional. A nuestra Coordinadora Msc. Teresita Freire, por su cariño, bondad y acompañamiento durante todo este ciclo. A cada uno de los docentes que brindaron todo su conocimiento para formarme como un profesional integro. A mis padres y hermanos, pero en especial a mi hermana Cristina Peña por todo el apoyo moral y afectivo durante este proceso.

DEDICATORIA

El presente trabajo investigativo está dedicado a mis padres y hermanos por haberme forjado como la persona que soy actualmente, muchos de los logros se los debo a ustedes, que, aunque se ha pasado por momentos difíciles siempre me han brindado su compresión y cariño.

A mis compañeros y amigos presentes y pasados quienes compartieron conmigo su compañía y conocimiento. A todas aquellas personas que estuvieron durante este proceso apoyándome y lograron que este sueño se haga realidad.

RESUMEN

Las empresas financieras manejan datos críticos que permiten accesos o permisos a sistemas de información financieros de los empleados, proveedores y clientes que necesitan ser protegidos de diferentes ataques cibernéticos como la ingeniería social. En la protección de datos es importante considerar el desarrollo de las capacidades físicas como humanas puesto que estos últimos son sujetos hacer persuadidos por ciberdelincuentes. En este sentido el objetivo del presente trabajo busca diseñar una guía de campañas de ingeniería social al interior de una institución financiera, con las técnicas de ingeniería social que utilizan los atacantes. Para cumplir con el mismo se hace uso de la metodología Kanban que tiene como primera fase estudiar diferentes metodologías del SGSI, en la segunda fase se realiza el diagnostico situacional de las instituciones financieras con una encuesta sobre seguridad de información a empleados de una institución financiera en este caso la Asociación Mutualista Ambato, en la tercera fase se realiza una evaluación de la guía desarrollada respecto a las recomendaciones de INCIBE, con los resultados obtenidos de las fase indicadas anteriormente se concluye que las entidades financieras debiesen fortalecer su Sistema de Gestión de Seguridad de la información además de capacitar a cada uno de los empleados sobre distintos métodos y técnicas de ingeniería social, que se proponen en la guía desarrollada.

Palabras clave: Ingeniería social, Seguridad de la información, Guía de ciberseguridad, Phishing.

ABSTRACT

Financial companies handle critical data that allow access or permissions to financial information systems of employees, suppliers and customers that need to be protected from different cyberattacks such as social engineering. In data protection it is important to consider the development of physical and human skills, the last ones are subjects to be persuaded by cybercriminals. In this sense, the objective of this work is to design a guide for social engineering campaigns within a financial institution, with the social engineering techniques used by attackers. In order to reach this objective, the Kanban methodology is used; its first phase is to study different ISMS methodologies. In the second phase, a situational diagnosis of the financial institutions is carried out with a survey on information security to employees of a financial institution, in this case the Asociación Mutualista Ambato, In the third phase an evaluation of the guide developed with respect to the recommendations of INCIBE is made, with the results obtained from the phase indicated above it is concluded that financial institutions should strengthen their Information Security Management System in addition to training each of the employees on different methods and techniques of social engineering that are proposed in the guide developed.

Keywords: Social Engineering, Information Security, Cybersecurity Guide, Phishing.

ÍNDICE

PRELIMINARES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Hoy en día el mundo se encuentra en una era globalizada e industrializada a nivel tecnológico, la cual ha ocasionado que las empresas siempre sean blanco ante ataques y delitos informáticos, sin importar si estas sean de carácter privado, público, educativo o hasta religioso. Este tipo de ataques afecta la privacidad de la información digital de los usuarios finales, o en ciertos casos dependen de la vulneración donde se ha llegado a poner en riesgo la seguridad regional o nacional de los estados.

En la actualidad la información se ha convertido en un bien valioso para las organizaciones, compartir o divulgar esta información con otras entidades o personas, conlleva un riesgo a la privacidad, porque se ve expuesta a una serie de vulnerabilidades como la manipulación de usuarios legítimos para obtener datos críticos que permitan accesos o permisos a sistemas de información. En las instituciones financieras el manejo de información sensible de los clientes seria manipulada con mucha precaución, pues son estas organizaciones las más atacadas por ciberdelincuentes que buscan acceder a los recursos financieros de las cuentas. Es común observar diversidad de ataques de tipo *phishing*, *malware* y de ingeniería social (IS) dentro de organizaciones financieras, de igual forma, las estadísticas muestran a las instituciones financieras como los primeros blancos de ataques de este tipo.

Si una empresa quiere ser competitiva en los tiempos que corren contaría con sistemas, recursos y plataformas de las Tecnologías de la Información y Comunicación (TIC) ágiles y con un alto nivel de disponibilidad, lo que exige una gestión efectiva y un amplio proceso de transformación digital. El proceso de transformación digital en el que están inmersas la mayoría de las organizaciones y la sociedad en general permite, que se cometan ataques contra la seguridad informática de las empresas desde cualquier parte del mundo que utiliza como herramienta tan solo un ordenador. Es por esto, las organizaciones tienen que prestar especial atención a protegerse de posibles ataques eventuales, nadie está a salvo de los malware (Tuyú Technology, 2017, p. 1)

Por otra parte, uno de los principales blancos para ataques y delitos informáticos son las entidades bancarias, debido a la sensibilidad de la información que manejan en el medio, así como también, por la diversidad de aplicaciones y canales electrónicos que utilizan para los clientes. Dicho de otro modo, según un estudio realizado por la multinacional Visa en el año

2020 se evidencia un aumento considerable en el uso de aplicaciones bancarias como la banca en línea, esto conlleva a tener riesgos y amenazas de atacantes, no solo externos sino también, internos, debido al desconocimiento de los vectores de ataques informáticos que, día a día se diversifican a gran escala.

Las estafas informáticas representan más del 80% de los delitos informáticos, según los últimos informes anuales publicados por la Fiscalía General del Estado, aunque hay otra gran variedad de acciones ilícitas que llegan a los tribunales. La implementación inmediata de medidas de seguridad técnicas específicas, para evitar las brechas de seguridad o las consecuencias de estas, es exigida por las diferentes normas que ya están en vigor como, por ejemplo, la NIS o el Reglamento General de Protección de Datos. La exigibilidad de esta última comenzó en 2018, con sanciones por su incumplimiento con multas de hasta 20 millones de euros o de hasta el 4% de la facturación global del año financiero anterior, eligiéndose la cifra más alta (Fernández, 2019, p.1).

Existe un factor importante en esta problemática, las organizaciones no toman en cuenta en el momento de planificar, la seguridad de la información; y centralizan sus esfuerzos en fortalecer la seguridad física. Es decir, al ser el usuario quien tiene la información, se le considera vulnerable para cualquier tipo de ciberataques en especial mediante ingeniería social. Las cuales serían de dos tipos: físico y psicológico. El primero se refiere al medio, que se va a utilizar para ejecutar el ataque, el segundo es la táctica adecuada que utiliza el atacante para obtener la información deseada. Estos dos tipos de ataques son recurrentes dentro de instituciones financieras debido a la efectividad que tienen dentro del mundo de la ciberseguridad. En base al contexto planteado la idea a defender es: La implementación de campañas de ingeniería social mejora el nivel de seguridad de la información dentro de la institución.

La importancia de la investigación se basa en que, según las entidades bancarias, los eventos de i) phishing, ii) ingeniería social, y, iii) software espía (malware o troyanos) fueron los más frecuentes contra sus usuarios de servicios financieros, situación que resulta congruente con lo manifestado por los usuarios al ser consultados por los incidentes experimentados. También resulta importante anotar que, en promedio, un 26% de las entidades bancarias detectaron estos tipos de eventos mediante sistemas propios, lo que pone en evidencia la necesidad de la implementación de algún método de protección ante estos tipos de ataques.

Por otra parte, Carvajal y Castellanos (2019) manifiestan que: Es necesario conocer el funcionamiento de la ingeniería social; esta apunta a persuadir el factor humano en la estructura organizacional, considerada para muchos como la parte más débil del sistema. Actualmente, la información es uno de los recursos más valiosos para las organizaciones, proteger adecuadamente los datos es de vital importancia, pondría en riesgo el funcionamiento y rentabilidad del negocio (p. 14). Argumento que resalta la importancia y necesidad de la investigación planteada.

A fin de prevenir la situación polémica actual que son: los ataques de ingeniería social en una institución financiera, el presente trabajo se sustenta en la elaboración de una guía para campañas de prevención, a fin de satisfacer las necesidades de la investigación planteada se han establecido los siguientes objetivos:

- Recopilar información del estado del arte y práctica actual de las técnicas y herramientas de campañas de ingeniería social para instituciones financieras.
- Comparar diferentes técnicas y herramientas de campañas de ingeniería social en instituciones financieras.
- Sintetizar mejores prácticas de campañas de ingeniería social aplicada a instituciones financieras
- Organizar los elementos constitutivos de una guía para campañas de ingeniería social con el personal interno de una institución financieras.

De acuerdo con los objetivos planteados, para el desarrollo del trabajo de investigación, y a fin de responder la idea a defender: La implementación de campañas de ingeniería social mejora el nivel de seguridad de la información dentro de la institución, se utilizan diversas metodologías, dentro del proceso investigativo se emplea el método inductivo-deductivo con la finalidad de investigar las necesidades del diseño de la guía, mediante del instrumento de la encuesta. Así también, se emplea el modelo descriptivo para el análisis de la información recopilada y el estudio de los datos planteados, a fin de la ejecución de una investigación moldeada a las necesidades de la organización.

Una vez realizada la encuesta, gracias al método mixto transversal se procede a la extracción de la información, de igual forma para el desarrollo de la campaña se emplea la metodología Kanban para la gestión del proyecto, una metodología comúnmente usada para la producción ajusta inventada e implementada por primera vez en la empresa Toyota, ayuda a

disminuir desperdicios en la producción sin afectar el costo de la producción, esta metodología se aplicaría en todos los procesos de mejora continua dentro de cualquier organización.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Análisis de la seguridad de la información.

En la actualidad, toda empresa pública o privada garantiza lo, que se conoce como la triada de la seguridad de la información, este concepto corresponde a la integridad, disponibilidad y confidencialidad de los datos, para sus usuarios finales, debido que, si la información digital fuera vulnerada de alguna forma, la compañía perdería credibilidad y se pondría en riesgo el prestigio de la empresa. Es por esta razón que, día a día la industria de la ciberseguridad se ha dedicado a diseñar e implementar medidas que permitan proteger los datos digitales sensibles dentro de cada una de las instituciones, para de esta forma garantizar a sus clientes la tranquilidad que, su información está en lo posible resguardada.

A estos métodos de protección de datos o información digital se le conoce como seguridad de información y en concordancia con Ramos, Urrutia, Ordoñez y Bravo (2017) juega un papel importante en el desarrollo empresarial del momento, en tal sentido las empresas independientemente del tipo de servicio que ofrezcan a la sociedad tienen que salvaguardar su información y es en este punto en el cual la seguridad informática juega un papel importante. En este sentido la información no solo seria referido como un problema tecnológico, sino también organizativo y de gestión para afrontar las amenazas desde diferentes puntos de referencia en el cual la tecnología juega un papel importante (p. 89).

Dicho de otro modo, la disciplina que contiene las diferentes medidas de protección física hacia los datos digitales dentro de una empresa u organización, se la conoce como seguridad de la información y su objetivo es garantizar el cumplimiento de la tríada de la información la cual hace referencia a tres aspectos:

1.1.1. Integridad

Garantiza que la información no sea modificada por agentes externos a la organización. La integridad implica mantener la consistencia, precisión y confiabilidad de los datos durante todo su ciclo de vida. Los datos no serían modificados en tránsito, y se tomarían medidas para garantizar que personas no autorizadas no alteren los datos (por ejemplo, en una violación de la confidencialidad). Estas medidas incluyen permisos de archivos y controles de acceso de usuarios (Ontek, 2018, p.1).

Una de las mejores técnicas utilizadas para evitar una vulneración a la integridad de la seguridad de los datos es, el control de versiones los cuales permiten evitar cualquier cambio o eliminación accidental o intencional de la información por usuarios no autorizados, además se considera que los cambios no solo ocurrirían por eventos de terceros como pulso electromagnéticos que bloquearían el servidor, otro método de protección es las sumas de verificación criptográficas o copias de seguridad con redundancias a fin de restaurar los datos por una manipulación (Ontek, 2018, p.1).

1.1.2. Confidencialidad

Prevenir la difusión de la información digital sensible de una organización. De acuerdo con el blog de seguridad Ontek (2018) la confidencialidad es aproximadamente equivalente a la privacidad. Las medidas emprendidas para garantizar la confidencialidad están diseñadas para evitar que la información confidencial llegue a las personas equivocadas, al tiempo, que se garantiza que las personas adecuadas accedan a ella: el acceso estaría restringido a aquellos autorizados para ver los datos en cuestión. También es común que los datos se clasifiquen de acuerdo con la cantidad y el tipo de daño, que se realizaría si cae en manos no deseadas. Se implementarían medidas más o menos estrictas de acuerdo con esas categorías (p. 1).

A fin de mantener la confidencialidad es necesario realizar capacitación al personal que posee acceso a la información digital sensible, la cual contendría temáticas acerca de los riesgos de seguridad, esto permite al usuario entender acerca de los riesgos, así como a protegerse de los mismos. Esta metodología incluiría técnicas como seguridad en contraseñas, prevención ante ataques de phishing o ingeniería social, de esta forma se busca evitar doblar la seguridad datos confidenciales (Ontek, 2018, p.1).

1.1.3. Disponibilidad

Ofrece el acceso a la información digital en cualquier momento que los usuarios requieran de la misma. Para garantizar este ítem, es necesario mantener la infraestructura en óptimas condiciones, es decir “se realiza reparaciones de hardware de inmediato cuando sea necesario lo que permite tener un entorno de sistema operativo que funcione correctamente y libre de conflictos de software. También es importante mantenerse al día con todas las actualizaciones necesarias del sistema” (Ontek, 2018, p.1).

Un sistema adecuado de protección es mantener un servicio con un ancho de banda adecuado a fin de que, los usuarios accedan al servicio de internet en alta demanda, así como servicios de alta disponibilidad mediante el arreglo de discos en servidores a fin de disminuir servicios en hardware. Un sistema de recuperación antidesastres o planes de contingencia está basada en escenarios de alto riesgo. Otro método importante de protección es además las copias de seguridad, a fin restaurar el servicio en caso de alguna caída o interrupción del servicio (Ontek, 2018, p.1).

La tríada de la información (CID), es la base de la ciberseguridad, es decir, cada ocasión que un usuario sufre un ataque, es debido a la vulneración de uno de estos tres principios. Todo profesional de ciberseguridad se encarga del análisis de amenazas y vulnerabilidades basado en el impacto potencial que cualquier ataque genere sobre la CID, en todos los aplicativos, y sistemas críticos dentro de su organización, con el uso de los controles de seguridad para reducir el riesgo informático.

La seguridad de la información (SI) tiene un ámbito trascendental para cualquier organización, debido a que si esta es vulnerada se perdería credibilidad ante los clientes. La economía actual determina el éxito o fracaso de las organizaciones en la medida que aprovechen su información para adaptar su oferta y obtener ventaja competitiva en el mercado. Sin embargo, esta realidad ha expuesto a la data como uno de los centros de atracción para la ciberdelincuencia. Citar casos como el Ciberataque a British Airways en el cual 380000 usuarios vieron comprometidos sus datos en operaciones realizadas a través de su página web. Nombres, emails y detalles de las tarjetas de crédito de clientes que tuvieron transacciones entre agosto y septiembre 2018, habían sido robados (Morales, Toapanta, Toasa, 2019, p. 554)

En caso de, que se filtre o se vulnere la información de los clientes en una organización, se generaría graves inconvenientes, y consecuencias como la pérdida del prestigio de los clientes hacia la empresa, lo que ocasionaría pérdidas económicas sustanciales en el negocio, o en ciertos casos hasta problemas legales por la filtración de información, hasta llegar al cierre definitivo de las empresas. Este ámbito resalta la importancia de asegurar los datos digitales sensibles, por lo que, la SI ha sufrido un crecimiento exponencial en los últimos años dentro de esta evolución se han planteado diversas técnicas de protección como:

- Planificación de la continuidad de negocio
- Ciencia forense digital.
- Administración de Sistemas de Gestión de Seguridad.

Toda metodología será implementada acorde a las necesidades de la organización a proteger, siempre con un estudio previo que permita definir el alcance para la técnica a emplear. A juicio de Guzmán (2015) la seguridad de la información dentro de las organizaciones, depende del nivel de protección y seguridad de sus activos de información, por lo tanto, es fundamental la implementación de medidas y controles de seguridad adecuados, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad (p. 31).

Dichas técnicas o métodos son denominados Sistema de Gestión de Seguridad de la Información (SGSI), y consiste en la secuencia estructurada orientada a la identificación y valoración documentada de los riesgos informáticos, que se generen dentro de una organización, para de esta forma adaptarse ante un proceso de mejora de prevención de los riesgos ante delitos informáticos. La SGSI tiene la necesidad de una intervención activa de toda la organización con base fundamentada en una planificación definida e implementación de técnicas para proteger la seguridad de la información al igual que el mantener el control de acceso a todos los recursos y activos de información.

La gestión de la seguridad de la información, implica que las organizaciones clasifican sus activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad, con el propósito de identificar los riesgos que afectarían su seguridad y determinar las medidas de prevención, detección, retardo y reacción, que se requieran implementar para controlar el acceder no autorizado a las instalaciones, recursos, sistemas e información de la organización, o cualquier amenaza proveniente del entorno, la naturaleza y las acciones del hombre que llegaria a comprometer el normal funcionamiento y operación del negocio (Guzmán, pp. 31-32).

Todo SGSI tiene un enfoque empresarial corporativo y está orientado al diseño de seguridad informática en una estructura organizacional en base a todos los activos informáticos y de esta forma establecer controles sobre los mismos para la protección de los datos, como se evidencia en la Figura 1.1:

Figura 1.1. Modelo Sistema de Gestión de la seguridad de la información

Fuente: Enterprise (2021, p. 1)

Se establecen los diferentes controles de seguridad sobre los activos de información en los distintos medios tecnológicos dentro de la organización. Además, se evidencia que los involucrados en el sistema son todos los usuarios mediante sus diferentes roles en la organización. De igual forma, dicho Sistema de Gestión de Seguridad de la Información contiene diversos procesos metodológicos para garantizar la tríada de la información y de esta forma dar una continuidad segura al negocio para sus clientes y usuarios.

Toda empresa posee dos tipos de información pública y privada, la cual solo sería vista por el personal autorizado, en este punto las entidades financieras son quizá una de las organizaciones con mayor cantidad de información sensible debido a las operaciones que manejan como las transacciones monetarias, por tal motivo son uno de los principales blancos de ataques informáticos no solo a nivel local sino también a una escala mundial. Por ello, dicha organización además de tener la obligatoriedad del aseguramiento de su infraestructura tecnológica también se encargaría de la regularización y control acerca del buen manejo, que se tiene en el uso de las plataformas que sostiene.

Por otra parte, una de las entidades que más han hecho énfasis en la implementación de modelos de Sistemas de Gestión de Seguridad de la Información, son las entidades financieras, esto es debido al despliegue de nuevas tecnologías que usan para sus usuarios, generan brechas y vulnerabilidades de la seguridad informática. “Solamente durante el año 2017, más de cuatro mil millones de registros fueron expuestos al robo informático los

ciberdelincuentes atacaron muchas organizaciones, desde pequeñas firmas hasta el sistema bancario internacional" (Computerworld, 2021, p. 1)

Todos estos avances tecnológicos evidencian un riesgo informático en las entidades financieras razón por la cual, dicho sector depende directamente de la correcta implementación de un SGSI para controlar su seguridad informática, es así como en el estudio planteado por los autores Ojera, Moreno y Torres se manifiesta que: los cambios que adopta la banca en la era digital representan hoy en día nuevos riesgos que amenazan su permanencia en el mercado, por lo que, el departamento de gestión de riesgo de las entidades financieras, entre estas cooperativas de ahorro y crédito, además de transfigurarse y familiarizarse a la digitalización para prevenir y mitigar de manera oportuna los riesgos, mediante reglamentos internos de protección de los usuarios y de toda la entidad (Ojeda & Moreno, 2020, p. 1)

Cabe destacar que, uno de los aspectos más importantes para la implementación de un Sistema de Gestión de Seguridad de la Información, es quizá el costo en análisis del alcance del mismo. Si bien, todo SGSI tiende a la protección de datos sensibles confidenciales, la realidad de cada empresa es diferente, por lo cual existen diversas metodologías para la correcta implementación del sistema; las entidades financieras no son la excepción y sus controles están regularizados por entes superiores como es el caso del Banco Central en el caso de los bancos y la Superintendencia de Economía Popular y Solidaria en el caso de las Cooperativas y Mutualistas, por otra parte la metodología más utilizada es la ISO 27000 la cual contiene ciertos ítems orientado a la protección de los datos digitales.

