DECANATO DE INGENIERIA E INFORMATICA

Escuela de Informática

Trabajo de grado para optar por el título de:

INGENIERO(A) EN SISTEMAS DE COMPUTACIÓN

TEMA:

Evaluación de la seguridad de la información utilizando ingeniería social como vector de ataque en la Administradora de Riesgos Laborales. Periodo cuatrimestral septiembre-diciembre 2019.

SUSTENTANTES:

Bryan Isaul Peña	2009-0238
Luis Rafael Segura	2015-2252

ASESOR

Ing. Edgar Morrobert Ovalles

Santo Domingo, D.N.

Noviembre, 2019

Los conceptos expuestos en esta investigación son de la exclusiva responsabilidad de sus autores.

Evaluación de la seguridad de la información utilizando ingeniería social como vector de ataque en la Administradora de Riesgos Laborales. Periodo cuatrimestral septiembre-diciembre 2019.

DEDICATORIA

Dedico este trabajo a mi familia por apoyarme y permitirme experimentar esta etapa de mi vida de lograr mis objetivos, a mi madre para que sea testigo de los resultados de sus sacrificios en mí formación, a mis compañeros de Universidad y amistades muy cercana por acompañarme recorrido que caminamos juntos durante estos años.

Bryan Isaul Peña.

DEDICATORIA

Mis primeras líneas están dedicadas a Dios sobre todas las cosas, aquel que obro y puso el juego a favor aun en los momentos negativos. Mis padres, hermanos y allegados involucrados en este grato proceso, sin duda alguna cada uno de ustedes fue un punto de apoyo en el momento necesario. A mis compañeros y cada persona que lea y sea testigo de este fruto, que les sirva de inspiración para alcanzar sus sueños plasmados en cada etapa de la vida.

Luis Rafael Segura.

AGRADECIMIENTOS

Mis primeras líneas de agradecimiento se las dedico a mi madre, Estefanía Peña Moreta, por permitirme haber llegado hasta este punto de mi vida, por darme una muy buena educación, apoyo y sabiduría necesaria para lograr una de las principales metas de la vida. Fue mucho el sacrificio que hizo para llevarme (y aun lo hace) hasta este momento y estaré hasta el final de mis días agradecido por darme este regalo invaluable de ser mi madre y todo. Muchísimas gracias.

En segundo lugar, quiero agradecerle a mi hermano por acompañarme y aguantarme día a día, y claro un apoyo y cariño que solo un hermano puede darte.

En tercera instancia, un gran agradecimiento al SR. Juan E. López, por permitirme introducirme en el mundo laboral, por darme la oportunidad y libertad de poder estudiar, de ser esas personas únicas en la vida que no piden nada a cambio, que te hacen sentir como si son parte de tu familia, aunque no tengan ninguna responsabilidad conmigo, muchas gracias, larga vida para él y su familia.

En cuarta instancia, agradecido con todos esos compañeros y maestros de la Universidad APEC, que me acompañaron en este camino laborioso y de muchos conocimientos. A esos compañeros que pasan a ser casi hermanos que te regala la vida muchas gracias por estar ahí. También al mi maestro y asesor Edgar Morrobert, por tan buenas enseñanzas y experiencias en el mundo profesional. Un excelente guía para la realización de este proyecto, muchísimas gracias.

Bryan Isaul Peña.

AGRADECIMIENTOS

Dios, sin duda alguna el guía y mejor acompañante en este proceso, hoy le doy las gracias por permitirme la sabiduría necesaria para llegar hasta aquí y no desistir en el camino. Mis maestros, en ocasiones un tanto estrictos, pero siempre queriendo lo mejor para cada uno de sus alumnos, gracias por ser fuente apoyo e inspiración para mí y mis compañeros universitarios.

Mi padre, Rafael Antonio Segura, desde el primer día fuiste y seguirás siendo fuente de inspiración y sinónimo de perseverancia para mí y todos tus hijos, del mismo modo, eres la prueba perfecta de que todo se logra bajo el manto de la persistencia, el trabajo duro y Dios como guía en cada etapa de la vida. Aún recuerdo tus palabras de aliento antes de tan siquiera iniciar este proceso, eres un padre excepcional. ¡Gracias!