1.2. Análisis de los Sistemas de Gestión en Entidades Financieras

Un SGSI permite a cada organización, mantener una gestión adecuada sobre los riesgos informáticos presentados en el medio, esto se lo realiza mediante el estudio de amenazas, que se comprometería la seguridad de los activos informáticos, lo que permite a sus usuarios mantener la certeza de la mitigación en las amenazas informáticas. Además, admite el gobierno sobre la protección de los datos, basado en una estructura organizacional. En las entidades financieras el control se ha planteado con el fin de garantizar a los clientes el resguardo adecuado del sistema monetario. Por otra parte, al mantener una consciencia de los peligros ante ataques, el Foro Económico lideró la creación del consorcio sectorial a

través del Centro Global de Ciberseguridad para una mejora continua de la ciberseguridad en el ámbito financiero, con sede en Ginebra Suiza.

La implementación de un SGSI, se basa en la detección de vulnerabilidades, prevención de amenazas, análisis de metodologías de protección y respuesta ante incidentes para el manejo de fraude y amenazas en ciberataques, esta estructura holística permite la capacidad de integrar herramientas para mantener integra la información, a criterio de Pincay (2021) estos controles están basados en:

- **Seguridad de la Información** como área responsable de definir, implementar, controlar y mantener el modelo de seguridad de la información con el fin de preservar la confidencialidad, integridad y disponibilidad del activo más importante de la organización: la información. El modelo de seguridad de la información es el conjunto de normas, políticas, procedimientos, estándares y herramientas que permiten preservar la confidencialidad, disponibilidad e integridad de la información. Igualmente, los procesos de investigación del evento, que se generen como alertas de incidentes de seguridad de la información.

- **Seguridad Informática** como área responsable del mantenimiento y monitoreo de herramientas tecnológicas que estarían administradas de acuerdo con las normas definidas en el modelo de seguridad de la información y que permite generar alertas de incidentes de seguridad.

- **Prevención de Fraudes** como área responsable de la analítica de grandes bases de datos y de la generación de modelos de correlación de variables que permitan identificar el comportamiento del fraude y generar acciones preventivas en herramientas de monitoreo de transacciones.

- **Seguridad Bancari**a como área de investigación de los eventos de fraude, que se presentan, con el fin de determinar causas y responsables, información que permite alimentar a los modelos de correlación de variables, que se desarrollan en el área de Prevención de Fraudes (Pincay, 2021, p.1).

Cada ítem corresponde a la implementación de un SGSI, sin embargo, la metodología para la implementación del sistema varia debido a la variedad de normativas como se muestra en la Tabla 1.1:

Tabla 1.1. Metodologías para Sistemas de gestión de seguridad de la información

Metodología	Caracterización
OCTAVE	Desarrollada por el Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa. Por tanto, se tienen en cuenta las necesidades de la empresa donde se implementa, lo que permite reducir los riesgos de seguridad de información, para lograr una mayor protección a estos elementos dentro del sistema. Equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que, a partir de éstos, los entes empresariales tomarían decisiones de protección de información basado en los principios de la seguridad de la información. Esta metodología persigue dos objetivos específicos que son: concientizar a la organización que la seguridad informática no es un asunto solamente técnico y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos.
MEHARI	Es definida por la organización francesa especializada en la seguridad de los sistemas de información (CLUSIF) como una metodología que proporciona un conjunto de herramientas que permiten hacer un análisis de riesgos cualitativo y cuantitativo, cuando sean necesario para tener una adecuada gestión de seguridad. De lo anterior, se deduce que está diseñada para acompañar los procesos de análisis de riesgos empresariales tanto actuales como futuros. En la metodología MEHARI se hace un análisis de la seguridad basado en tres criterios básicos confidencialidad, integridad y disponibilidad.
MAGERIT	Es reconocida por ENISA (Agencia Europea de Seguridad de las Redes y de la Información) y promovida por el Consejo Superior de Administración Electrónica con el fin de sistematizar el análisis de los riesgos, que se presentarían los activos de una organización Esta metodología es importante porque el crecimiento de la tecnología dentro de las organizaciones se genera de manera exponencial y, por lo tanto, es necesario minimizar los riesgos asociados al uso de los sistemas que garantiza la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización. MAGERIT es una de las metodologías más utilizadas en el ámbito empresarial , les permite prepararse para procesos de auditorías, certificaciones y acreditaciones

CRAMM	Es el método de análisis y control de riesgos de la Central Computer and Telecomunicaciones Agency (CCTA) del gobierno británico, permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las organizaciones día a día y es definida como una metodología que aplica los conceptos de manera formal, estructurada y disciplinada para proteger los principios de seguridad de la información de un sistema y de sus activos. Cabe resaltar que CRAMM realiza un análisis de riesgos cualitativo y cuantitativo por lo, que se conoce como una metodología mixta, ésta se apoya de una herramienta de gestión, lo que permite a las organizaciones tener una visión clara y priorizada de las amenazas a las que está expuesta y que afectarían los recursos y la continuidad del negocio, basándose en una matriz donde las filas representan los activos y las columnas los riesgos que afectarían la integridad, disponibilidad y confidencialidad de los mismos, por otro lado, CRAMM proporciona información acerca de las características de funcionamiento del sistema y una identificación profunda y clara de los activos, que se encuentran más expuestos. Los elementos, que se tendrían en cuenta para realizar un adecuado análisis de riesgos con la metodología CRAMM son: activos, vulnerabilidades, riesgos, amenazas, contramedidas, implementación y auditoría, los cuales permiten obtener un mejor resultado y asegurar la continuidad de negocio.
EBIOS	Es una metodología francesa de gestión de riesgos, fue creada por la dirección Central de seguridad de los sistemas de Información de Francia DCSSI, con el fin de posibilitar la comunicación con los clientes internos y externos para contribuir al proceso de la gestión de riesgos de seguridad de los sistemas de información, de igual manera, ayuda a la empresa a tener un mayor reconocimiento en sus actividades de seguridad, esta tiene compatibilidad con las normas internacionales como la ISO. Este procedimiento permite a la organización tener un mayor conocimiento de sus activos y las necesidades de seguridad que permite identificar las amenazas y vulnerabilidades a las, que se encuentran expuestos para su posterior mitigación
NIST SP 800:30	Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI (Tecnología de la Información), proporciona un guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica. Por otro lado, esta guía provee fundamentos para la administración de riesgos, así como la evaluación y mitigación de los riesgos identificados dentro del sistema de TI con el objetivo de apoyar a las organizaciones con todo lo relacionado a Tecnología (CERT,2013).La metodología NIST SP 800:30 está compuesta por nueve fases: caracterización del

	sistema, la cual permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa; identificación de amenazas, es donde se definen las fuentes de motivación de las mismas; identificación de vulnerabilidades, en esta fase desarrolla una lista de defectos o debilidades del sistema que serían explotadas por una amenaza; análisis de controles; determinación de la probabilidad; análisis de impacto; fase de determinación del riesgo, ayuda a evaluar el riesgo en el sistema de información, recomendaciones de control en donde se proporcionan los controles que mitigarían el riesgo identificado disminuyéndolo hasta un nivel aceptable, finalmente está la documentación de resultados la cual genera un informe con la descripción de amenazas y vulnerabilidades, que permite medir el riesgo y realizar recomendaciones para la implementación de controles.

Fuente: Tejena (2018, pp. 234-237)

Cada metodología se basa y se adapta a las necesidades empresariales, al igual que todas ellas especifican en sus apartados, la concientización de la información digital no solo del personal externo sino también interno. Por otra parte, gran parte de las metodologías detalladas tiene una relación directa con la Normativa ISO 27000, la cual: es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 (Nieves, 2017, p.12)

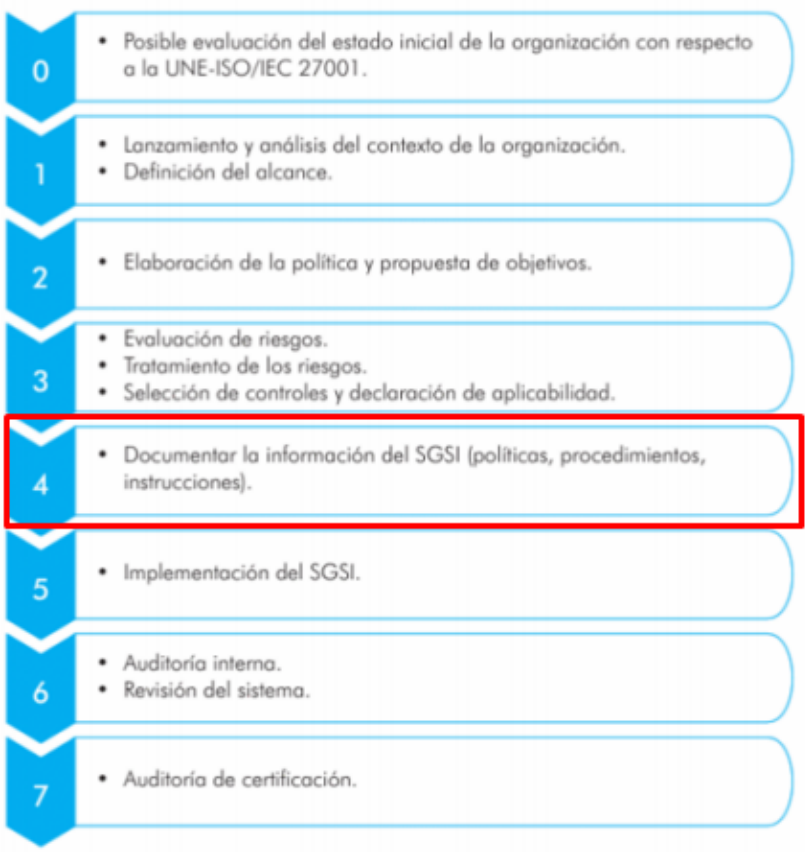
La Normativa ISO ayuda a mantener la mejora continua en el ámbito de la seguridad sobre los activos físicos y digitales como es el caso de la información, esto se basan en una serie de estándares enfocados en los riesgos de cada organización, dicho proceso consta de niveles o escalones centralizados en las funciones de cada usuario interno y externo de la organización, estos de acuerdo al estudio planteado por Muñoz (2020) son:

- Nivel 0, el 'sentido común'.
- Nivel 1, el cumplimiento de la legislación obligatoria.
- Nivel 2, evaluación del proceso de Gestión de Seguridad.
- Nivel 3, analizar el riesgo y la gestión de su resolución.

- Nivel 4, adquisición de productos para integrarlos en los Sistemas de Gestión.
- Nivel 5, integración de los componentes certificados en sistemas compuestos y su certificación.

En el contexto de la investigación, el desarrollo de una metodología para campañas de prevención de ataques de ingeniería social en entidades financieras, parte del principio de un Sistema de Gestión de Seguridad de la Información, por la evidente necesidad al respecto de altas vulnerabilidades que poseen no solo el personal externo a la organización. Por tal motivo, dentro de la gestión de una información segura no solo se haría énfasis en asegurar la infraestructura tecnológica, sino más bien se haría uso de las gestión documental y procesos como una fase importante en el SGSI, la cual consta dentro de la normativa ISO como recomendaciones para garantizar la Disponibilidad, Confidencialidad e Integridad de los datos de la institución financiera, todas estas fases están detalladas a continuación:

Figura 1.2. Fases del proyecto de implementación de un SGSI



Fuente: Cárdenas y Solares (2016, p.73)

Todas las fases de la implementación de un Sistema de Gestión de Seguridad de la información, corresponde a un solo objetivo el cual es mitigar el riesgo ante las vulnerabilidades dentro de la organización, los cuales se clasifican en:

- ***Origen Natural:*** Catástrofes Naturales.
- ***De entorno:*** Cualquier daño en la organización.
- ***Defecto de aplicaciones:*** Fallas en el software o la aplicación.
- ***Accidentales:*** Mal uso por desconocimiento de las aplicaciones o equipos por parte de los usuarios.
- ***Intencionales:*** Ataques directos la infraestructura tecnológica de la Institución.

1.3. Diagnóstico de los ataques informáticos en entidades financieras

Con el pasar del tiempo y los avances de la tecnología, ha dado inicio a nuevos vectores de ataques informáticos, así como también nuevos métodos para delitos informáticos, los cuales

han dado un nuevo giro a las comunicaciones mediante las tecnologías informáticas. En base al contexto planteado Mieres (2009) defino a un ataque informático en: aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, que causa un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización (p. 4).

Un ataque informático seria hacia la base de datos, servidores, equipos de comunicación, y tiene por objetivo perjudicar cualquier componente de la tríada de la seguridad, para detener los servicios brindados por la organización, o utilizar la información sustraída y realizar estafas, espionaje o en ciertos casos hasta acciones más fuertes como secuestros. La gran demanda de herramientas digitales para la comunicación ha elevado el riesgo de ciberataques, los cuales usan como uno de los principales vectores de ataque u objetivos las entidades financiares debido a que la mayoría de los ataques son orientados al lucro o retribución económica.

Todo ataque, que se realiza a una Institución Financiera se la conoce como Fraude Financiero, que es definido como "la acción dolosa que provoca un perjuicio a un tercero, con la información obtenida hacen traspasos bancarios, venden información y hasta extorsionar a los propietarios de las claves" (Angulo & Córdova, 2019, pp. 7-8). El caso más común de un fraude financiero es vía *on-line* y consiste en que, un atacante ingresa a la banca en línea de la víctima y de esta forma sustrae todos sus fondos, y los traspasa a otra cuenta, que se encuentren ubicadas cerca para retirar el dinero de manera inmediata, dicho modo de ataque ha ocasionado que muchos usuarios pierdan los ahorros de toda su vida.

En base a este contexto, en los últimos años se ha presentado aumento considerable de ataques con y sin éxito a las entidades bancarias. A juicio de Gavilánez y Zambrano (2017) manifiestan que las instituciones más vulnerables a estos ataques cibernéticos considerándose su importancia y relevancia para el desarrollo económico de las naciones son precisamente las entidades financieras; para constancia se incorpora el golpe financiero sucedido en el año 2013 frente a la substracción de aproximadamente 1.000 millones de dólares a 100 entidades financieras en alrededor de 30 países. Convirtiéndose hasta la fecha, en el más grande robo de la historia perpetuado a este segmento del mercado de dinero (Gavilánez & Zambrano, 2017, p.31).

Estos ataques han sido efectuados a diferentes bancos a nivel mundial, es así como el reporte de Harán en el *Live Security de Eset* del año 2018 indica que, en febrero de 2018, el banco central de Rusia reveló que en 2017 un grupo de atacantes robó el equivalente a 6 millones de dólares de un banco local que utilizo el sistema internacional de mensajería SWIFT. Los atacantes comprometieron el equipo de un empleado antes de utilizar SWIFT para transferir fondos a sus propias cuentas. Este ciberataque es similar al, que se produjo contra la cuenta del Banco Central de Bangladesh ubicada en el Banco de la Reserva Federal de Nueva York. Apenas unos días previos, se conoció la noticia de que un grupo de atacantes que logró vulnerar los sistemas del *City Union Bank* de India intentó llevarse cerca de 2 millones de dólares, que también utilizo el sistema de intercambio SWIFT (Harán, 2018, p.1).

Entre los delitos informáticos a entidades financieras Ecuador tiene uno de los índices delictivos más elevados en los últimos años, es por tal motivo que, se resalta la importancia de evidenciar los tipos de ataques más comunes, que se dan las instituciones mencionadas, entre las, que se tiene son los siguientes:

- **La clonación de tarjetas de crédito:** En la clonación de tarjetas de crédito o *Skimming*, el delincuente, utiliza un aparato conocido como *Skimmer* u otro dispositivo similar, captura la información, que se encuentra grabada en una tarjeta de crédito o débito, para posteriormente pasarla a la banda magnética de otro plástico, o tarjeta, a fin de utilizarla de forma fraudulenta, procurándose bienes y/o servicios, cuyo importe serán cargados a la tarjeta original cuya información fue copiada (Pereira, 2012, p.42).

- **Suplantación de identidad:** Para suplantar la identidad los atacantes roban los datos de los usuarios para utilizarlos en su propio beneficio. Uno de los métodos más usados es el *spam*, que consiste en enviar una gran cantidad de mensajes de 'publicidad' no deseada al usuario, mediante un correo electrónico o mensaje de texto, con el objetivo que 'pinche' en el enlace adjunto y redirigirle a una *web* falsa controlada por el atacante, con el objetivo de robarle sus datos personales, cuenta bancaria, claves de acceso, entre otros (Arcotel, 2021, p.1).

- **Robo de credenciales:** El robo de identidad es un delito en el que, el atacante sustrae la información personal de la víctima, normalmente con la intención de cometer un

> fraude. La definición de robo de identidad engloba muchos tipos de información personal y fraudes perpetrados, desde el robo de dinero hasta la utilización de los datos de la víctima con objeto de recibir un tratamiento médico o solicitar un crédito. Robar una identidad sería tan sencillo como *hackear* la cuenta de la red social de una persona o tan complejo como presentar declaraciones fiscales en nombre de ella. Puesto que muchas personas publican libremente información sobre sí mismas en Internet, el robo de identidad es cada vez más frecuente, muchas víctimas de robo de identidad y fraude pasan años busqueda de resolver los delitos, sin garantía alguna de recuperar totalmente sus pérdidas (Avast, 2021, p. 1).

1.4. Ataques de ingeniería social

La ingeniería social basa su comportamiento en una premisa básica 'es más fácil manejar a las personas que a las máquinas'. Para llevar a cabo este tipo de ataque se utilizan técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que beneficiaría al ciberdelincuente. Los ataques de ingeniería social usan como canal principal para su propagación el correo electrónico gracias al uso masivo que tienen tanto por empresas, como por particulares. Pero no es la única vía de la que hacen uso los ciberdelincuentes, utilizarían otros canales de comunicación como llamadas telefónicas, aplicaciones de mensajería, redes sociales, etc (Incibe, 2019, p.1).

En la actualidad, se han desarrollado diversidad de técnicas a fin de generar los ataques existentes, por tal motivo, es importante tener conocimiento acerca de estos métodos para el análisis, y así garantizar que la implementación del SGSI, contenga un contexto acerca de prevención de estos ciberataques, estas técnicas se clasifican en:

Ingeniería social basada en humanos: Aquí se requiere conseguir datos sensibles a través de interacciones. Al respecto Hinojosa (2010) indica que, el ingeniero social entabla una relación con el objetivo o alguien cercano al mismo y de esta manera obtiene la información que desea. Los ingenieros sociales saben exactamente como explotar la parte humana, saben cómo llegar a las personas y hacer que ellos actúen de la manera que más les conviene (p. 53). Se las conoce como técnicas por comportamiento humano, a criterio de Hinojosa (2010) estas son:

- ***Ingeniería Social Inversa:*** Es cuando el atacante produce un daño en la red con el objetivo de ir a solucionar la falla el mismo, de esta forma se ha ganado la confianza del personal; La Ingeniería Social Inversa implica dos factores: Sabotaje y Marketing.
- ***Desarrollar confianza:*** Consiste en generar una confianza con la víctima y de esta forma empezar a obtener información confidencial.
- ***Afectividad:*** Utiliza el estado emocional de la víctima y se basa en miedo, emoción o pánico.
- ***Sobrecarga:*** Se basa en la premura de tratar mucha información en poco tiempo lo que ocasiona que la víctima sea manipulada.
- ***Relaciones basadas en engaños:*** Se basa en ganarse la confianza de la víctima para sustraer información y realizar así el ataque.
- ***Difusión:*** Se presenta cuando la víctima siente demasiada responsabilidad sobre sus funciones lo que es usado por el atacante para acercarse y ayudar supuestamente, cuando el objetivo es sustraer información.
- ***Integridad y consistencia:*** Se basa en la tendencia de entregar información solo al dejarse llevar por comentarios engañosos.
- ***Buscar en la basura:*** En la actualidad existen personas, que se encargan de buscar información sensible en los documentos desechados.
- ***Suplantación de identidad:*** En esta técnica el atacante se hace pasar por la víctima, ante algún conocido y de esta forma sustraer información.
- ***Ataques internos:*** Es uno de los ataques más frecuentes en la actualidad, se da cuando un miembro de la organización filtra información sensible de la misma.
- ***Acceso físico:*** Es cuando un atacante ingresa a las instalaciones de la organización y sustrae la información confidencial sensible del negocio.

Ingeniería social basada en computadores: La ingeniería social basada en computadores es aquella, que se lleva a cabo con la ayuda de computadoras o elementos tecnológicos, con los cuales se logra que el usuario crea que este interactua con el sistema computarizado real y se obtendría información confidencial a través de estos medios. Por ejemplo, el usuario encuentra una ventana emergente, informándole que su aplicación tiene un problema y que el usuario va a tener que autenticarse de nuevo para continuar. Una vez que el usuario haya ingresado su usuario y su clave en la ventana emergente, el daño está hecho. El hacker que

ha creado el Pop-Up ahora tiene el identificador o usuario y la clave y tendría acceso a la red y al sistema computacional (Hinojosa, 2010, p. 73).

Los ataques de ingeniería social por computadores están categorizados en:

- ***Correo:*** Envío de correos engañosos o *spam*.
- ***Windows Pop-Up:*** Se da cuando el usuario navega en el internet y se abren ventanas emergentes con el fin de sustraer información.
- ***Sitios Web:*** Paginas de premios engañosas, rifas fantasmas loterías.
- ***Phishing:*** Robar identidades mediante correos engañosos enviados.

Según la cantidad de interacciones que tenga el atacante con su víctima, los ataques de ingeniería social se clasifican en:

- ***Hunting:*** Este ataque de ingeniería social tiene como objetivo afectar la mayor cantidad de usuarios posibles con una comunicación, es el más común en técnicas de *phishing* y el vector de ataque está centralizado en entidades públicas o bancarias, entre los principales ejemplos se tiene la Figura 1.3 mostrada a continuación:

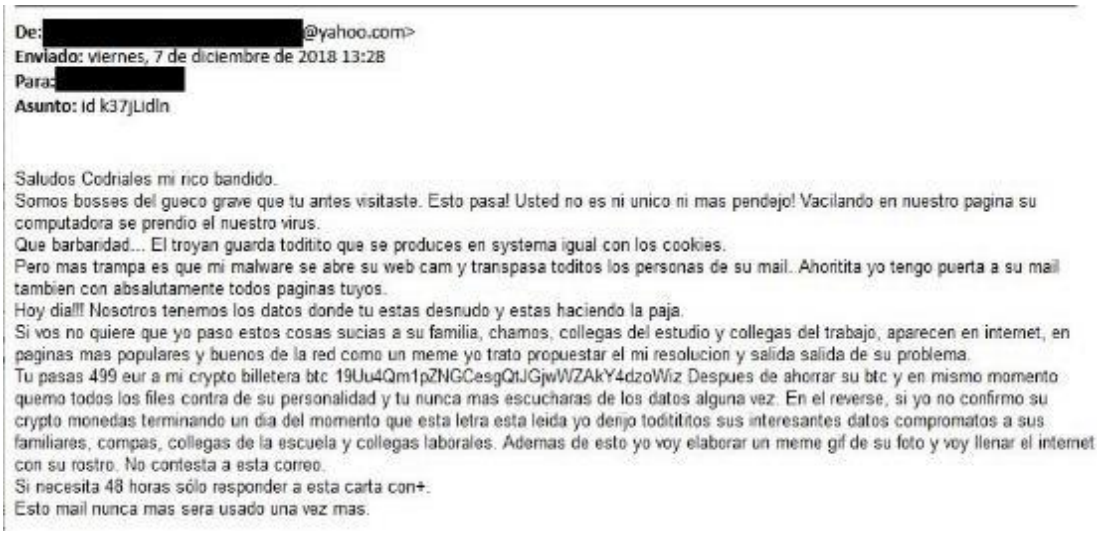
Figura 1.3. Ejemplo de *Hunting*

Fuente: elaboración Propia

Nótese en la figura presentada, como el correo es muy similar a los enviados por Banco Pichincha, sin embargo, el remitente es *'dah183@hotmail.com'* además manifiesta una 'supuesta' cuenta bloqueada y pide ingresar mediante un enlace, mismo que, al ingresar comprometerá la información de la víctima: En el año 2020 también se dio un caso similar con un ataque a través de la Agencia Nacional de Transito (ANT), esta consistía en un correo que manifestaba una multa por exceso de velocidad en la ciudad de Quito, la ANT de forma inmediata supo realizar un comunicado para aclarar la falsedad de ese correo y de esta forma prevenir a la ciudadanía en general.

- ***Farming:*** En el mencionado ataque los atacantes, para cumplir con el objetivo establecen una conversación con la víctima, mediante esta se sustrae la mayor cantidad de información, una estrategia planteada para este tipo de ataque es infundir miedo para que, las víctimas caigan en un chantaje, por supuestos videos privados o amenazas, como se evidencia en la Figura 1.4:

Figura 1.4. Ejemplo de correo de chanta



De: [redacted]@yahoo.com>
Enviado: viernes, 7 de diciembre de 2018 13:28
Para: [redacted]
Asunto: id k37jLidln

Saludos Codriales mi rico bandido.
Somos bosses del gueco grave que tu antes visitaste. Esto pasa! Usted no es ni unico ni mas pendejo! Vacilando en nuestro pagina su computadora se prendio el nuestro virus.
Que barbaridad... El troyan guarda toditito que se produces en systema igual con los cookies.
Pero mas trampa es que mi malware se abre su web cam y transpasa toditos los personas de su mail. Ahoritita yo tengo puerta a su mail tambien con absalutamente todos paginas tuyos.
Hoy dia!!! Nosotros tenemos los datos donde tu estas desnudo y estas haciendo la paja.
Si vos no quiere que yo paso estos cosas sucias a su familia, chamos, collegas del estudio y collegas del trabajo, aparecen en internet, en paginas mas populares y buenos de la red como un meme yo trato propuestar el mi resolucion y salida salida de su problema.
Tu pasas 499 eur a mi crypto billetera btc 19Uu4Qm1pZNGCesgQtJGjwWZAkY4dzoWiz Despues de ahorrar su btc y en mismo momento quemo todos los files contra de su personalidad y tu nunca mas escucharas de los datos alguna vez. En el reverse, si yo no confirmo su crypto monedas terminando un dia del momento que esta letra esta leida yo derijo toditititos sus interesantes datos compromatos a sus familiares, compas, collegas de la escuela y collegas laborales. Ademas de esto yo voy elaborar un meme gif de su foto y voy llenar el internet con su rostro. No contesta a esta correo.
Si necesita 48 horas sólo responder a esta carta con+.
Esto mail nunca mas sera usado una vez mas.

Fuente: Albors (2018, p. 1)

Como se evidencia en la figura, la víctima recibe una amenaza la cual argumenta que la víctima estuvo en sitios para adultos, y el equipo está infectado con un *malware*, además se argumenta que si quiere que no se divulgue las acciones la víctima realice una transferencia de 499 euros, que se traduce a 594,63 dólares americanos.

Como se evidencia en estos dos simples ejemplos, la ingeniería social posee un sin número de técnicas que buscan confundir a las víctimas mediante engaños y mentiras, para de esta forma conseguir información verídica que les permita acceder a sus dispositivos tecnológicos y así obtener algún rédito económico ya sea de forma directa o indirecta, este es un ataque al que toda la ciudadanía seria víctima, en algún momento, por lo cual el trabajo de investigación planteado busca generar una concientización a fin de mitigar estos riesgos, pero esto al ser un tema de índole mundial, cada institución toma medidas al respecto, por ejemplo Banco Pichincha (2020) en su página oficial manifiesta:

- Los ciberdelincuentes intentarán aprovecharse de tu curiosidad y buenas intenciones, que en ciertas ocasiones llegan a establer contactos no solicitados a nombre de gente que conoces o de una institución en la que confías.
- Los ataques de ingeniería social se suelen ejecutar a través de correos electrónicos o mensajes en redes sociales que contienen links o contenidos para abrir o

descargar. De esta manera, los estafadores no solo tendrán acceso a tu información sino a la de todos tus contactos.

- Intentarán generar un vínculo para que te sientas cómodo y confíes en ellos.
- Una vez que entablen una relación contigo, te pedirán acceso a tus cuentas y claves, para luego presionarte hasta que entregues esos datos.
- También influirian en tu decisión a través de incentivos, al recibir mensajes de una aparente fuente confiable en la que te piden que hagas clic para recibir regalos o descuentos no solicitados (Banco Pichincha, 2020, p. 1)

Por lo general, estos ataques hacen un análisis de vulnerabilidades a las personas mediante conversaciones o mediante un seguimiento, una vez que el atacante conoce a su víctima, este la manipularía de cualquier modo. Para realizar este tipo de ataque se hace uso de distintas técnicas como: pasivas (vigilancia), no presenciales (recuperación de contraseñas, correo, mensajería instantánea o vía telefónica), de forma presenciales no ofensiva (seguimiento a la víctima, búsqueda de información en agenda o inclusive hasta en la basura), agresivo (Chantaje, suplantación de personalidad, manipulación psicológica). Los atacantes también son conocidos como Ingenieros Sociales, por lo general están obsesionados con la información, razón por la cual pasan la mayor parte de su tiempo en la lectura acerca de nuevas tendencias tecnológicas y oscilan en un rango de edad entre 16 a 35 años.

Como manifiesta la institución financiera, los ataques de ingeniería social no tienen por objetivo dañar computadores ni celulares sino más bien, su fin es obtener un lucro de sus víctimas mediante la manipulación psicológica. Por tal motivo, la medida de protección que toma Banco Pichincha (2020) es recomendar 10 pasos para evitar ataques de ingeniería social, mismos que son presentados en la Tabla 1.2 mostrada a continuación:

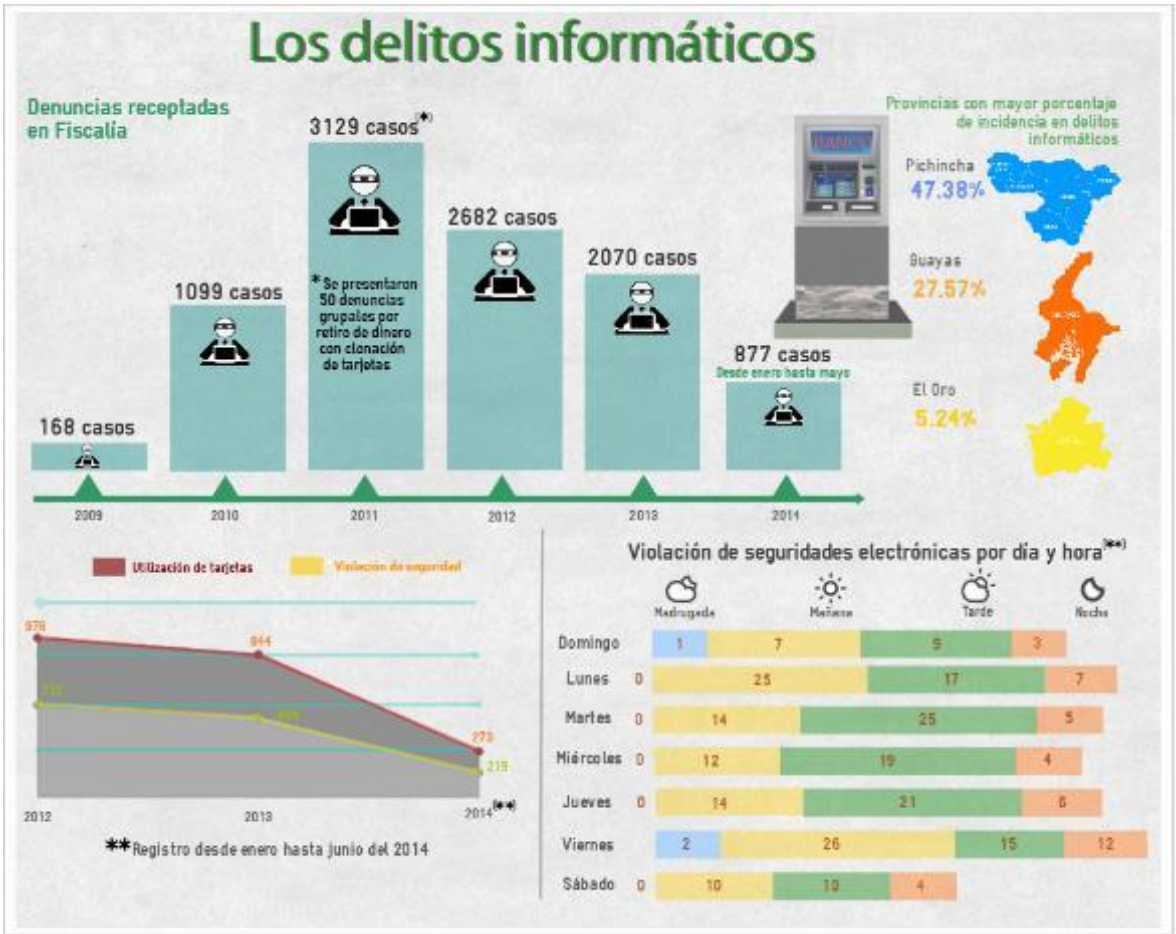
Tabla 1.2. Recomendaciones para evitar ataques de ingeniería social

Paso 1	Nunca entregar credenciales de acceso a plataformas.
Paso 2	No compartir información sensible en redes sociales.
Paso 3	Evitar abrir correos y archivos adjuntos de fuentes sospechosas. Si no se conoce al remitente, no responder el correo hasta verificar su autenticidad.
Paso 4	En caso de recibir correos con ofertas, regalos o beneficios tentadores, pensar dos veces antes de hacer *clic* y aceptarlos. Para verificar si son de verdad, basta con hacer una búsqueda rápida en *Google*.
Paso 5	Contactarse de forma directa con el remitente para obtener información sensible, para verificar su identidad.
Paso 6	Actualiza el *software* y antivirus del equipo de cómputo constantemente, para evitar archivos maliciosos.
Paso 7	Eliminar el historial y caché de la computadora para que no recuerde las credenciales de acceso a plataformas.
Paso 8	Seguir las políticas y consejos de seguridad de cada empresa.
Paso 9	Monitorear constantemente los perfiles sociales y cuentas bancarias para confirmar que todo está en orden.
Paso 10	Evitar conectarte a redes *wi-fi* públicas para navegar por internet.

Fuente: Banco Pichincha (2020, p.1)

Estas recomendaciones ayudan a disminuir la cantidad de fraudes financieros debido a que, en años pasados, estos delitos aumentaron de forma abrumadora, como es el caso del año 201, en el cual se dio un hecho inusual, se presentaron 50 denuncias grupales por retiro de dinero debido a una clonación de tarjetas. Por otra parte, cabe señalar que, son las ciudades grandes quienes tienen el mayor índice de ataques bancarios, según el reporte presentado por el Código Orgánico Integral Penal (COIP), que se muestra en la Figura 1.5:

Figura 1.5. Estadísticas de los fraudes bancarios en entidades financieras



Fuente: Fiscalía General del Estado (2014, p. 1)

Acorde al informe presentado por el COIP, las provincias de Pichincha y Guayas poseen la mayor cantidad de ataques y fraudes financieros, según el reporte presentado por la fiscalía Pichincha reporta un promedio entre 6 a 10 denuncias sobre delitos informáticos y fraudes financieros por semana. Además, el reporte de la Fiscalía General del Estado (FGE) sostiene que, este tipo de ilícitos se cometen a través de transferencias electrónicas, clonación de tarjetas o claves y al momento del realizar pagos en centros comerciales. Sin embargo, hay quienes sospechan que las transferencias ilícitas se realizan con información dentro de la misma institución financiera porque no emiten alertas a correos o su teléfono como se lo realiza en el caso de transferencias licitas (Fiscalía General del Estado, 2014, p. 1).

Cualquier tipo de fraude financiero compromete a la víctima debido a la pérdida económica y de alguna forma a la Institución Financiera debido a que, esta sin importar el método

utilizado para el fraude, pierde la garantía y la confianza de los clientes. Es por tal motivo que, siempre será un deber de cualquier entidad bancaria no escatimar esfuerzos con respecto a la generación de metodologías de prevención ante robos informáticos, dentro del Sistema de Gestión de Seguridad de la Información. Por otra parte, una de las estrategias más utilizadas y que no requiere la mayor cantidad de dinero para una empresa es el diseño de diversas guías de protección y para prevención, entre las más comunes se tiene:

- Creación de políticas.
- Planes de contingencia y respuesta a incidentes.
- Campañas de concientización y prevención ante delitos informáticos.
- Diseño de equipo de respuesta a incidentes por sus siglas (CSIRT)

Cada una de estas estrategias ha permitido a las instituciones disminuir el riesgo, sin embargo, no todas las entidades financieras poseen las mismas realidades, razón por la cual, el tratamiento, que se da a la información es diferente, en especial cuando se trata de la gestión documental. En el caso de las campañas de concientización y guías de prevención ante ataques permite a los usuarios conocer los riesgos a los que se enfrentan día a día, y conozcan cómo actuar en caso de ser víctima de un fraude bancario.

Por otra parte, esta técnica brinda una integración entre usuarios internos y externos de la organización, pues en ciertas ocasiones los ataques no se dan solo desde medios externos, sino también por desconocimiento de los colaboradores al compartir contraseñas, navegación en sitios indebidos o ingresar a las cuentas institucionales desde equipos públicos. Cabe señalar que “las organizaciones cambiarían en su cultura organizacional enfocada a la seguridad de la información y en los procesos de la compañía en donde todos los colaboradores se sientan incluidos y así generar un cambio y un apoyo y de esta manera mitigar el riesgo al que se encuentra expuesta la información” (Vargas, 2018, p. 12).

En un estudio denominado 'Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa' realizado por Vargas (2018) resalta la importancia de generar campañas y guías para la prevención de ataques informáticos, es por ello que, en el presente estudio consta el diseño de las guía para la prevención de ataques por ingeniería social, el cual está debidamente estructurado, en base a los usuarios y clientes de la entidad financiera donde se está implementado dicha guía, este procedimiento se detalla en el Capítulo II.

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y a la persona, que tenga equipos conectados a la *World Wide Web*. A diferencia de lo que sucedía años atrás, donde personas con amplias habilidades en el campo informático disfrutaban investigar estos aspectos con el ánimo de incorporar mayor conocimiento; en la actualidad se ha desvirtuado completamente, que origina nuevos personajes que utilizan los medios informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

Cada día se descubren nuevos puntos débiles, por lo general, son pocos los responsables de las Tecnologías de la Información (TI) que comprenden en su justa medida la importancia que tiene la seguridad y cómo abordaría el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados. Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos.

Pero para lograr mitigar de manera eficaz el impacto provocado por los ataques informáticos, es de capital importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotados en los, que se enfocaría los esfuerzos de seguridad tendientes a la prevención de los mismos. En consecuencia, el presente documento pretende ofrecer una rápida visión sobre las debilidades comúnmente explotadas por atacantes para traspasar los esquemas de seguridad en los sistemas informáticos, junto a posibles contramedidas bajo las cuales es posible ampararse para prevenir de manera efectiva los diferentes tipos de ataques que diariamente recibe un sistema.

CAPÍTULO II. DISEÑO METODOLÓGICO

El estudio de la presente investigación es de tipo cualitativo, con un diseño de corte mixto transversal, tiene un alcance descriptivo y el método utilizado es el inductivo-deductivo.

2.1. Caracterización de la institución

Mutualista Ambato (MA) es una institución financiera con años de prestigio en el país, cuya misión y visión son:

- **Misión**

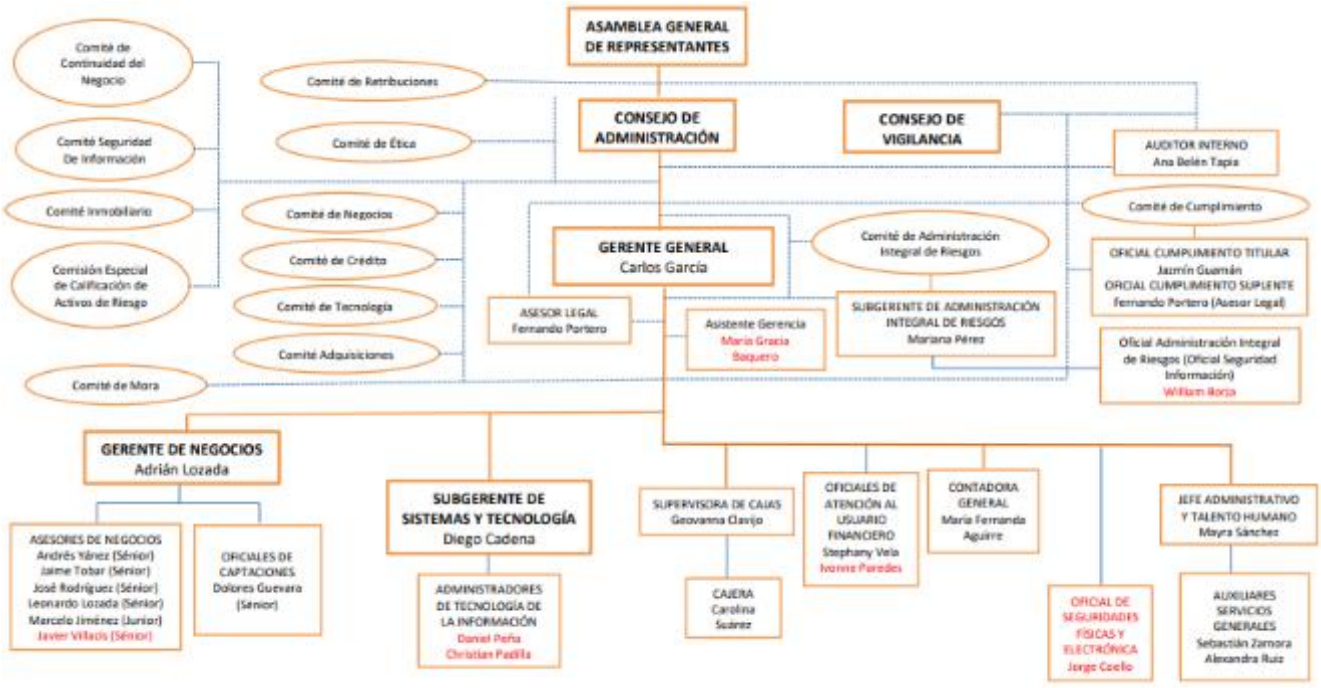
Somos una Institución Financiera orientada a crear valor a favor de nuestros socios y clientes, mediante modelos de negocios transparentes de calidad, con permanente innovación tecnológica, capital humano y gobierno corporativo comprometidos (Mutualista Ambato, 2016).