Mi madre, Luisa Aracelys Melo, aquella que sin importarle nada siempre estuvo ahí para mí en cada momento. Desde darme los alimentos, una educación basada en valores y hasta tus regaños, hoy quiero que te sientas orgullosa de ti misma pues esta meta alcanzada es tuya. Gracias por tus consejos y tus palabras que me tranquilizaban en los momentos más extenuantes, tú sí que eres una verdadera madre MVP.

Mis hermanos, son y serán fuentes de inspiración al ver sus metas logradas, aunque somos diferentes sin duda alguna cada uno tiene las mejores cualidades que Dios me ha permitido conocer. Gracias por sus risas, abrazos y momentos de

alegría, si tuviera la oportunidad de volver a nacer sin dudarlo sería al lado de ustedes.

Mi abuela Violeta Aristy, aún recuerdo aquella tarde que llego con el libro Nacho en sus manos, a partir de ese momento mis tardes fueron dedicadas a ese hermoso regalo que me abrió las primeras puertas del aprendizaje. Gracias por cuidarme y reír de mis travesuras, esta meta cumplida también es suya.

Por último, a todas y cada de una de las personas que intervinieron y se sienten identificadas en este arduo proceso, en especial al señor Josué Fortunato, por confiar en mi e intervenir dentro de sus posibilidades para mis facilidades universitarias. Nuestro asesor de y guía Edgar Morrobert, pieza fundamental en este engranaje, sus clases y charlas fueron musa para este proyecto. ¡Gracias!

Luis Rafael Segura.

Índice de contenido

Índice de Figuras.

Índice de Tablas.

INTRODUCCIÓN

Desde tiempos remotos las personas han intentado manejar y manipular el ambiente que los rodea a su parecer, con la finalidad sacarle el provecho que crean necesarios; ya sea a través de la domesticación de animales o simplemente fingiendo interés en alguien y por las cosas que realiza. Asimismo, se pueden apreciar distintas formas de mover el juego a favor de un individuo en particular. En este caso, podemos encontrar diversas situaciones que se producen luego de que una manipulación intrapersonal, como lo son: ruptura de confianza, negación, frustración y las más famosa de todas, ¿Por qué a mí?

Tomando en cuenta lo antes dicho, sacamos a relucir un término no tan novedoso pero el cual ha tenido un auge sobresaliente en los últimos años, “La ingeniería social”. Retrocediendo un poco y poniendo énfasis en que muchos autores la describen como la parte oscura de la psicología humana, no es para menos que este altamente relacionada en los ataques a la seguridad de la información en empresas y organizaciones multinacionales en todo el mundo.

Dependiendo de la finalidad con la cual sea utilizada, “La ingeniería social” puede ser catastrófica a la hora de su implementación como vector de ataque. En efecto, la misma posee dos de las características más temidas en el mundo de la seguridad de la información, la posibilidad del robo de credenciales de usuarios de alta categoría simplemente bajo el manto de la confianza y que prácticamente la víctima no tiene idea del ataque hasta que ya es demasiado tarde.

Por tal razón en comparación con otros métodos de ataques con relación a la protección de los datos, esta resulta bastante atractiva para los victimarios. Sobre todo, por su bajo costo a la hora de ser llevada a cabo y sin duda alguna, la falta de documentación en las personas con relación a este tema la hace ideal y propicia para casi todos los ambientes.

En la Republica dominicana tan solo para el año 2014 se produjo una fuga de más de RD$120 millones de pesos, según establece la Asociación de Bancos Comerciales de la República Dominicana en su resumen del mes de febrero del mismo año. En más del 50 % de todos los reportes estudiados, el vector de ataque fue la ingeniería social como tal o cualquiera de sus múltiples facetas.

Por consiguiente, se toma la iniciativa de evaluar la seguridad de la información dentro una institución gubernamental utilizando la ingeniería como vector de ataque. Poniendo a prueba los conocimientos y capacidades de sus empleados en cuanto a este tema se refiere y sobre todo la cantidad de información privilegiada que tienen en sus manos.

Al momento de realizar esta investigación La Administradora de Riesgos Laborales se encontraba en un proceso de transición que bajo la promulgación de la nueva Ley 397-19 se establece que pasara a ser llamado Instituto Dominicano de Prevención y Protección de Riesgos Laborales (IDOPPRIL).