- **Visión**

Consolidar el posicionamiento de Mutualista Ambato en los próximos tres años, sobre la base de prácticas éticas, competitivas, rentables y tecnológicas (Mutualista Ambato, 2016).

La Institución está compuesta por más de 50 colaboradores en su matriz los cuales están estructurados acorde al organigrama elaborado por la Gerencia de Control de Gestión y aprobado por el Directorio en sesión ordinaria en el año 2016, la estructura organizacional se evidencia en la Figura 2.1 presentada a continuación:

Figura 2.1. Estructura Organizacional Mutualista Ambato



Fuente: Mutualista Ambato (2016)

De acuerdo al organigrama estructural evidenciado en la Figura 2.1 el departamento de Sistemas y Tecnologías, cuenta con personal especializado y dedicado al tratamiento de la seguridad, es así como de acuerdo al Manual De Seguridad de la Información de la Asociación Mutualista Ambato (2019) se tiene las principales funciones del área que son:

- **Art. 1.** Es responsabilidad del OSI recomendar la creación y / o actualización de las políticas de seguridad de la información, y el monitorear del cumplimiento de los controles establecidos.
- **Art. 2.** Analizar Políticas y Procedimientos relacionados con la seguridad de la Información aplicables a las distintas Áreas y Unidades de la Institución.
- **Art. 3.** Identificar amenazas y vulnerabilidades tecnológicas para mitigar los riesgos que afectarían los servicios que brinda la Institución al aplicar la metodología de Gestión de Riesgo Operativo.
- **Art. 4.** Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomado en cuenta las políticas de control de acceso aplicables.
- **Art. 5.** Difusión y capacitación al personal de la Institución de políticas, estrategias y procedimientos establecidos en el presente manual.

- **Art. 6.** Analizar posibles escenarios de riesgos, que se den en la Institución conjuntamente con el Área de Sistemas para determinar las estrategias necesarias para asegurar la Continuidad del Negocio.
- **Art. 7.** Proponer al Comité de seguridades de la Información el inventario, clasificación y asignación de responsables de la información.
- **Art. 8.** Informar al Comité de Seguridad de la Información en forma bimensual las actividades relacionadas con la seguridad de la información.

2.2. Argumentación metodológica de la investigación

La investigación busca diseñar una guía de campañas de ingeniería social al interior de una institución financiera, con la finalidad de proteger la información de los usuarios de dicha entidad. A continuación, se detalla la metodología de investigación usada en el estudio:

2.2.1. Modalidad de la investigación

El estudio es de tipo cualitativo, mismo que, permite comprender la complejidad del hecho o fenómeno de estudio desde el punto de vista de quienes son partícipes de aquel contexto. Desde la perspectiva de, Abreu (2014) “los métodos cualitativos continuarán buscaran descubrir nuevos conceptos que no son evidentes, al mismo tiempo, presentan una oportunidad para presenciar nuevas perspectivas para aquellas situaciones en las que ciertas señales ocultas revelan un mayor conocimiento del fenómeno de investigación” (p. 197). Es decir, este método se centra en el interior del hecho o fenómeno de estudio cuyo proceso de indagación es inductivo.

Bajo esta perspectiva, en el estudio la metodología cualitativa ayuda al investigador a interactuar con la información o los datos recopilados, de las metodologías para campañas de ingeniería social en instituciones financieras, para buscar dar respuesta a las interrogantes que se presente, tras el desarrollo del diseño de la campaña y la interacción con los usuarios.

El diseño de la investigación es de corte mixto transversal , la recopilación de los datos se realiza en un instante único y una sola vez, no se repetirá. Al respecto Hernández, Fernández y Baptista (2010) indican que en la investigación transversal se “recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado. Es como tomar una fotografía de algo que sucede” (p.

151). Es así que, en la investigación que preside, con el uso de este método, se acopian los datos e información de las guías para campañas de ingeniería social al interior de una institución financiera, en un momento determinado y una vez.

Por otro lado, las investigaciones mixtas "permiten la obtención de una mejor evidencia y comprensión de los fenómenos y, por ello, facilitan el fortalecimiento de los conocimientos teóricos y prácticos" (Pereira, 2011, p. 19). Esta metodología se robustece al incorporar en ella información como narrativas de los participantes e imágenes para darle mayor comprensión a los datos numéricos, que se hallan. Dentro del presente estudio la investigación admite recolectar, analizar e interpretar las guías para campañas de ingeniería social al interior de una institución financiera.

2.2.2. Método

El método utilizado en la investigación es inductivo- deductivo, y se detalla en la siguiente sección:

- **Método Inductivo:** Es uno de los métodos que caracterizan a una investigación que busca llegar de indicios particulares a generales. Al respecto Andrade, Alejo y Armendariz (2018) indican que este método, es conocido por los "procedimientos utilizados para llegar de lo particular a conclusiones generales a base de la información de la muestra. Es decir que, a partir de los resultados de una investigación realizada con una muestra… se infiere sobre las características poblacionales" (p. 118). Por lo tanto, a través de este método, la investigación parte de la observación particular de ciertos aspectos de las guías de campañas de ingeniería social para llegar características universales de las mimas.

  El método inductivo, permitirá dilucidar de forma individual las diversas guías en campañas de ingeniería social aplicadas a las diferentes instituciones financieras, ,, el inductivismo "se desarrolla con base en hechos o prácticas particulares, para llegar a organizar fundamentos teóricos" (Abreu, 2014). De tal forma que, de cada una de las guías, se logre establecer cuál es, la que mejor se ajusta para dichas instituciones.

Es necesario el uso del método inductivo, mediante un análisis del diagnóstico situacional en la entidad financiera Mutualista Ambato y mediante el uso del instrumento como es la encuesta, aplicada a los directivos de Mutualista Ambato, permitirá conocer las

vulnerabilidades acerca del tratamiento de la información digital sensible dentro de la institución, y a través de este medio se logre obtener el diagnóstico situacional de la problemática existente.

Por otro lado, otro método utilizado es el deductivo, mismo que se explica a continuación:

- **Método Deductivo**: Esta metodología permite al investigador inferir sobre el hecho o fenómeno observado a partir de una característica general. Específicamente "el método deductivo basa sus cimientos en determinados fundamentos teóricos, hasta llegar a configurar hechos o prácticas particulares" (Prieto, 2017, p.11). Por ello, este método ayuda a que, por medio de la información recopilada acerca de las guías para campañas de ingeniería social en instituciones financieras se llegaría a conclusiones contundentes.

  Dicho de otro modo, el deductivismo, admite comprender que, las guías utilizadas en campañas de ingeniería social son eficaces dentro de instituciones financieras, tras conocer la forma en cómo funcionan. A través de este método se evidencia la necesidad de la implementación de una guía para campañas de prevención ante ataques de ingeniería social, gracias a los resultados obtenidos en la entrevista.

2.3. Metodología de desarrollo

Para el desarrollo de la guía se hace uso de la metodología de Kanban, la cual permite perfeccionar la productividad dentro de cualquier institución, sin diferenciar que se dedica; la técnica está centralizada en organizar y distribuir las tareas de manera flexible, a fin de que, la persona no tenga tareas acumuladas, incompletas y atrasadas. Consta de un tablero con tres etapas: pendiente, en proceso, terminado, y en cada una de ellas se asigna las tareas acordes a las necesidades de la investigación.

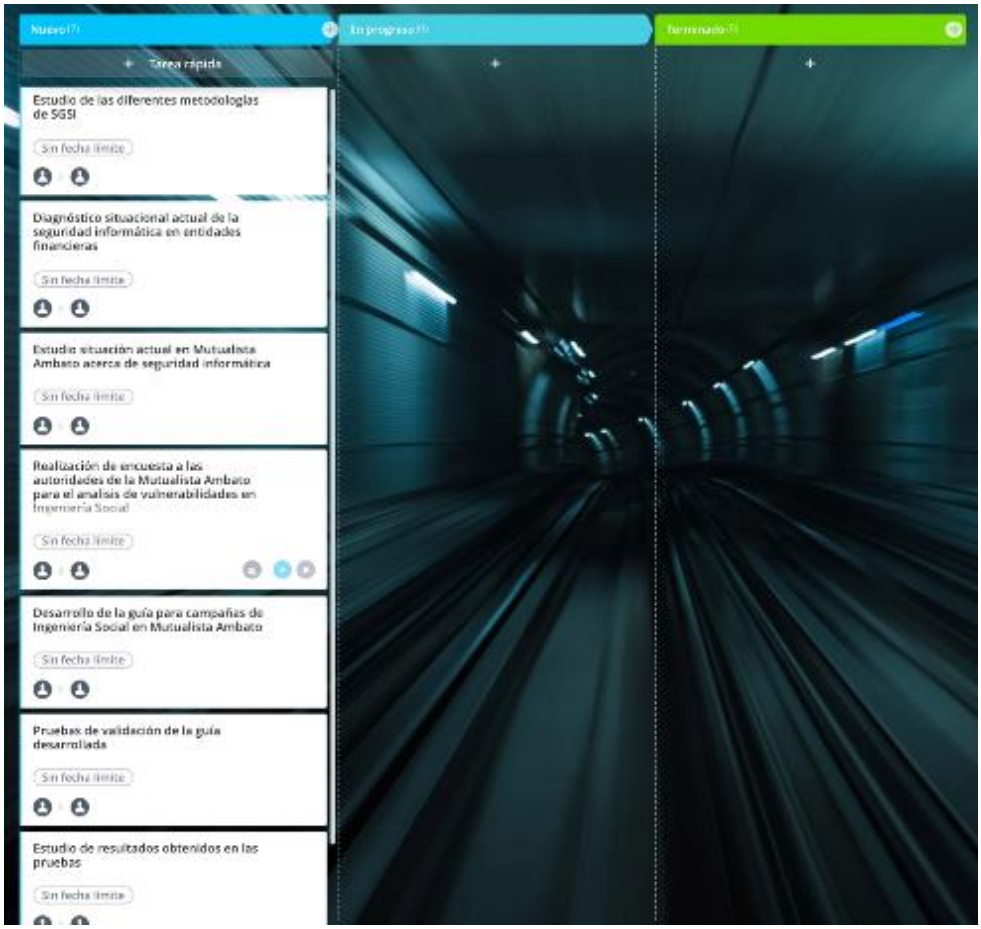
Kanbanize (2021) manifiesta que, la metodología Kanban está basada en 4 principios fundamentales para su correcta implementación, estos son:

- **Principio 1:** Empezar con lo que hace ahora.
- **Principio 2:** Comprometerse a buscar e implementar cambios incrementales y evolutivos.
- **Principio 3:** Respetar los procesos, las responsabilidades y los cargos actuales.

- **Principio 4:** Animar el liderazgo en todos los niveles.

En base a los principios establecidos, esta metodología permite una gestión en el flujo de trabajo y de esta forma brindar una mejora continua dentro del proceso, no requiere de una configuración específica y se aplicaría en diversos flujos de trabajo, los cambios son mínimos y de forma secuencial. Para el desarrollo de la presente investigación se ha desarrollado el tablero de Kanban acorde a los pasos planteados en la Tabla 2.1

Tabla 2. 1. Planificación Kanban



Fuente: elaboración propia

2.3.1. Estudio de las diferentes metodologías del SGSI

De acuerdo con la investigación realizada en el estado de arte, se entiende que, un sistema de gestión de la información es el compuesto de políticas establecidas dentro de una organización para el manejo de la información digital sensible, con el fin de mantener

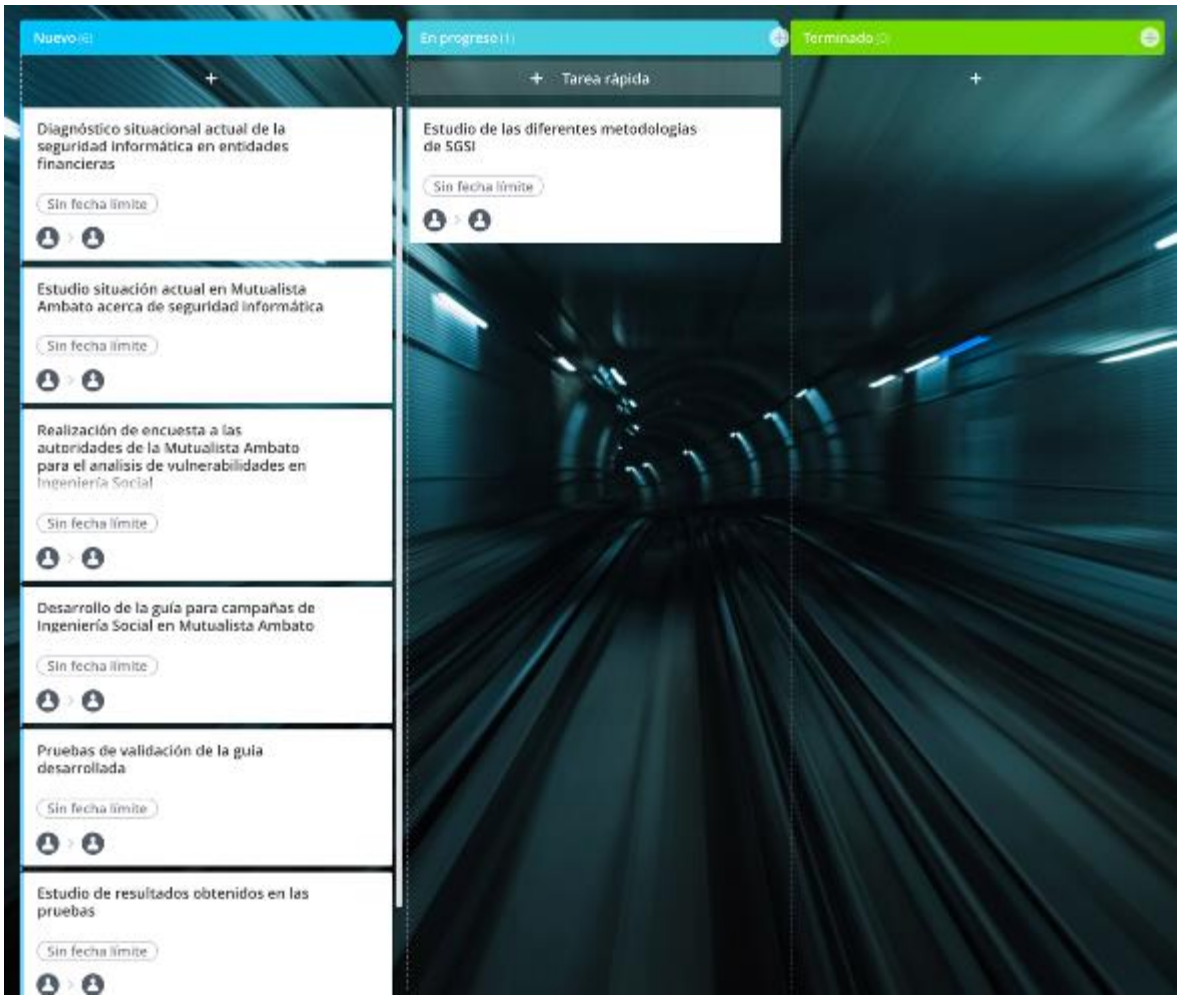
seguros los datos a nivel interno y externo de la organización, un SGSI por lo general se encuentra regido por el estándar ISO 27000 y entre las diferentes metodologías se tiene:

- OCTAVE
- MEHARI
- CRAMM
- MAGERIT
- EBIOS
- NIST SP 800:30

El estudio de las diferentes metodologías en un SGSI se encuentran previamente documentadas en el Capítulo I de la investigación, la importancia de este estudio se basa en la necesidad de conocer las diferentes técnicas utilizadas para la protección de la información digital sensible de la organización, una vez conocido como funciona el SGSI, se entiende a la gestión documental como parte importante dentro del sistema, es por eso que, como paso posterior se procede a realizar el análisis de la seguridad informática en entidades financieras.

Acorde al principio de Kanban los procesos serian realizados uno a uno y en manera secuencial. En base a este contexto, el análisis del SGSI dentro de la Institución resalta la importancia de elaborar la guía dentro del análisis de documentación y mejora de procesos de seguridad informática a nivel interno de la organización. El proceso metodológico se evidencia en la Tabla 2.2. presentada a continuación:

Tabla 2.2. Fase 1 en proceso, estudio de las diferentes metodologías SGSI



Fuente: elaboración propia.

2.3.2. Diagnóstico situacional actual de la SI en entidades financieras

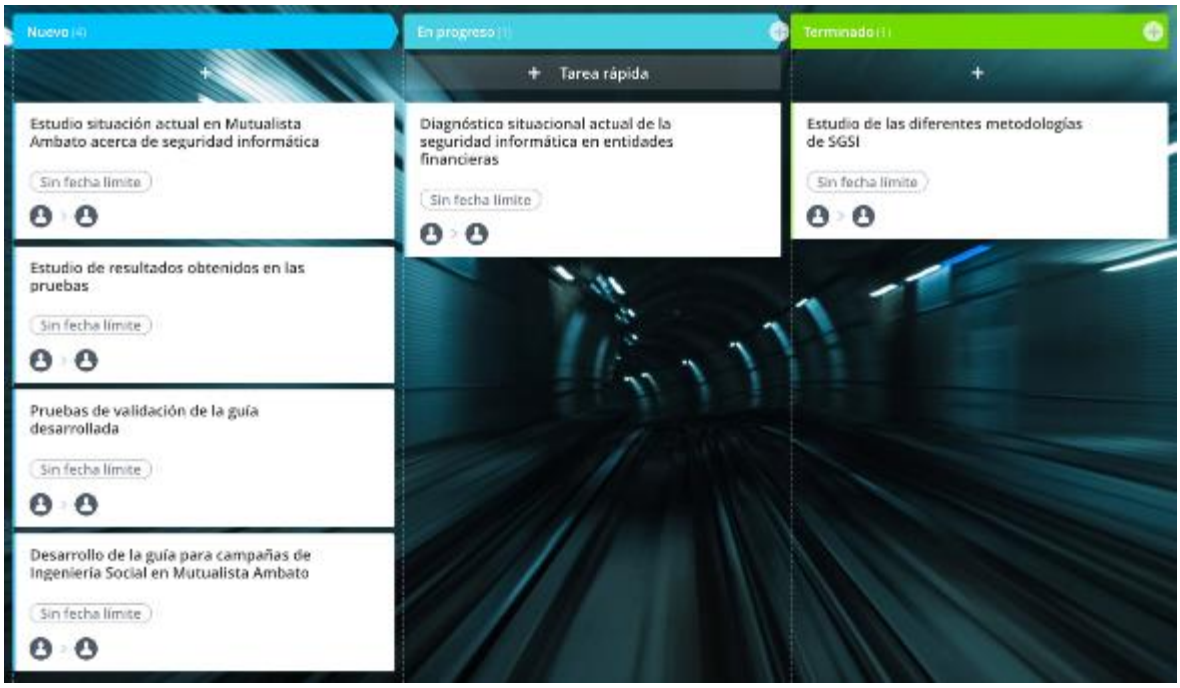
El estudio del diagnóstico situacional del trato de la información digital sensible dentro de las entidades financieras permite obtener una visión general acerca del trato a la seguridad de la información dentro de la organización, así como también, fraudes bancarios más comunes y de los cuales son víctimas los usuarios, entre los cuales se tiene:

- La clonación de tarjetas de crédito.
- Suplantación de identidad.
- Robo de credenciales.

Acorde al análisis del diagnóstico situacional dentro de las entidades financieras realizado en el Capítulo I de la presente investigación, permite analizar los diferentes métodos de

protección planteados por las organizaciones, el proceso debidamente documentado en Kanban, se muestra en el proceso dentro de la Tabla 2.3:

Tabla 2. 3. Fase 2 en proceso, diagnóstico situacional en entidades financieras



Fuente: elaboración propia

Gracias al estudio realizado en las entidades financieras se permite conocer a la gestión de los SGSI a nivel interno de la institución. Es decir, se conocerían diferentes técnicas utilizadas por organizaciones financieras para proteger la información digital sensible, y de esta forma aplicar métodos y técnicas al interior de Mutualista Ambato. Para conocer el estado actual de la organización se ha procedido con la Fase 3.

2.3.3. Análisis del diagnóstico situacional de la Institución Financiera

Para la presente investigación se usa como técnica la observación cualitativa y como instrumento la encuesta.

Técnica

- **La observación cualitativa:** Este tipo de observación es un procedimiento semiestructurado donde se captan datos generales sobre el comportamiento de la unidad de población escogida para aplicar la técnica con el objetivo de ejecutar análisis sobre la información que resulte del estudio. Desde la perceptiva de Urbano (2016) es una técnica donde el observador describe los sucesos exactos que surgen en el momento de aplicar la técnica… En este caso el observador incluye datos de la forma cómo él los interpretó en el transcurso de la aplicación de los instrumentos o en la aplicación del método (p. 117).

  Dentro de la investigación esta técnica admite mostrar la necesidad de un diseño de una guía para campañas de ingeniería social al interior de la institución financiera Mutualista Ambato

Instrumento

- **Encuesta:** Este instrumento es utilizado para extraer información significativa para la investigación y es que**,** constituye una forma concreta de la técnica de observación, esto permite al investigador fijar su atención en ciertos aspectos y se sujeten a determinadas condiciones… Contiene los aspectos del fenómeno que se consideran esenciales; permite, además, aislar ciertos problemas que interesan principalmente; reduce la realidad a cierto número de datos esenciales y precisa el objeto de estudio (Gómez, 2012, p. 58).

Mediante este instrumento se extraerá información valiosa de la situación actual, en cuanto a las vulnerabilidades acerca del tratamiento de los datos sensibles dentro de la entidad financiera Mutualista Ambato.

Alcance

La presente investigación al ser de tipo descriptivo detalla los aspectos más relevantes del tratamiento de la información digital sensible dentro de la Institución Financiera a evaluar. Según Abreu (2014) la metodología descriptiva, busca un conocimiento inicial de la realidad que se produce de la observación directa del investigador y del conocimiento que se obtiene mediante la lectura o estudio de las informaciones aportadas por otros autores. Se refiere a

un método cuyo objetivo es exponer con el mayor rigor metodológico, información significativa sobre la realidad en estudio con los criterios establecidos por la academia (p. 198).

En resumen, el alcance descriptivo permite obtener la información referente a una guía para campañas de ingeniería social al interior de una institución financiera, para ello se seguirá los objetivos del estudio, además, tiene por objetivo comprender las vulnerabilidades ante amenazas de ataques de ingeniera social, para lo cual se hace uso de la técnica de la entrevista, orientada a los directivos de la institución

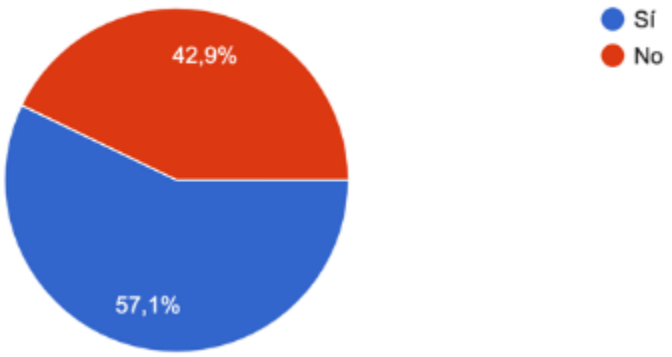
El proyecto de investigación es un estudio de tipo descriptivo, mismo que se encarga de detallar los aspectos más relevantes de la población participante del mismo. Los estudios descriptivos “son particularmente útiles cuando un investigador se inicia en un tema nuevo. En este caso, comenzaría a recabar datos vinculados al problema o tema que recortó, sistematizarlos y exponerlos, sin pretender establecer relaciones de causalidad entre variables (Echeverría, 2016, p. 111). Es decir, la investigación se concentra en los 'qué', en vez de los 'por qué', describe un segmento de población, y descarta razones por la que se da u hecho o fenómeno.

Participantes

La encuesta está dirigida a las autoridades de la Mutualista Ambato (Gerente y Subgerentes), esto por la importancia de la información que ellos manejan y gestionan, así como también son los encargados en conjunto con el departamento de Sistemas y Tecnologías proveer los métodos de protección de los datos, esto permite obtener el diagnostico situacional de la empresa, lo cual pone en evidencia la importancia de la implementación de la guía dentro de la organización, la encuesta consta de 9 preguntas de aspecto técnico-administrativo y se detallan a continuación:

Figura 2.2. Ingeniería social

Pregunta 1: ¿Conoce usted lo que es Ingeniería Social?



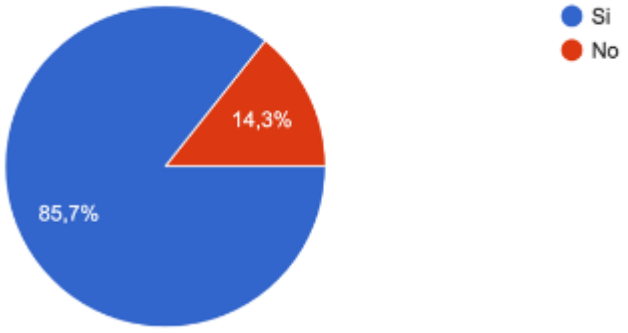
Fuente: elaboración propia

Análisis e interpretación:

Como se muestra en la Figura 2.2 de acuerdo con la pregunta realizada se evidencia que, alrededor del 50% de personas encuestadas no conocen acerca de la temática de ataques generados por ingeniería social, esto pone en evidencia una vulnerabilidad dentro de la Institución financiera por desconocimiento, y se considera una amenaza dentro del SGSI, por otra parte si bien más del 50% de los encuestados conocen el concepto de ingeniería social no saben cómo actuar ante un ataque de este tipo lo que genera una amenaza igual.

Figura 2.3. Revisión de antecedentes

Pregunta 2: ¿Revisa los antecedentes de las personas que van a trabajar con usted?



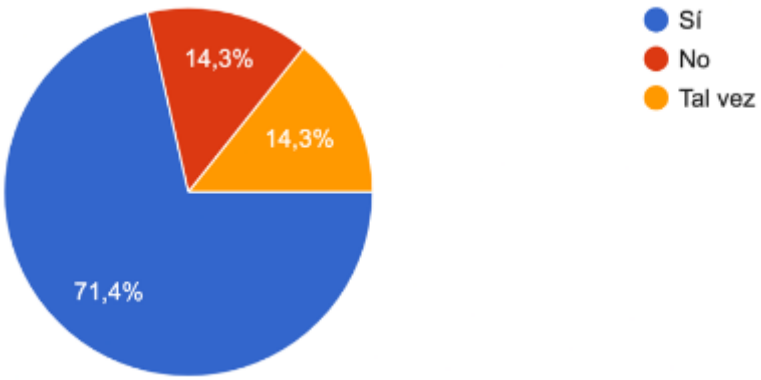
Fuente: elaboración propia

Análisis e interpretación:

De acuerdo a los resultados mostrados en la Figura 2.3 se evidencia que alrededor del 87%, de las autoridades, si hacen un seguimiento acerca de los antecedentes que tienen los aspirantes para ingresar a laborar en la institución, este seguimiento es muy importante debido al manejo de información sensible y confidencial que manejan en cada área y dependen de las funciones que le son encargadas a cada colaborador, sin embargo dentro de la Institución no se evidencia una alta amenaza gracias al seguimiento que realizan los Directores a su personal.

Figura 2.4. Seguridad de la organización

Pregunta 3: ¿La gente de seguridad de tu empresa tiene acceso a información de la infraestructura de la misma?



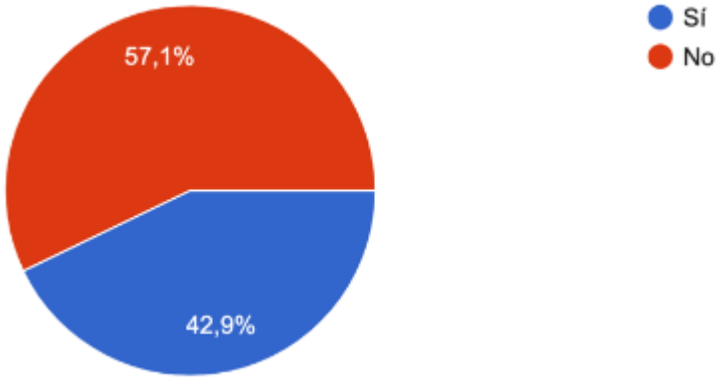
Fuente: elaboración propia

Análisis e interpretación:

De acuerdo a los resultados mostrados en la Figura 2.4 muestra que gran parte del personal posee acceso a la información de la infraestructura tecnológica de la institución, esto pone en evidencia un riesgo ante un ataque, no solo de ingeniería social, debido a la falta de control de acceso y permisos a la infraestructura, es decir no se tiene bien definido el acceso a la información sensible de la empresa, lo que genera una amenaza dentro del SGSI.

Figura 2.5. Capacitaciones en seguridad informática

Pregunta 4: ¿Es pro-activo en cuanto la capacitación de su personal sobre temas de seguridad de información?



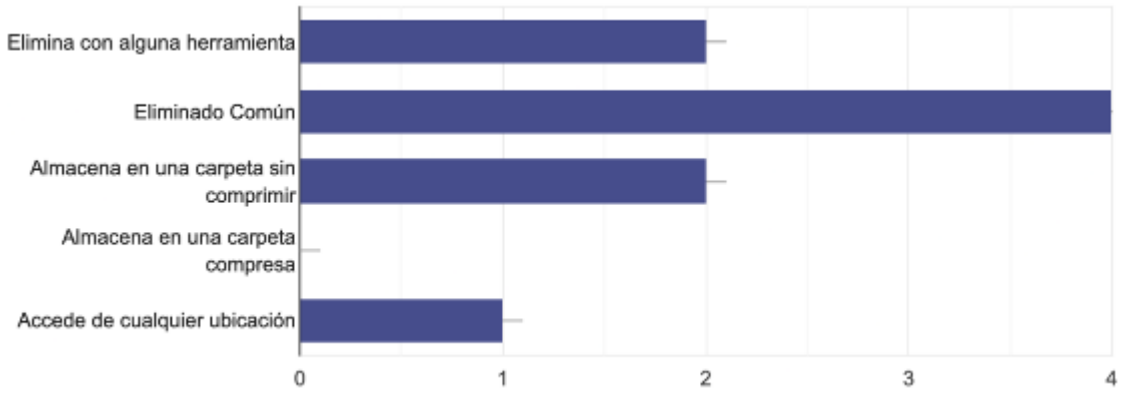
Fuente: elaboración propia

Análisis e interpretación:

De acuerdo a la Figura 2.5 el personal no posee un adecuado conocimiento acerca de los temas de seguridad de la información, esto muestra el riesgo que tiene la entidad ante ataques informáticos, por desconocimiento de este peligro, además se manifiesta un desinterés en temas de este índole, dicho de otro modo, la mayor parte del personal no sabrían cómo actuar ante un ataque informático.

Figura 2.6. Gestión de contraseñas

Pregunta 5: ¿De qué manera elimina o almacena un correo electrónico que contiene información confidencial?



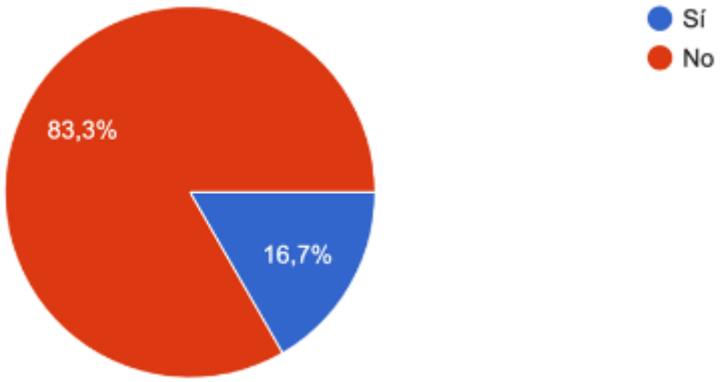
Fuente: elaboración propia

Análisis e interpretación:

En la Figura 2.6 se evidencia el riesgo de la mala eliminación de archivos por parte del personal, al considerar que no existe una concientización acerca de la información que se desecha esto genera una amenaza latente ante un ataque de ingeniería social debido a que inconscientemente se eliminaría información sensible caería en manos de algún atacante.

Figura 2.7. Ataques de ingeniería social

Pregunta 6: ¿Ha detectado usted ataques de ingeniería social dentro de su empresa?



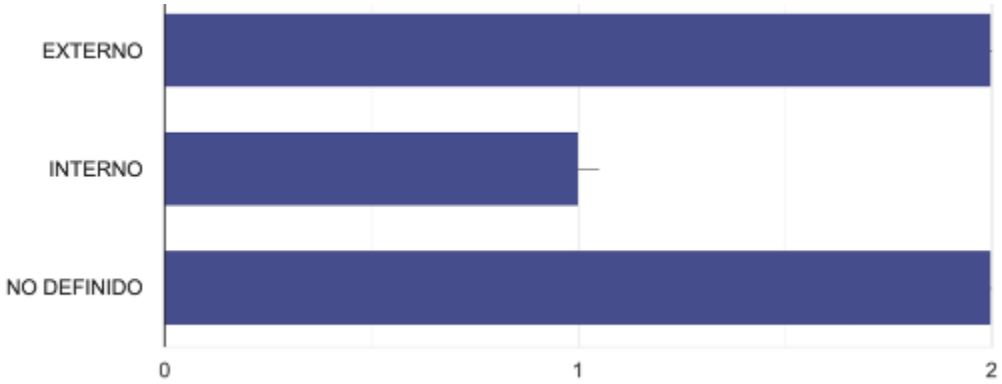
Fuente: elaboración propia

Análisis e interpretación:

En la Figura 2.7 se evidencia que existe un riesgo de ataques realizado por ingeniería social, este porcentaje a pesar de ser mínimo no deja de lado el hecho de que, ha existido ataques de este tipo dentro de la entidad financiera, además por otra parte y de acuerdo con la pregunta 1 de la encuesta existe un desconocimiento acerca de este tema es decir este valor no es del todo exacto pues no todo el personal conoce la temática propuesta.

Figura 2.8. Ataques internos y externos

Pregunta 7: ¿Se ha respondido si a la anterior pregunta, estos ataques fueron internos o externos?



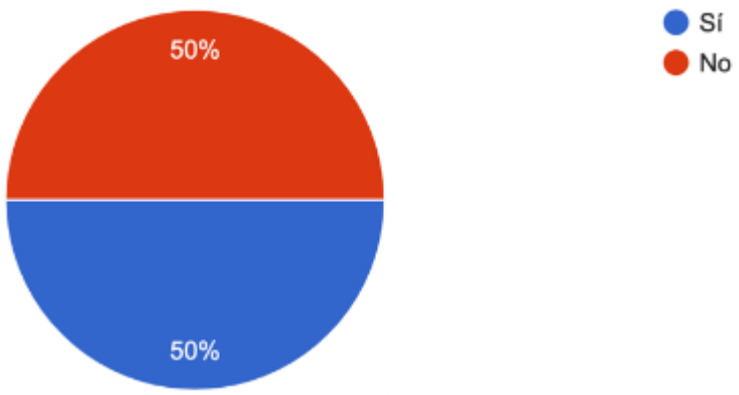
Fuente: elaboración propia

Análisis e interpretación:

En la Figura 2.8 se evidencia un desconocimiento de como son los vectores de ataques de ingeniería social, gran parte del personal no tiene un concepto definido acerca de cuál es el vector de ataque en este tipo de temas, es importante resaltar la importancia de conocer este tipo de vectores, a fin de generar una concientización y conocimiento acerca de esta problemática, por otra parte se evidencia la importancia de generar métodos de respuesta ante este tipo de ataques, y de esta forma mitigar en su mayor parte esta amenaza dentro de la Institución.

Figura 2.9. Acciones de seguridad

Pregunta 8: ¿Se realizaron acciones de seguridad para evitar ser víctimas de un nuevo ataque de ingeniería social dentro del área de sistemas?



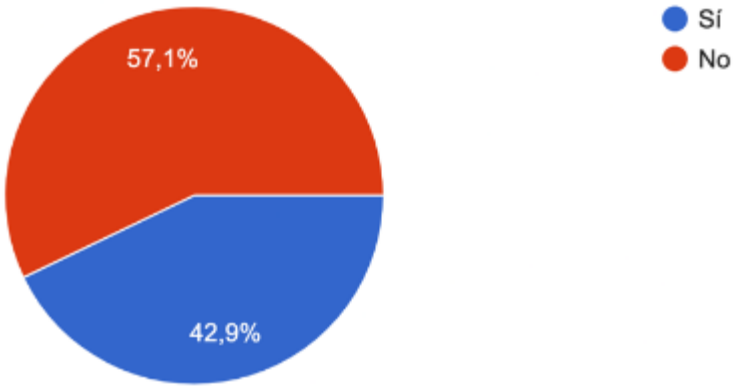
Fuente: elaboración propia

Análisis e interpretación:

En la Figura 2.9 se muestra como el personal dentro de la entidad financiera no tiene un conocimiento adecuado del tratamiento de prevención de fuga de información dentro de la institución, y tampoco saben cómo reaccionar ante un ataque informático, de este modo se evidencia la necesidad de mejora del SGSI a través de métodos y estrategias como la gestión documental planes de contingencia políticas y guías de ciberseguridad.

Figura 2.10. Capacitación ataques en ingeniería social

Pregunta 9: ¿Se capacita constantemente al personal de sistemas sobre ataques de ingeniería social?



Fuente: elaboración propia

Análisis e interpretación:

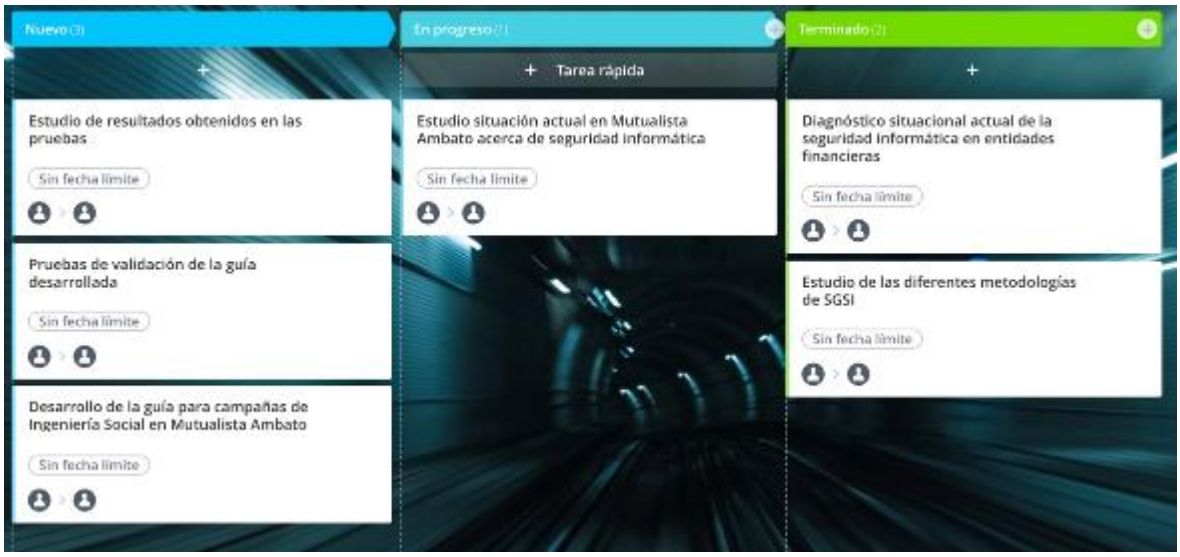
En la Figura 2.10 se muestra la necesidad de realizar capacitaciones de manera frecuente al personal involucrado acerca de la temática de fraudes financieros por ingeniería social, a fin que estos posean el conocimiento necesario para una respuesta a incidentes dentro de la Institución, se considerar también que el personal de sistemas es la primera línea de protección ante ataques y delitos informáticos razón por la cual estaría en constante preparación.

Interpretación Global de resultados

De acuerdo a los resultados obtenidos en la encuesta se evidencia ciertos aspectos importantes como: existe un desconocimiento de casi el 40% de las personas encuestadas acerca de los ataques de ingeniería social, es decir 4 de cada 9 personas desconocen esta temática, razón por la cual les hace vulnerables ante un incidente de este tipo. También se apreciaria como una pequeña cantidad de usuarios manifiestan que ha existido algún tipo de ataque de ingeniería social a nivel interno, sin embargo, desde un aspecto positivo se muestra como las autoridades mantienen un interés latente en mejorar la seguridad informática. Esto permite a la empresa y al personal de Sistemas y Tecnologías generar nuevas estrategias para la protección de los datos, y resalta la importancia del desarrollo de la guía en el estudio planteado.

Para el diagnóstico de la gestión de seguridad de la información en Mutualista Ambato se procede con la Fase 3 como se evidencia en la Tabla 2.4.

Tabla 2.4. Fase 3 en proceso, estudio situación actual Mutualista Ambato



Fuente: elaboración propia

2.3.4. Desarrollo de la guía para campañas de Ingeniería social en Mutualista Ambato

Una vez realizado el análisis interno de Mutualista Ambato mediante la entrevista, se entiende la necesidad de la implementación de la guía que, ayude a prevenir ataques de ingeniería social y de esta forma disminuir amenazas a nivel interno de la organización.