METODOLOGÍA

La siguiente investigación busca como resultado final, evaluar la seguridad de la información en la Administradora de Riesgos Laborales e identificar y mitigar las razones principales de la plena desinformación por parte de los empleados con relación a los danos que los ataques de ingeniería social pueden provocar. Por tal razón, podemos clasificar la investigación de tipo explicativa, pues su objetivo final es explicar por qué ocurre dicho fenómeno y en qué condiciones se ejecuta el mismo.

Debemos tener claro que en esta investigación ocurrirá un proceso deliberado de observación, el cual ayudara a lograr resultados de los objetivos ya planteados previamente. A su vez, podemos afirmar que iremos de la mano con el método de estudio deductivo, pues partiremos de una vista general para luego identificar las verdades particulares. Sin embargo, también nos apoyaremos en el método analítico, el cual puede establecer la relación causa-efecto.

Teniendo claro que las fuentes de la investigación vendrán por parte de libros, textos y trabajos de estudios previamente realizados, la podemos clasificar como primarias. Al mismo tiempo que, iremos apoyados con técnicas como las encuestas, cuestionarios, observación y sondeos, para llegar de una manera focal a los objetivos.

RESUMEN EJECUTIVO

La Administradora de Riesgos Laborales (ARL) tiene bajo su tutela un gran manejo de información personal y financiera de sus afiliados en los casos presentados, así mismo como todos los datos interinos de la institución, referencia delicada y de sumo interés para atacantes maliciosos. Es por ello, que la institución coloca bastante énfasis en sobre guardar todos estos datos privilegiados. Sin embargo, en los últimos años se ha incrementado considerablemente la penetración, sustracción y des integridad de los datos por parte de dichos agentes malintencionados.

A razón de esto, es importante evaluar las debilidades en la integridad y confiabilidad de los datos en dicha institución, los cuales son manejados día tras día por usuarios que no siempre están conscientes de lo que tienen en sus manos. Manejadores de información con nivel pobre de conocimiento de que tan importante son los recursos que tienen a su disposición y en cuanto a los vectores de ataque existentes para el hurto de información pertinente.

Cabe señalar que en la actualidad existen normas y protocolos a seguir, pero la mayoría de estos son totalmente desconocidos por los empleados. Dichas normas y protocolos no son para erradicar por completo el riesgo latente antes visto, sino que buscan disminuir y colocar más cerca de la marca cero los éxitos en los ataques de ingeniería social a usuarios no entrenados. Hay que destacar que la mayoría de las instituciones y organizaciones no le es atractivo sacar a flote este tipo de problemas; pero, en definitiva, es preciso insistir en el conocimiento y capacitación

pertinente sobre dicha situación. No ver el problema como enemigo en todo esto, sino más bien hacerlo evidente a nivel interno estos detalles y así atacar directamente para brindar un seguimiento y soporte de ayuda a situaciones presentadas.

CAPÍTULO I:

ASPECTOS INTRODUCTORIOS DE LA INVESTIGACION

1.1 Selección del tema

Evaluación de la seguridad de la información utilizando ingeniería social como vector de ataque en la Administradora de Riesgos Laborales. Periodo cuatrimestral septiembre-diciembre 2019.

1.2 Planteamiento del problema

La Administradora de Riesgos Laborales es la institución guía plasmada en el sistema de Seguridad Social por el gobierno dominicano para brindar un seguimiento propicio de los accidentes laborales en todo el a país. A razón de esto, la misma se encarga de velar por el cumplimiento de la ley 87-01 en todos sus ámbitos, siendo uno de los más importantes el pago de coberturas medicas e incapacidades laborales.

En consecuencia, dicha institución tiene bajo su mando información privilegia de alto nivel de cada uno de sus afiliados. Datos que en las manos equivocadas podrían ser explotados y poner en jaque a personas que en su mayoría pertenecen a una clase social desfavorecida y no tan afortunada. Por tal razón, estos datos deben estar bajo completo anonimato y fuera del alcance de personas no autorizadas. Pero esto no es 100 % que sea llevado a cabo ya que se pueden

identificar los siguientes problemas dentro de la institución en cuanto a la seguridad de la información de refiere:

Falta de documentación en temas de la seguridad de la información por parte de los empleados.

Desconocimiento total en los empleados de los diferentes vectores de ataques que existen.

Alta confianza depositada a nivel externo e interno.