La guía está basada en la Norma ISO27000 la cual menciona a la gestión documental como parte importante dentro de un SGSI, y a vez, esta se complementa con la Metodología Magerit 3.0 para el desarrollo estructural de una guía. El diseño de la guía se evidencia en la Figura 2.11:

Figura 2.11: Guía para campañas de ingeniería social

Fuente: elaboración propia

Las Autoridades de la entidad financiera Mutualista Ambato en conjunto con el Departamento de Sistemas y Tecnologías, mantienen un esfuerzo constante por conservar la confidencialidad, integridad y disponibilidad de la información digital de la Institución. Todo ello con el fin de, garantizar un óptimo servicio para sus clientes, y de esta forma, mantener la continuidad del negocio seguro, ante las amenazas internas o externas que se presentaria, en este ámbito y como parte de un plan de mejora dentro del departamento se ha propuesto la elaboración de una guía para campañas de Ingeniería Social, la cual esta centrada en:

- ***ISO 27000:*** Normativa para la implementación de un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
- ***MAGERIT v3:*** Normativa centrada en la elaboración de guías para la protección de información digital.

El diseño de la guía está formado por los siguientes contenidos:

- Introducción
- Objetivo
- Alcance
- Materiales
- Dirigido a
- Elaboración
    - Pretexting (Pretexto)
    - Dumpster diving (Buceo en la basura)
    - Shoulder surfing
    - Baiting
    - Phishing
    - Smishing
    - Vishing
    - Sextorsion
- Recomendaciones

La presente guía tiene por alcance, enseñar a todos los usuarios internos dentro de Mutualista Ambato métodos de protección de la información sensible ante ataques por ingeniería social, a fin de que, estos posean un conocimiento amplio acerca de las diversas técnicas de ataques por dicho método. De esta forma, sepan utilizar diversas sistemáticas de prevención de modo que, la Organización no se vea vulnerada en uno de los activos más importantes que posee, la cual es, la información digital sensible.

La presente guía está dirigida a, todos los usuarios internos de la organización, misma que se basa en tres aspectos fundamentales: prevención, protección, y seguridad de la información, de esta forma, se busca que, cada usuario sin importar su cargo sepa la importancia de los datos confidenciales sensibles que maneja la Mutualista Ambato, el proceso en KANBAN se evidencia en la Tabla 2.5.

Tabla 2.5. Fase 4 en proceso, desarrollo de la guía

Fuente: elaboración propia

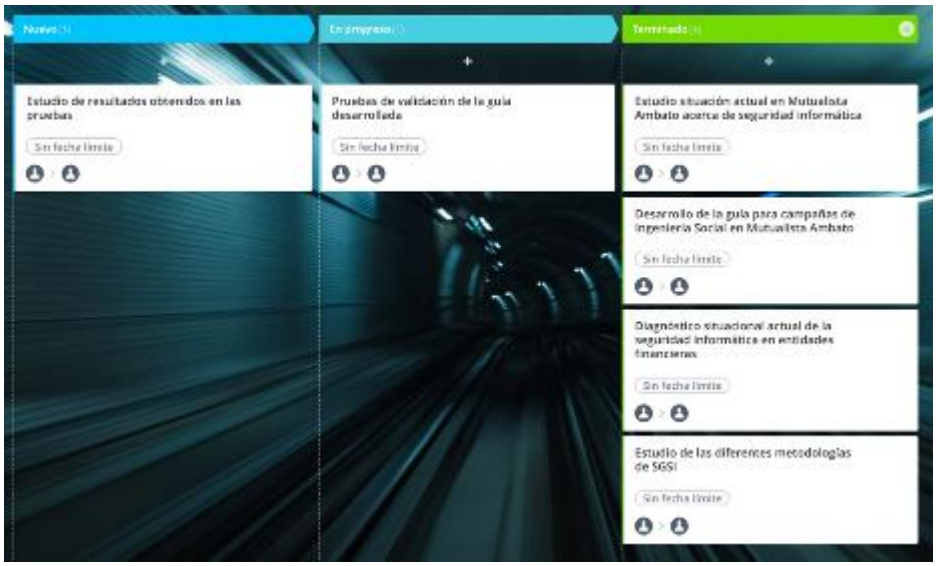
2.3.5. Pruebas de validación de la guía desarrollada

Es importante realizar la validación conocimientos impartidos en la guía, a fin de analizar el impacto generado en los usuarios de la organización, es importante resaltar que, la presente guía está alineada a las recomendaciones planteadas por el Instituto Nacional de Ciberseguridad (INCIBE), y para la validación se hace uso de la prueba desarrollado por el Ing. Darwin Naranjo creado en el año 2019.

Para esta validación de resultados se realizó una encuesta dentro de la institución financiera con los empleados, la misma que se basó en los conocimientos de la guía diseñada con varios ataques comunes en estas redes empresariales. Estos datos serán encontrados en el capítulo 3.

La guía comprende ciertos ítems los cuales serían evaluados para analizar su efectividad, estos ítems son valorados acorde a los requerimientos planteados por Magerit en conjunto con las recomendaciones establecidas por el Instituto Nacional de Ciberseguridad (INCIBE) ante la minimización de estos riesgos por ataques de ingeniería social, una vez realizadas estas pruebas esta fase se evidencia en la Tabla 2.6.

Tabla 2.6. Fase 5 en proceso, pruebas de validación

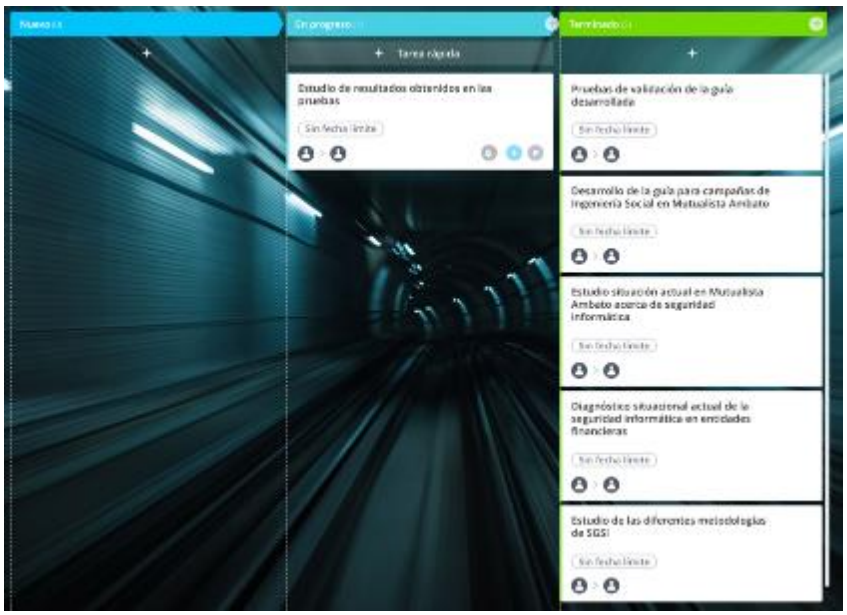


Fuente: elaboración propia

2.3.6. Estudio de resultados obtenidos en las pruebas

Es importante realizar un estudio de las pruebas de la guía, con el fin de determinar el impacto generado por la guía dentro de la institución, para realizar este análisis se procede con la fase final dentro de la metodología de *Kanban* como se evidencia en la Tabla 2.7 y el análisis de los resultados se detalla en el Capítulo III de la presente investigación.

Tabla 2.7. Fase 6 en proceso, estudio de resultados obtenidos en las pruebas



Fuente: elaboración propia.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Al concluir el desarrollo de la guía para campañas de prevención contra ataques de ingeniería social dentro de Mutualista Ambato, en concordancia con el proceso metodológico planteado en Kanban se procede a la evaluación, validación del mismo y de esta forma obtener los resultados para la investigación. Cabe señalar que, la guía desarrollada se encuentra estructurada de acuerdo con los lineamientos planteados por la Oficina de Seguridad Internauta (OSI) en conjunto con INCIBE y su boletín presentado en el año 2020, el cual se aprecia en la Figura 3.1 a continuación:

Figura 3.1. Guía de prevención INCIBE

Fuente: OSI (2020, p. 1)

La guía desarrollada, contiene las técnicas más utilizadas en ataques de ingeniería social, de acuerdo con los requerimientos sugeridos por OSI, en cada tipo vector de ataque desarrollado en la guía se presenta tres aspectos esenciales:

1) **Concepto del ataque:** A fin de que, el usuario final entienda la conceptualización de los tipos de ataques, además de explicar cómo funcionan cada uno de ellos, y generar conocimiento en el personal de la institución.
2) **Consecuencias:** Esto permite al usuario final, entender lo que pasaría si es víctima de ataques por ingeniería social. Por otra parte, la persona tomará conciencia de la importancia del manejo de su información personal.

3) **Métodos de prevención:** Es la parte final de la guía y busca que el usuario final sepa cómo protegerse ante este tipo de ataques y de esta forma, no sea víctima de los ciberdelincuentes.

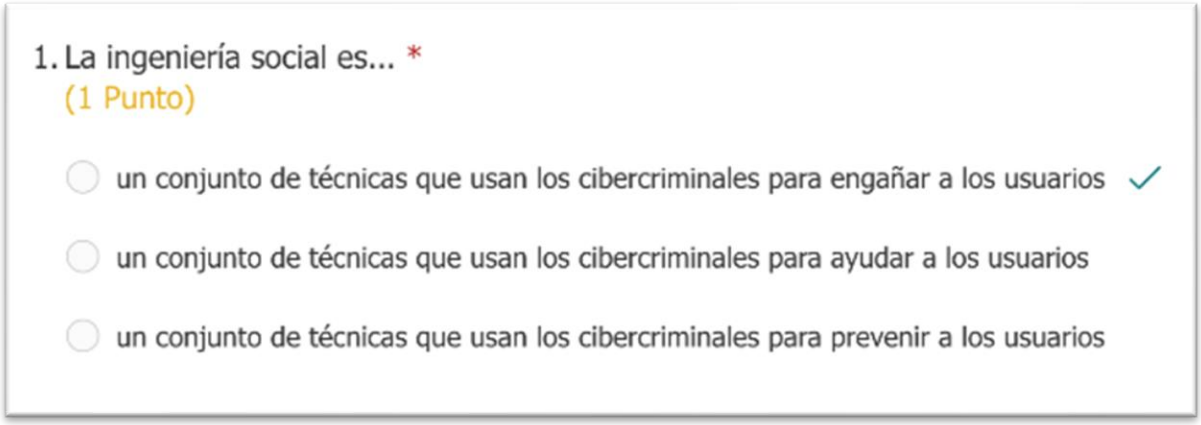
3.1. Evaluación de la guía

Para la validación de la guía y con el objetivo de medir el impacto generado dentro de la institución financiera, se procedió con la realización de un cuestionario para evaluar los conocimientos del personal antes y después del desarrollo de la guía. Este cuestionario consta de 11 preguntas mismas que se detallan a continuación:

Pregunta 1: Concepto de ingeniería social

La pregunta 1 está orientada a evaluar el conocimiento acerca del concepto general de ingeniería social, la interrogante y su respuesta se aprecia en la Figura 3.2 presentada a continuación:

Figura 3.2. Pregunta 1 Cuestionario de evaluación

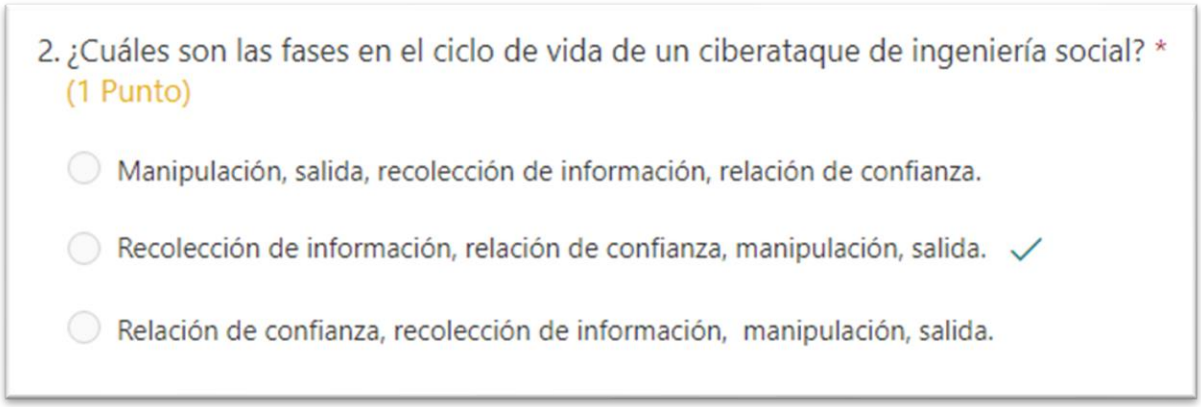


Fuente: elaboración propia.

Pregunta 2: Fases del ciclo de vida de un ciberataque

La pregunta 2 tiene por objetivo señalar si los usuarios finales poseen un conocimiento acerca del proceso que se realiza en un ataque de ingeniería social, la pregunta y su respuesta se evidencia en la Figura 3.3.

Figura 3.3. Pregunta 2 Cuestionario de evaluación

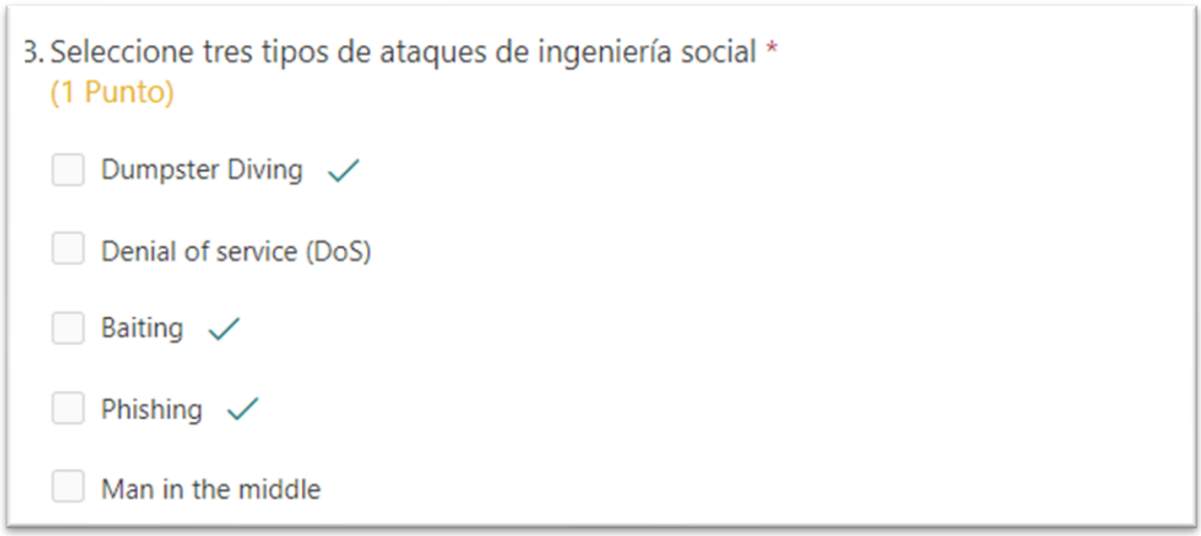


Fuente: elaboración propia.

Pregunta 3: Tipos de ataques en ingeniería social

La pregunta 3 está orientada a las diferentes técnicas utilizadas en los ataques de ingeniería social, la interrogante y sus respectivas respuestas se evidencia en la Figura 3.4.

Figura 3.4. Pregunta 3 Cuestionario de evaluación

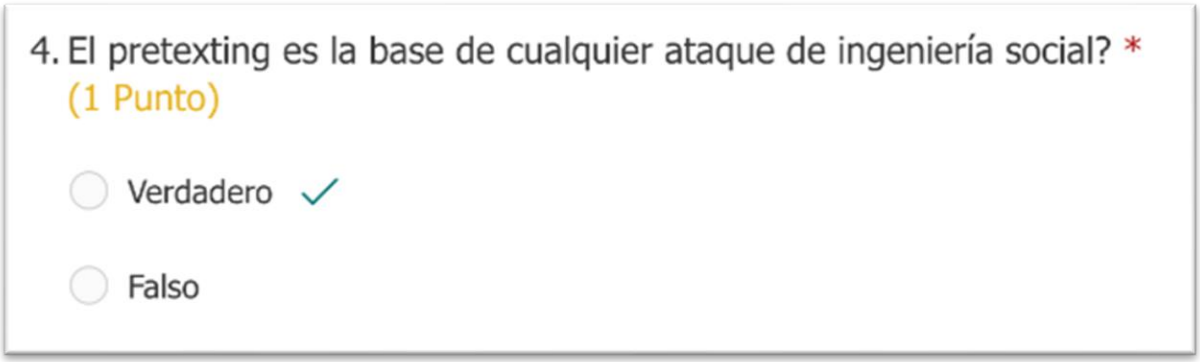


Fuente: elaboración propia.

Pregunta 4: Pretexting

La pregunta 4 se basa en el conocimiento acerca de la técnica de *pretexting*, esta se encuentra en la Figura 3.5.

Figura 3.5. Pregunta 4 Cuestionario de evaluación

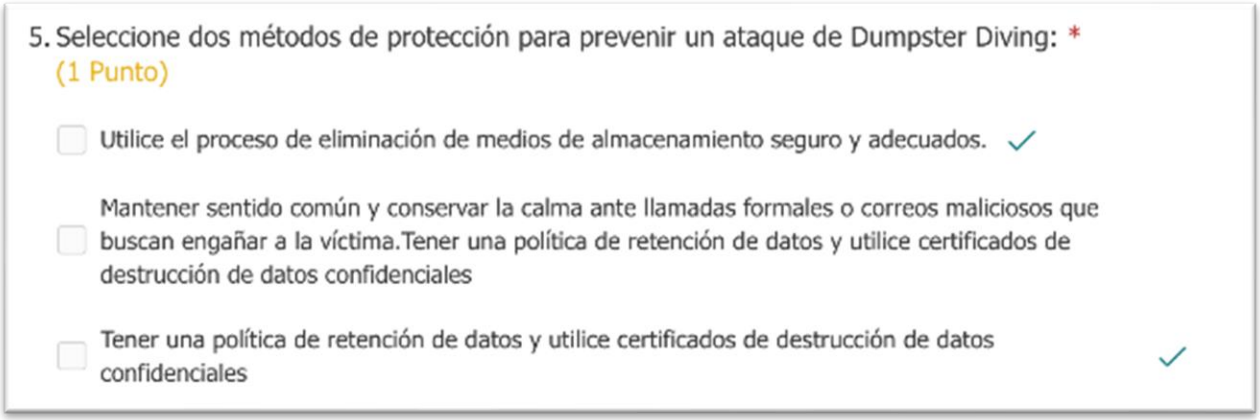


Fuente: elaboración propia.

Pregunta 5: Dumpster Diving

La pregunta 5 está orientada al conocimiento acerca de *Dumpster Diving* y los métodos de prevención ante este ataque, la pregunta se encuentra detallada en la Figura 3.6.

Figura 3.6. Pregunta 5 Cuestionario de evaluación

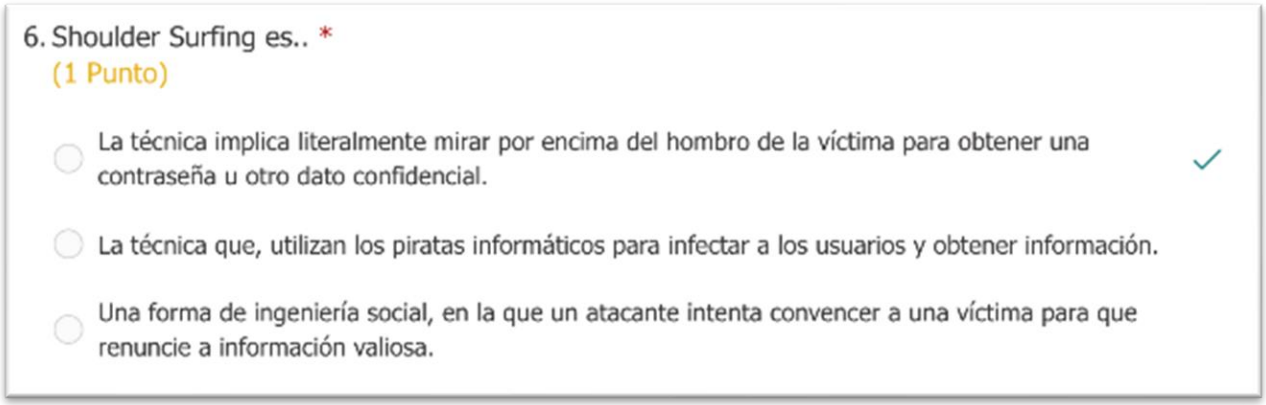


Fuente: elaboración propia.

Pregunta 6: Shoulder Surfing

La pregunta 6 se basa en el conocimiento acerca de la técnica de ataque *Shoulder Surfing*, la interrogante se evidencia en la Figura 3.7.

Figura 3.7. Pregunta 6 Cuestionario de evaluación

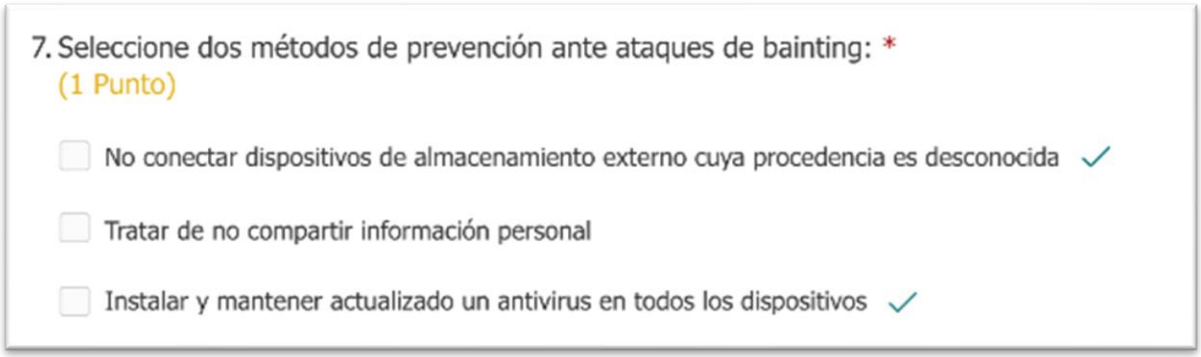


Fuente: elaboración propia.

Pregunta 7: Baiting

La pregunta 7 evalúa los métodos de prevención en los ataques de *Baiting*, esta pregunta se evalúa en la Figura 3.8.

Figura 3.8. Pregunta 7 Cuestionario de evaluación



Fuente: elaboración propia.

Pregunta 8: Phishing

La pregunta 8 evalúa el conocimiento acerca de la técnica de *phishing*, uno de los ataques más utilizados en la actualidad, la interrogante se muestra en la Figura 3.9.

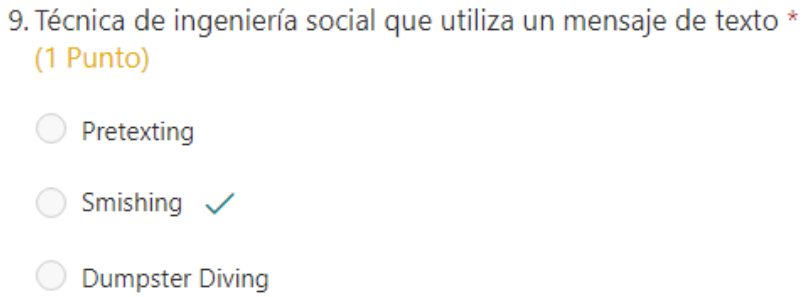
Figura 3.9. Pregunta 8 Cuestionario de evaluación

Fuente: elaboración propia.

Pregunta 9: Smishing

La pregunta 9 evalúa el conocimiento acerca de la técnica de *smishing*, misma que, hace uso de mensajes de texto, la pregunta se aprecia en la Figura 3.10.

Figura 3.10. Pregunta 9 Cuestionario de evaluación

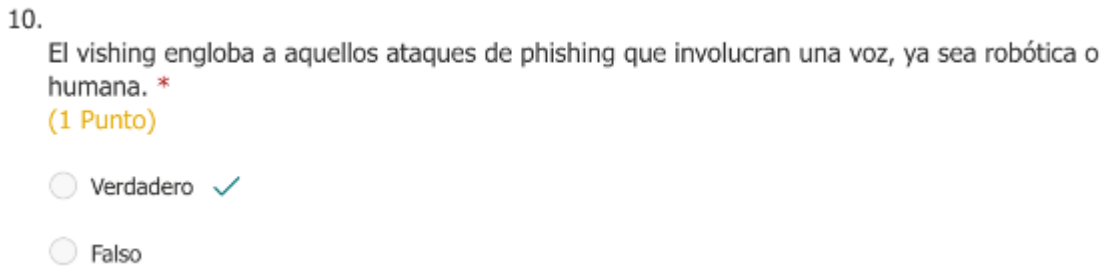


Fuente: elaboración propia.

Pregunta 10: Vishing

La pregunta 10 evalúa el conocimiento acerca de la técnica de *vishing*, la cual, hace uso de telefonía, la interrogante se visualiza en la Figura 3.11.

Figura 3.11. Pregunta 10 Cuestionario de evaluación

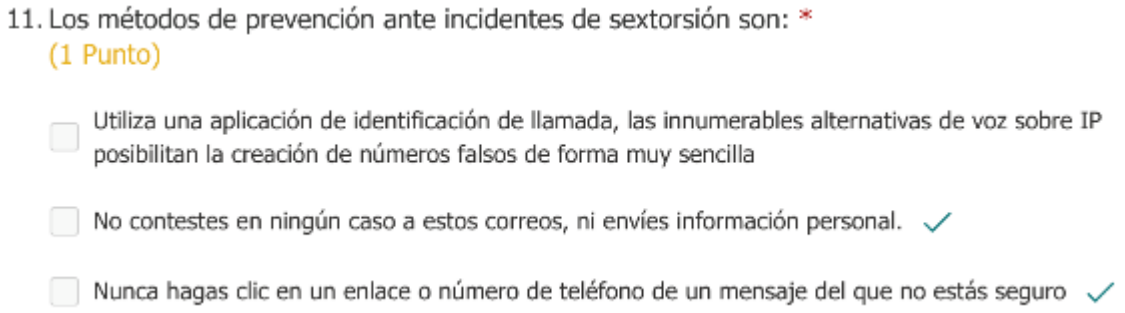


Fuente: elaboración propia.

Pregunta 11: Sextorision

Uno de los ataques más delicados es el de sextorsión, pues inclusive el daño psicológico ocasionado por este tipo de ataques pone en manifiesto la importancia de la interrogante, misma que, se evidencia en la Figura 3.12.

Figura 3.12. Pregunta 11 Cuestionario de evaluación



Fuente: elaboración propia.

3.2. Análisis de la evaluación

El cuestionario presentado está planteado en base a la guía desarrollada, cada una de las preguntas tiene una validez de 1 punto, con un valor total máximo de 11 puntos y mínimo de 0. El resultado final permite la obtención de un promedio general, el cual, indica el nivel de conocimiento expuesto por los participantes antes y después de la guía. Por otra parte, la interpretación de los datos obtenidos está basado en dos aspectos: cualitativo y cuantitativo, mismos que, se evidencian en la Tabla 3.1 detallada a continuación:

Tabla 3.1. Parámetros de evaluación

Valor Cualitativo	Valor Cuantitativo
Muy Bueno	≥ 8 y ≤ 11
Bueno	≥ 6 y < 8
Regular	≥ 4 y < 6
Malo	< 4

Fuente: elaboración propia.

A fin de validar el conocimiento que la guía ha generado en los usuarios, el cuestionario se presenta en dos ocasiones antes y después del desarrollo de la guía. En el promedio del primer cuestionario realizado al personal de Mutualista Ambato se obtuvo un promedio cualitativo equivalente a regular y cuantitativo equivalente a 5 sobre 11, los resultados promedio de esta prueba se evidencia en la Figura 3.13, presentada a continuación:

Figura 3.13. Promedio general de la primera evaluación

Fuente: elaboración propia.

De acuerdo con el alcance planteado por la guía desarrollada, ésta ha sido distribuida a todo el personal de la organización. Sin embargo, la evaluación es ejecutada al personal estratégico de Mutualista Ambato con un total de 10 usuarios encargados del manejo de la información sensible de la Institución. Posteriormente a la distribución de la guía, se procede a repetir la evaluación a los mismos usuarios y bajo los parámetros de calificación expuestos en el primer cuestionario, los resultados se evidencian en la Figura 3.14, a continuación:

Figura 3.14. Promedio general de la segunda evaluación

Fuente: elaboración propia.

El promedio final obtenido en la segunda evaluación, da como resultado, un valor cualitativo de *Muy Bueno*, con un valor cuantitativo equivalente a *8.4* sobre 11. Además, con el objetivo de obtener un resultado más detallado del cuestionario, se presenta la Tabla 3.2, la cual evidencia un resumen comparativo de los datos de cada interrogante:

Tabla 3.2. Resultados comparativo primera y segunda evaluación

Interrogante	Primera evaluación	Segunda evaluación
Pregunta 1	0,5	1
Pregunta 2	0,6	1
Pregunta 3	0,2	0,5
Pregunta 4	0,4	0,8
Pregunta 5	0,3	1
Pregunta 6	0,7	0,8
Pregunta 7	0,3	0,6
Pregunta 8	0,6	0,8
Pregunta 9	0,5	0,8
Pregunta 10	0,6	0,8
Pregunta 11	0,3	0,3
Total	5/11	11,4

Fuente: elaboración propia.

3.3. Análisis global de resultados

En la Tabla 3.3 se aprecia las puntuaciones obtenidas por cada participante en las dos evaluaciones realizadas para la validación de la guía.

Tabla 3.3. Puntuaciones por participante

Evaluados	Primera evaluación	Segunda evaluación
Participante 1	4	10
Participante 2	6	8
Participante 3	11	8
Participante 4	5	9
Participante 5	8	7
Participante 6	4	9
Participante 7	0	9
Participante 8	4	5
Participante 9	4	10
Participante 10	4	9
Total	5/11	11,4

Fuente: elaboración propia.

De acuerdo con los resultados obtenidos, se evidencia la mejora en el conocimiento de los participantes a través de la distribución de la guía realizada. Dicho de otro modo, los datos son consistentes en cuanto a que, el desarrollo de una guía es un método eficiente para la prevención de ataques de tipo Ingeniería Social, así como también, el desarrollo de este tipo de gestión documental se apega al plan de mejoras planteados por los Sistemas de Gestión de Seguridad de la Información.

Esta metodología de prevención es una opción de bajo costo para cualquier tipo de organización, quienes están en la obligación de garantizar la Integridad, Confidencialidad y Disponibilidad de los datos sensibles de la información, ante cualquier ataque, sea interno o externo a la Institución.

CONCLUSIONES

- La recopilación de la información realizada en el estado del arte, ha permitido evidenciar, cómo las instituciones financieras, están en la obligación de generar contantes mejoras dentro de su SGSI, con la finalidad de garantizar la CID en la información sensible de sus clientes.

- El estudio comparativo planteado en el estado del arte, muestra las técnicas de prevención más utilizadas por las entidades financieras. Esto significa que, no existe un método específico de protección ante este tipo de ataques, debido a que, la mayor vulnerabilidad en ingeniería social es el ser humano.

- La síntesis desarrollada como guía para prevenir los ataques de ingeniería social y las diferentes técnicas empleadas, permitió que, los usuarios internos, generen una concientización acerca de la información sensible que manejan, así como también, ello coadyuva a la organización a prevenir este tipo de ataques.

- La organización de los elementos constitutivos obtenidos en la guía, muestran que, el vector principal de ataque es el ser humano. Por la tanto, es importante que los usuarios mantengan un conocimiento sobre las amenazas de la ingeniería social dentro de las instituciones financieras.

RECOMENDACIONES

- Se recomienda mantener un sistema de gestión documental dedicado a la protección de la información, mismo que, seria continuamente adaptado en concordancia a las necesidades actuales.

- Al no existir una técnica específica de prevención de ataques de ingeniería social, se recomienda, combinar las diferentes estratégicas planteadas. De esta forma, se obtiene, una metodología completa para prevenir el riesgo de un ciberataque.

- Es recomendable que, las organizaciones mantengan informados a su personal en cuanto a temas de seguridad y protección de la información y de este modo, no ser proclives ante nuevas amenazas en cuanto a ciberataques.

- Al tener un impacto positivo el desarrollo de la guía, se recomienda realizar más investigaciones de este tipo, para generar mayor conocimiento en los usuarios sobre ataques y delitos informáticos, con un costo exequible para cualquier institución.

BIBLIOGRAFÍA

Abreu, J.L. (2014). El método de investigación. *International Journal of Good Conscience, 9* (3), 195-204.

Andrade, F., Alejo, O. J. & Armendariz, C. R. (2018). Método inductivo y su refutación deductista. *Revista Conrado, 14* (63), 117-122.

Arcotel. (2021). *Protocolo de seguridad para evitar la suplantación de identidad*. Recuperado de https://www.arcotel.gob.ec/protocolo-de-seguridad-para-evitar-la-suplantacion-de-identidad/

Albors, J. (2018). *Los correos de chantaje evolucionan e incluyen el secuestro de archivos*. Recuperado de https://blogs.protegerse.com/2018/12/11/los-correos-de-chantaje-evolucionan-e-incluyen-el-secuestro-de-archivos/

Angulo, J., & Córdova, M. (2019). *Análisis de la taxonomía de los delitos informáticos en el sector Bancario del Ecuador en el período 2014 – 2019 (Tesis de pregrado).* Recuperada de http://repositorio.ug.edu.ec/bitstream/redug/44411/4/2.-%20Titulacion%20-%20%20Julian%20Angulo%20Ramirez%20y%20Mariana%20Cordova%20Santana.pdf

Avast. (2021). *La guía más completa sobre el robo de identidad*. Recuperada de https://www.avast.com/es-es/c-identity-theft

Banco Pichincha. (2020). *Qué son los ataques de ingeniería social y cómo evitarlos*. Recuperado de https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social

Cárdenas, F. & Solares, P. (2016). *SGSI en las sociedades de información crediticia*. Recuperado de https://www.ecorfan.org/handbooks/Ciencias%20Sistemas%20Informacion%20T-I/Handbook%20Universidad%20Iberoamericana_7.pdf

Computerworld. (2021). *Ciberseguridad financiera: la experiencia del usuario versus la seguridad de la información*. Recuperado de

http://computerworld.com.ec/actualidad/tendencias/1314-ciberseguridad-financiera-la-experiencia-del-usuario-versus-la-seguridad-de-la-informacion.html

Enterprise (2021). *Sistema de gestión de la seguridad de la información*. Recuperado de https://enterpriseit.cl/conoces-lo-que-es-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Fernández, P. (2019). *Apuntes de verano sobre seguridad informática en el sector bancario*. Recuperado https://www.pablofb.com/2019/08/apuntes-de-verano-sobre-seguridad-informatica-en-el-sector-bancario/

Fiscalía General del Estado. (2014). *El COIP contempla una pena de tres a cinco años de prisión por robos de cuentas bancarias*. Recuperado de https://www.fiscalia.gob.ec/el-coip-contempla-una-pena-de-tres-a-cinco-anos-de-prision-por-robos-de-cuentas-bancarias/

Gavilánez, R., & Zambrano, D. (2017). Análisis de los ataques de hackers a entidades financieras: Una revisión post-literaria. *Journal of Economics and Management, 1*, 31-34.

Gómez, S. (2012). *Metodología de la investigación*. México: Red Tercer Milenio S.C.

Guzmán, C. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso (Tesis de pregrado).* Recuperada de https://alejandria.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=

Harán, J. (2018). *Los ciberataques dirigidos a bancos más importantes de los últimos tiempos*. Recuperado de https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/

Hernández, R., Fernández, C., y Baptista, M. (2010*). Metodología de la investigación* (5ª ed.). México: McGRAW-HILL.

Hinojosa, L. (2010). *Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del Ecuador (Tesis de pregrado).* Recuperada de

https://repositorio.uisek.edu.ec/bitstream/123456789/547/1/TESIS_GABRIELA_HINOJOSA.pdf

Incibe. (2019). *Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

Kanbanize. (2021). Qué es Kanban: Definición, Características y Ventajas. Recuperado de https://kanbanize.com/es/recursos-de-kanban/primeros-pasos/que-es-kanban

Lundberg, G. (2004). *Técnica de la investigación social*. México: Fondo de cultura económica.

Mieres, J. (2009). *Ataques informáticos Debilidades de seguridad comúnmente explotadas.* Recuperado de https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Morales, F, Toapanta S. & Toasa, R. (2019). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 27*, 553-565.

Muñoz, O. (2020). *Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el departamento de tecnologías de la información en la Cooperativa de Ahorro y Crédito Indígena SAC (Tesis de pregrado).* Recuperada de https://repositorio.uta.edu.ec/bitstream/123456789/31305/1/t1709si.pdf

Mutualista Ambato. (2021). *Mutualista Ambato*. Recuperado de https://www.mutualistaambato.fin.ec/?page_id=1980

Nieves, A. (2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013 (Tesis de pregrado).* Recuperada de https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Ojeda, F. & Moreno, V. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *CIENCIAMATRIA. Revista Interdisciplinaria de*

Humanidades, Educación, Ciencia y Tecnología, 6 (6), 192-219. DOI 10.35381/cm.v6i2.366

Ontek. (2018). *¿Qué es? Tríada CID (Confidencialidad, Integridad y Disponibilidad).* Recuperado de https://www.ontek.net/que-es-triada-cid/

OSI. (2020). *Campañas de concienciación*. Recuperado de https://www.osi.es/es/campanas

Pereira, F. (2012). *La clonación de tarjetas de crédito en el Ecuador, ¿un delito económico? (Tesis de posgrado).* Recuperada de https://repositorio.uasb.edu.ec/bitstream/10644/3021/1/T1096-MDE-Pereira-La%20clonacion.pdf

Pereira, Z. (2011), Los diseños de método mixto en la investigación en educación: Una experiencia concreta. *Revista Electrónica Educare, 15* (1), 15-29.

Pincay, O. (2021). *La seguridad bancaria y de la información*. Recuperado de https://www.segurilatam.com/seguridad-por-sectores/financiero/la-seguridad-bancaria-y-de-la-informacion_20200526.html

Prieto, B. (2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. *Cuadernos de Contabilidad, 18* (46). ISSN: 0123-1472

Ramos, Y., Urrutia, O. & Ordoñez, D., Bravo, A. (2017). *Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca*. Recuperado de https://revistas.utp.ac.pa/index.php/memoutp/article/view/1475/2121

Tejena, M. (2018). Análisis de riesgos en seguridad de la información. *Polo de Conocimiento, 18* (3), 230-244. DOI: 10.23857/pc.v3i4.809

Tuyú Technology. (2017). *¿Por qué es tan importante la Seguridad Informática?* Recuperado de https://www.tuyu.es/importancia-seguridad-informatica/

Urbano, P. (2016). Análisis de datos cualitativos. *Revista Fedumar Pedagogía y Educación, 3* (1), 113-126.

Vargas, J. (2018). *Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa*. Recuperado http://polux.unipiloto.edu.co:8080/00004663.pdf

ANEXOS

ANEXO A: Guía para campañas de ingeniería social

mutualista ambato

Orgullo Ambateño!

DEPARTAMENTO DE SISTEMAS Y TECNOLOGÍA

DISEÑO DE UNA GUÍA PARA CAMPAÑAS DE INGENIERÍA SOCIAL AL INTERIOR DE UNA INSTITUCIÓN FINANCIERA.

ELABORADO POR: DANIEL ROBERTO PEÑA PÉREZ

AMBATO-ECUADOR

2021

DISEÑO DE UNA GUÍA PARA CAMPAÑAS DE INGENIERÍA SOCIAL AL INTERIOR DE UNA INSTITUCIÓN FINANCIERA.

ÍNDICE

1. INTRODUCCIÓN

Las Autoridades de la entidad financiera Mutualista Ambato en conjunto con el Departamento de Sistemas y Tecnologías, mantienen un esfuerzo constante por conservar la confidencialidad, integridad y disponibilidad de la información digital de la Institución. Todo ello con el fin de, garantizar un óptimo servicio para sus clientes, y de esta forma, mantener la continuidad del negocio seguro, ante las amenazas internas o externas que se puedan presentar, en este ámbito y como parte de un plan de mejora dentro del departamento se ha propuesto la elaboración de una guía para campañas de Ingeniería Social, la cual esta centrada en:

- ***ISO 27000:*** Normativa para la implementación de un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
- ***MAGERIT v3:*** Normativa centrada en la elaboración de guías para la protección de información digital.

1. ANTECEDENTES

En los últimos años se ha evidenciado un crecimiento exponencial en los ataques y delitos informáticos. Por otra parte, los ataques informáticos a entidades bancarias conocidos como *"fraude financiero"*, es uno de los ataques de mayor incidencia a nivel mundial, siendo la técnica de ingeniería social uno de los vectores más utilizados por los ciber delincuentes. En el contexto planteado, acorde a los ítems de la Norma ISO 27000 la cual manifiesta que, toda Institución ya sea pública o privada deberá garantizar la Integridad, Confidencialidad y Disponibilidad de sus datos, toda organización tiene que, crear métodos para proteger su información digital sensible.

Acorde al reporte generado por la Organización de Estados Americanos alrededor del 70% de la población está conectada a servicios en línea, es por tal motivo que, en la acutalidad el internet es uno de los medios de comunicación mas utilizados. Por todo ello, el sector financiero fue uno de los primeros en adoptar las tecnologías y ofrecerlas a sus clientes. Este

ha experimentado uno de los mayores indices de digitalización en los últimos años, cada día un mayor número de clientes usan medios no presenciales para realizar transacciones por internet, pagos a través de dispositivos móviles o cualquier otro tipo de trámites bancarios.