Falta de entramiento básico para los empleados en temas de la seguridad de la información.

Todas las anteriores son las bases para llevar a cabo esta investigación, trabajada y enfocada directamente en los empleados de la Administradora de Riesgos Laborales y como responden a los métodos de ataque externos. Asimismo,

evaluando su nivel de vulnerabilidad en cuanto al tema de la seguridad de la información se refiere.

1.3 Justificación

1.3.1 Teórica

Es claro que a instituciones y organizaciones de mediana y gran escala no le convence del todo decir que hasta cierto punto si son vulnerables y poseen mínimas debilidades que corren el riesgo de ser explotadas por una amenaza latente; los agentes maliciosos. Siguiendo lo antes dicho, podemos decir abiertamente que poseemos un enfoque fuera de lo común en cuanto a esto, pues buscamos la aceptación propia para así poder construir una base fructífera en cuanto a protección y prevención de los ataques de ingeniería social se refiere.

Justificamos este estudio por como la información debe ser tratada y a su vez manipula, teniendo como enfoque primario la desinformación por parte de los empleados con relación a estos casos. Entendemos que en ocasiones es de suma importancia dar el primer paso y más aún cuando nos referimos a la seguridad de la información, lo más preciado en nuestra actualidad. Sin duda alguna.

1.3.2 Practica

Esta investigación se realiza porque existe la necesidad de mejorar el nivel de información por parte de los empleados en relación con los ataques de ingeniería

social y las consecuencias de los mismos. Asimismo, entendemos que dicho trabajo de investigación llevara a la contribución de medidas que podrían ser aplicadas a partir de nuestros resultados obtenidos.

1.3.3 Metodológica

A sabiendas que la observación es el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en el ambiente y que el método deductivo parte de lo general a lo particular, justificamos la implementación de estos por ser y poseer las características más adecuadas para esta investigación.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Evaluar la seguridad de la información en la Administradora de Riesgos Laborales.

1.4.2 Objetivos específicos

- Cuantificar las consecuencias ante la inseguridad de los datos.

- Enumerar los pasos existentes en la elaboración de la seguridad de la información.
- Clasificar las vulnerabilidades en la seguridad de los datos.

1.5 Métodos de investigación

1.5.1 Observación

“Es el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en la realidad por medio de un esquema conceptual previo y con base en ciertos propósitos definidos generalmente por una conjetura que se quiere investigar” (Sevilla, M, 2011).

1.5.2 Deductivo

“Consiste en ir de lo general a lo particular; se inicia con la observación de fenómenos generales con el propósito de señalar las verdades particulares, el proceso deductivo no es suficiente por sí mismo para explicar el conocimiento” (Sevilla, M, 2011).

1.6 Tipos de investigación

1.6.1 Investigación explicativa

“Buscan encontrar las razones o causas que ocasionan ciertos fenómenos, su objetivo último es explicar por qué ocurre un fenómeno y en qué condiciones se da éste” (Sevilla, M, 2011).

1.6.2 Investigación de campo

“Es el conjunto de acciones encaminadas a obtener en forma directa datos de las fuentes primarias de información, es decir, de las personas y en el lugar y tiempo en que se suscita el conjunto de hechos o acontecimientos de interés para la investigación” (Rivero, 2009).

CAPÍTULO II:

SEGURIDAD DE LA INFORMACIÓN, RIESGOS, CONTROLES Y ATAQUES

2.1 Seguridad de la información

2.1.1 La Seguridad de la Información

“La seguridad de la información permite asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización” (MAGERIT,2012). Su principal objetivo no es solo proteger TIC (Tecnología de información y comunicación), sino de todos los activos que son de gran valor para la organización.

En ese sentido, la seguridad de información son un conjunto de técnicas y medidas que tienen como propósito de mantener protegida la información importante para una institución. Estos tipos de sistemas se apoyan mucho de las nuevas tecnologías de información, tales como routers, servidores, switch, firewalls, software, etc. Sistemas de control que de alguna manera aseguran que quienes tienen acceso a estos datos solo pueden ser usuarios autorizados.

Todos los archivos de información de las organizaciones, hoy en día se enfrentan a amenazas tales como espionaje industrial, sabotaje, fraudes electrónicos, fenómenos naturales, o simplemente un mal uso al tratar la información. Muchas de estas amenazas provienen de hackers, empleados, errores humanos, ingenieros sociales, entre otros, con el propósito de dañar la imagen o conseguir información de importancia de una organización.