Dentro de las metodologías de protección de la información digital sensible, es de vital importancia el uso de técnicas documentadas como son las guías, políticas y planes de contingencia, esto a fin de tener un respaldo escrito acerca de los correctos procesos del manejo de la información, además, permite al usuario final, conocer los diferentes riesgos a los que se enfrenta día a día. En este ámbito, las Autoridades de Mutualista Ambato en conjunto con el Departamento de Sistemas e Informática, consideran la importancia de la elaboración de una guía de campañas de Ingeniería Social a fin de mitigar casi en su totalidad los riesgos existentes ante dicha vulnerabilidad, y de esta forma, brindar a sus usuarios un conocimiento de como deben prevenirse estos ataques, así como también, saber qué hacer en caso de ser vulnerados por la metodología de Ingeniería Social.

2. OBJETIVO

Brindar métodos de protección ante ataques informáticos por la técnica de ingeniería social al personal interno de Mutualista Ambato.

3. ALCANCE

La presente guía tiene por alcance, enseñar a todos los usuarios internos dentro de Mutualista Ambato, métodos de protección de la información sensible ante ataques por ingeniería social, a fin de que estos posean un conocimiento amplia acerca de las diversas técnicas de ataques por dicho método y de esta forma, sepan utilizar diversas sistemáticas de prevención de tal modo que, la Organización no se vea vulnerada en uno de los activos mas importantes que posee, la cual es, la información digital sensible.

4. MATERIALES

Para el desarrollo de la presente guía se hace uso de las siguientes herramientas:

- *Hardware*:
  - Equipos de cómputo.
  - Teléfonos inteligentes (*Smartphone*)
  - Laptops.
- *Software*:
  - Sistema Operativo Kali Linux (Vitrtualizado)
  - Sistema Operativo Parrot (Virtualizado)
  - Sistema Operativo Windows
  - Correo Electrónico
  - Software pruebas
  - Internet

5. DIRIGIDO A

La presente guía está dirigida a, todos los usuarios internos de la organización, misma que se basa en tres aspectos fundamentales: prevención, protección, y seguridad de la información, de esta forma, se busca que, cada usuario sin importar su cargo sepa la importancia de los datos confidenciales sensibles que maneja la Mutualista Ambato.

6. ELABORACIÓN

La ingeniería social es un conjunto de técnicas que usan los ciberciminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios maliciosos. Además, los hackers pueden tratar de

aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información.

Figura 1: Ciclo de vida de un ciberataque de ingeniera social

Nota: Hacer click en la imagen para acceder al video

Casi todos los tipos de ataques conllevan algún tipo de ingeniería social. Por ejemplo, están los clásicos correos electrónicos de *"phishing"* y estafas de virus, con un gran contenido social. Los correos electrónicos de phishing intentan convencer a los usuarios de que su origen es legítimo, con la esperanza de obtener información personal o datos de la empresa, por insignificante que parezcan. Por otra parte, los correos que, contienen archivos adjuntos con virus a menudo aparentan provenir de contactos confiables u ofrecen contenido multimedia que parece inofensivo, como videos "divertidos" o "tiernos".

En algunos casos, los atacantes utilizan métodos más simples de ingeniería social para acceder a una red o computadora. Por ejemplo, un hacker puede frecuentar el comedor

público de un gran edificio de oficinas, buscar usuarios que estén trabajando en sus tablets o computadoras portátiles y mirar los dispositivos por encima de su hombro. Con esta táctica pueden conseguir una gran cantidad de contraseñas y nombres de usuario, todo sin necesidad de ni enviar un solo correo electrónico de ni escribir una línea de código de virus. Otros ataques requieren una comunicación real entre el atacante y la víctima; en estos casos, el atacante presiona al usuario para que le otorgue acceso a la red con el pretexto de un problema grave que es necesario resolver de inmediato. Los atacantes utilizan en igual medida la rabia, la culpa y la tristeza para convencer a los usuarios de que necesitan su ayuda y no pueden negársela. Para terminar, es importante prestar atención a la ingeniería social como un medio para crear confusión. Numerosos trabajadores y consumidores no se dan cuenta de que, con solo un poco de información (como el nombre, la fecha de nacimiento o la dirección), los hackers pueden acceder a múltiples redes haciéndose pasar por usuarios legítimos o miembros del personal de TI. Después de lograrlo, les resulta fácil restablecer contraseñas y obtener acceso prácticamente ilimitado.

La protección contra la ingeniería social comienza con la educación; los usuarios necesitan aprender que no deben hacer nunca clic en enlaces sospechosos y siempre deben proteger sus credenciales de inicio de sesión, incluso en la oficina y en el hogar. Sin embargo, si las tácticas sociales logran su objetivo, el resultado probable es una infección por malware. Para combatir los rootkits, troyanos y otros bots, es fundamental implementar una solución de seguridad de Internet de alta calidad que sea capaz de eliminar infecciones y rastrear su origen, en los principales ataques de ingeniería social se tiene:

Figura 2: Ataques de ingeniería social

Nota: Hacer click en la imagen para acceder al video

6.1. PRETEXTING (PRETEXTO)

El pretexting es una forma de ingeniería social, en la que un atacante intenta convencer a una víctima para que renuncie a información valiosa, así como al acceso a un servicio o sistema. La función distintiva de este tipo de ataque es que, los artistas de las estafas vienen con una historia -o pretexto- con el fin de engañar a la víctima. Por lo general, el pretexto le asigna al atacante el papel de alguien con autoridad que tiene derecho a acceder a la información que se busca, o que, puede usar la información para ayudar a la víctima.

Figura 2: Pretexting

Nota: Hacer click en la imagen para acceder al video

De acuerdo con el concepto de INCIBE el ***pretexting*** es la base de cualquier ataque de ingeniería social. Consiste en crear elaborar un escenario o historia ficticia, donde el atacante tratará que la víctima comparta información que, en circunstancias normales, no revelaría.

Métodos de Protección

Para ser víctima de un ataque de Pretexting no se necesita equipo sofisticado sino más bien, muchos de estos ataques solo se dan por astucia del atacante e inocencia de la víctima al caer en engaños, por ello, se recomienda:

- Mantener sentido común y conservar la calma ante llamadas formales o correos maliciosos que buscan engañar a la víctima.
- No ceder información fácilmente evitando caer en trampas y siempre usar programas de seguridad informática y equipos actualizados.

6.2. DUMPSTER DIVING (BUCEO EN LA BASURA)

El Dumpster diving (buceo en el contenedor) en informática se refiere a la exploración de la papelera de un sistema con el fin de encontrar detalles para que, un pirata informático pueda realizar un ciberataque. El primer paso para realizar un ataque a un servicio de redes sociales es bucear en el contenedor. Y la fase de ingeniería social vendrá después, cuando los usuarios en línea son llevados a una trampa para que, revelen datos privados sobre ellos.

Figura 2: Buceo en la basura

Nota: Hacer click en la imagen para acceder al video

Es el acto de acceder sin autorización a determinada información que, pasa por la basura de una empresa, ya sea dentro o fuera del edificio. El atacante generalmente busca algún tipo de información confidencial que se arrojó a la basura. La información de secreto comercial debe eliminarse adecuadamente, una eliminación inadecuada de la información podría brindar a los atacantes:

- Dirección de correo electrónico / dirección.
- Números telefónicos para realizar Fishing.
- Contraseñas y otros números de seguridad social que podríamos haber escrito en notas adhesivas para nuestra conveniencia.
- Estados de cuenta bancarios / estados financieros.
- Registros médicos.
- Documentos importantes.
- Credenciales de inicio de sesión de cuenta.
- Secretos comerciales.
- Secretos de marketing.
- Información de la base de empleados.
- Información sobre el software / herramientas / tecnologías que se utilizan en la empresa.

Métodos de protección:

Es importante siempre tener mucho cuidado al desechar la basura de Institución, en esto se recomienda la implementación de procesos a fin de prevenir este tipo de ataques, como:

- Tener un proceso de desmantelamiento de equipos documentados.
- Utilice el proceso de eliminación de medios de almacenamiento seguro y adecuados.
- Tenga una política de retención de datos y utilice certificados de destrucción de datos confidenciales.
- Haga que triturar sea conveniente.
- Educar a los empleados.
- Asegure la basura.

6.3. SHOULDER SURFING

Esta técnica implica literalmente mirar por encima del hombro de la víctima para obtener una contraseña u otro dato confidencial.

Hay otras variaciones del ataque. Los atacantes determinados pueden robar contraseñas y otros datos a una distancia significativa también con la ayuda de binoculares o equipos de filmación costosos. Por ejemplo, y en una variante especialmente de James Bond, los malvados incluso utilizan la tecnología de seguimiento ocular para adivinar cuál es su contraseña al examinar qué botones del teclado en pantalla se pulsan.

Figura 2: Mirando por encima

Nota: Hacer click en la imagen para acceder al video

Según recuerdan los expertos de la firma *Secure&IT*, muchos usuarios no son conscientes de que cuando viajan en bus, metro o tren, o se sientan en el banco de un parque o una terraza, alguien puede observar las operaciones que realizan en sus dispositivos. Además, el shoulder surfing también se utiliza en los cajeros automáticos de las entidades bancarias o cuando las víctimas mantienen una conversación telefónica.

Métodos de protección:

Evitar los ataques de shoulder surfing en una organización requiere esfuerzos concertados de concientización de seguridad cibernética para cambiar el comportamiento. Sin embargo, a nivel individual, es posible seguir varios consejos para reducir drásticamente las posibilidades de ser víctima del shoulder surfing:

- Utilizar la verificación en dos pasos.
- Utilizar un gestor de contraseñas.
- Evitar que terceros tengan visión de la pantalla.

- Tratar de no compartir información personal.
- Cifrar el dispositivo.

6.4. BAITING

Baiting es una de las muchas amenazas que hay en la red. Es una técnica que, utilizan los piratas informáticos para infectar a los usuarios y obtener información. Tiene muchas similitudes con el Phishing.

El objetivo principal del Baiting es atraer a la víctima, hacerle ver que, están ante algo legítimo y positivo para ellos. Busca usuarios desprevenidos que hagan clic y accedan a un enlace. Suele ser una oferta muy ventajosa, algo que provoque que esa persona tenga la necesidad de entrar, de informarse, y de esta forma entregar sus datos.

Figura 2: Baiting

Nota: Hacer click en la imagen para acceder al video

Métodos de protección:

Existen diversas medidas preventivas para evitar en lo posible este ciberataque. La principal es concienciar y educar al personal. Ellos son la mejor defensa ante este tipo de amenazas,

debido a que, los sistemas de seguridad más sofisticados no son seguros si dejamos las "puertas abiertas":

- Estar alerta a terceros que puedan ver la pantalla de teléfonos móviles y tabletas
- Resguardar el teclado al introducir los dígitos de contraseñas.
- Instalar en el móvil un 'Privacy Screen Protector', es decir, un protector de pantalla de vidrio templado que protege los dispositivos y obstruye la vista de la pantalla a los intrusos.
- No conectar dispositivos de almacenamiento externo cuya procedencia es desconocida.
- Instalar y mantener actualizado un antivirus en todos los dispositivos.

6.5. PHISHING

El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que, en realidad pretenden manipular al receptor para robar información confidencial. Por eso siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador.

Figura 2: Phishing

Nota: Hacer click en la imagen para acceder al video

La mayoría de los ataques de phishing comienzan con la recepción de un correo electrónico o un mensaje directo en el que, el remitente se hace pasar por un banco, una empresa u otra organización real con el fin de engañar al destinatario. Este correo electrónico incluye enlaces a un sitio web preparado por los criminales que imita al de la empresa legítima y en el que, se invita a la víctima a introducir sus datos personales.

Métodos de protección:

En este sentido existe una vinculación entre el spam y el phishing, ya que, los correos electrónicos fraudulentos suelen enviarse de forma masiva para multiplicar el número de víctimas potenciales de los hackers. De hecho, si bien el e-mail continúa siendo el medio más utilizado por los ciberdelincuentes para este tipo de fraudes, el phishing puede utilizar otros medios de comunicación, es por tal razón que, se debe tomar en cuenta las siguientes recomendaciones:

- Después de leer el correo no hagas clic en ningún enlace.
- Realiza las verificaciones pertinentes en tu espacio personal de cliente, acudiendo directamente desde la Url del navegador.
- Mantener tu equipo protegido, pero, además, siempre debes tener las actualizaciones más recientes de tu sistema operativo y navegador web.
- Además, lo ideal es que cuentes con una capa adicional con un antivirus profesional.
- Introduce tus datos confidenciales sólo en sitios web seguros. Para que un sitio se pueda considerar como 'seguro', el primer paso, aunque no el único es que, empiece por https://
- Revisa periódicamente tus cuentas. Nunca está de más revisar facturas y cuentas bancarias cada cierto tiempo para estar al tanto de cualquier irregularidad en las transacciones.
- Ante cualquier duda, no te arriesgues. El mejor consejo ante el phishing es siempre fomentar la prudencia entre todas las personas que forman parte de la organización. Asegurar la autenticidad del contenido ante la más mínima sospecha es la mejor política.

6.6. SMISHING

Es una forma de phishing que involucra un mensaje de texto. A menudo, esta forma de phishing involucra un mensaje de texto en un SMS o un número de teléfono. El smishing es alarmante porque las personas tienden a confiar más en los mensajes de texto que en los mensajes de correo electrónico. La mayoría de las personas son conscientes del riesgo que conlleva hacer clic en vínculos incluidos en mensajes de correo electrónico. Sin embargo, no puede decirse lo mismo cuando se trata de mensajes de texto.

Figura 2: Smishing

Nota: Hacer click en la imagen para acceder al video

El smishing usa elementos de ingeniería social para que comparta información personal. Esta táctica se aprovecha de su confianza para obtener información. Los atacantes buscan todo tipo de información: desde contraseñas en línea hasta el número de la seguridad social o

información de su tarjeta de crédito. Una vez que los obtienen, pueden comenzar a realizar compras a su nombre. En ese momento es cuando comienzan los problemas.

Métodos de protección:

La solución para el 'smishing' es no hacerle caso a los mensajes que solicitan realizar una llamada, operación, o brindar datos, además de tomar en cuenta las siguientes recomendaciones:

- Considerar las alertas de seguridad urgentes y los canjes de cupones, ofertas u oportunidades que requieren que actúes rápido como signos de advertencia de un intento de pirateo.
- Ninguna institución financiera o empresa te enviará un mensaje de texto que te pide que actualices la información de tu cuenta o que confirmes el código de tu tarjeta de cajero automático.
- Nunca hagas clic en un enlace o número de teléfono de un mensaje del que no estás seguro.
- Busca números sospechosos que no parezcan números de teléfono móvil auténticos, como "5000". Como señala Network World, estos números están relacionados con servicios de correo electrónico como mensaje de texto, que los estafadores a veces utilizan para evitar proporcionar sus números de teléfono reales.
- No guardes tu tarjeta de crédito o información bancaria en el smartphone.
- Niégate a morder el anzuelo, simplemente no respondas.
- Informa de todos los ataques de smishing a la FCC para tratar de proteger a los demás.

6.7. VISHING

La palabra vishing nace de la unión de voice y phishing, es decir, engloba a aquellos ataques de phishing que involucran una voz, ya sea robótica o humana. En estas, los atacantes pueden llegar a la víctima mediante llamadas telefónicas masivas, tal como un call-center corporativo, o dejando correos de voz. Además, entre las temáticas predilectas elegidas por

los estafadores para estas comunicaciones encontramos referencias a problemas financieros o de seguridad de nuestro ordenador o dispositivo móvil, o la suplantación de identidad de un supuesto familiar o conocido, entre otros.

Si bien esta técnica puede representar un mayor costo y trabajo del lado de los cibercriminales, es más efectiva que otras formas de ataque similares como el phishing: a través de una llamada telefónica se logra una comunicación más personal que a través de un correo electrónico, por lo que la manipulación emocional es más fácil de llevar a cabo. En casos extremos, el atacante simula tristeza o llanto ante un supuesto problema que se le presenta y que solo la víctima puede resolver.

Figura 2: Vishing

Nota: Hacer click en la imagen para acceder al video

Este ataque es peligrosamente eficaz y se apoya en técnicas de ingeniería social, en el cual el atacante se comunica telefónicamente o vía mensaje de voz haciéndose pasar por una empresa o entidad confiable con la intención de engañar a la víctima y convencerla de que realice una acción que va en contra de sus intereses.

Métodos de protección:

La solución pasa por hacer caso omiso a los SMS que nos solicitan llamar o efectuar alguna otra operación ni dar datos por teléfono, al igual que las siguientes recomendaciones:

- Utiliza una aplicación de identificación de llamada, las innumerables alternativas de voz sobre IP posibilitan la creación de números falsos de forma muy sencilla.
- No hagas clic en los enlaces ni respondas a las indicaciones. Si recibes un mensaje automatizado o un correo electrónico en el que se te pide hacer clic en enlaces o responder preguntas.
- Verifica la identidad de la persona que se ha puesto en contacto contigo. Si el remitente proporciona un número de devolución de llamada, puede ser parte de la estafa, así que no lo uses.
- Nunca facilites información personal o confidencial: ni tampoco respondas a requerimientos sobre tu tarjeta de débito o crédito, documento de identidad, dirección, fecha de nacimiento, entre otros.
- Cuelga si sospechas, en el momento en que sospeches que, se trata de una llamada telefónica fraudulenta, no sientas la obligación de tener que, mantener una conversación cortés.
- Actualiza constantemente tu sistema de antivirus y las herramientas antispyware.

6.8. SEXTORSION

Los delincuentes roban el dinero a sus víctimas mediante una gran variedad de métodos, pero hackear los mensajes de texto y las webcams eleva su despiadada eficiencia a un tipo de delincuencia muy personal llamada sextorsión, consiste en la amenaza de revelar información íntima sobre una víctima a no ser que esta pague al extorsionista. En esta era digital conectada, dicha información podría incluir mensajes de texto sexuales (en inglés conocidos como sexts), fotos íntimas e, incluso, vídeos. Los delincuentes suelen pedir dinero, pero a veces buscan material más comprometedor (envía más o divulgaremos tus secretos).

Puede que lo más interesante de la sextorsión sea que la gran mayoría de victimas son adolescentes, y no es que se les conozca por tener mucho dinero, pero esta parte de la población representa a la víctima perfecta para estos extorsionistas.

Figura 2: Sextorsion

Nota: Hacer click en la imagen para acceder al video

Métodos de protección:

Cada individuo tiene libre albedrío en referencia a su vida privada, siempre y cuando sus actos no infrinjan daño a si mismos o a terceros, o estén involucrados menores de edad, incapacitados o quien no tenga plena capacidad para prestar su consentimiento. Es por eso que, en caso de ser víctima de este tipo de ataque se recomienda tener las siguientes consideraciones:

- Si te llegan correos que no has solicitado o de desconocidos, no los abras y eliminalos.
- No contestes en ningún caso a estos correos, ni envíes información personal.
- Mantén todos tus dispositivos y antivirus actualizados.
- En ningún caso envíes datos de tus contactos, ni reenvíes el correo, de este modo ayudarás a que no se extienda el fraude.
- En caso de duda, consulta directamente con las fuerzas y cuerpos de seguridad del estado.

7. RECOMENDACIONES

De acuerdo a LISA Institute (entidad especializada en formación en Inteligencia, Ciberseguridad y Ciberinteligencia), en concordancia con el Instituto Nacional de Ciberseguridad INCIBE, a fin de mitigar las vulnerabilidades existentes en ataques de ciberseguridad se plantea tomar las siguientes consideraciones:

- No abras correos electrónicos de origen desconocido o que no hayas solicitado. Es importante que nada más los recibas, los elimines directamente.
- No contestes nunca a los mensajes sospechosos ya sea por móvil o email.
- Toma medidas de precaución a la hora de seguir los enlaces que te han enviado a través del correo electrónico, SMS, WhatsApp o redes sociales, aunque sean de contactos conocidos.
- Ten cuidado cuando te descargues archivos adjuntos de correos, SMS, WhatsApp o en redes sociales, aunque sean de contactos conocidos.
- Ten siempre actualizado el sistema operativo y el antivirus, además de tenerlo siempre activo.
- Verifica siempre la seguridad de los sitios web en los que introduzcas tus datos personales y/o bancarios. Deben utilizar un certificado de seguridad y utilizar el protocolo HTTPS.
- Verifica la seguridad de las redes wifi-públicas a las que te conectas. Si dudas, es mejor que no compartas información confidencial ni introduzcas credenciales de usuario o contraseñas que puedan ser robadas.
- Escribe las URL de forma manual y no uses los enlaces de los mensajes sospechosos.
- Desconfía de las personas que acabas de conocer, aunque sean afines a ti, especialmente si te están informando de riesgos y oportunidades urgentes o de alto impacto.
- Sospecha en caso de que te ofrezcan un premio o trabajo idílico que sea rápido o fácil de conseguir. Como norma general, recuerda que, todo en la vida cuesta tiempo y/o dinero.

8. FIRMAS DE ENTREGA Y REVISÍON

X

Daniel Roberto Peña Pérez
Administrador de Redes y Soporte Técnico

X

William Fernando Borja Riveneira
Oficial de Seguridad de la Información

X

Diego Mauricio Cadena Velasco
Subgerente de Sistemas Y Tecnología

X

Mariana de Jesus Pérez Suarez
Subgerente de Administración Integral de R...