2.1.2 Objetivos de la seguridad de la información

Los objetivos de la seguridad de información son la Integridad, Disponibilidad y Confidencialidad. Se debe llevar un plan de acción donde se contemplen las políticas, el uso de las tecnologías, controles de seguridad y todos los procesos que detecten cualquier tipo de riesgo a los que pueden exponerse los recursos de información. En el caso de la información, sin importar el estado en el que esta se encuentre (tránsito, almacenada, durante su captura, etc.). El experto de seguridad (E. Spafford, 2013), afirma que “El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de hormigón, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él”.

Figura 2.1. Propiedades fundamentales de la Seguridad.

Fuente: (InfoSegur, 2014)

Confidencialidad

Según Beckers, K. (2015) la confidencialidad "es la propiedad, esa información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados". Esta debe garantizar que solo las personas autorizadas tienen acceso los datos de la organización y que estos no sean divulgados a entidades o individuos que no estén autorizados a manejar ese tipo información.

A ninguna persona le gusta pensar que su información privada de salud o información financiera caiga en manos de un extraño. A ningún propietario de un negocio le gusta la idea de que su información comercial patentada se divulgue a sus competidores. Deja en evidencia que la información es valiosa.

Integridad

La Revista de la segunda cohorte del doctorado en seguridad estratégica (2014) define la integridad como “Intenta que los datos almacenados por un usuario no sufran ninguna alteración sin su consentimiento”. Los datos o información de debe ser alterado por usuarios no autorizados, estos deben mantenerse tal cual como fue generado previamente. Solo los usuarios con la autorización requerida pueden alterar los datos.

La integridad de los datos es un requisito para que la información y los programas se cambien solo de manera específica y autorizada. En otras palabras, ¿la información es la misma que estaba destinada? Por ejemplo, si guarda un archivo con información importante que debe transmitirse a los miembros de su

organización, pero alguien abre el archivo y cambia parte o toda la información, el archivo ha perdido su integridad. Las consecuencias podrían ser desde compañeros de trabajo que se pierden una reunión que planeó para una fecha y hora específicas, hasta 50,000 piezas de máquinas que se producen con las dimensiones incorrectas.

La integridad y la confidencialidad están interrelacionadas. Si se revela una contraseña de usuario a la persona incorrecta, esa persona a su vez podría manipular, eliminar o destruir datos después de obtener acceso al sistema con la contraseña que obtuvo. Muchas de las mismas vulnerabilidades que amenazan la integridad también amenazan la confidencialidad. Sin embargo, lo más notable son los errores humanos. Las salvaguardas que protegen contra la pérdida de integridad incluyen el control de acceso, como el cifrado y las firmas digitales, los controles de proceso, como las pruebas de código, los controles de monitoreo, como el monitoreo de integridad de archivos y el análisis de registros, y los controles de comportamiento, como la separación de funciones, la rotación de funciones y formación.

Disponibilidad

Según la Revista de la segunda cohorte del doctorado en seguridad estratégica (2014) la disponibilidad “Se refiere a todas las técnicas dirigidas a mantener activo un servicio”. La información o los datos deben estar siempre disponibles para las personas, sistemas o procesos en cualquier momento que lo requieran.

Se podría decir que este componente de la triada de seguridad suele dejarse de lado cuando se piensa en seguridad. ¿Qué significa estar seguro? ¿Te sentirías seguro si estuvieras muy enfermo y no pudieras encontrar a tu médico? Si los sistemas y los datos están disponibles o no para su uso es tan crucial como la confidencialidad e integridad de los datos en sí. La disponibilidad es la garantía de que los usuarios autorizados pueden acceder a los sistemas y los datos cuando sea necesario. Si no podemos acceder a los datos que necesitamos, cuando los necesitamos, no estamos seguros.

Al igual que la confidencialidad y la integridad, valoramos la disponibilidad. Queremos que nuestros amigos y familiares estén allí cuando los necesitemos, queremos comida y bebida disponibles todo el tiempo, queremos nuestro dinero disponible, etc. En algunos casos, nuestras vidas dependen de la disponibilidad de estas cosas, incluida la información. Pregúntese cómo se sentiría si necesitara atención médica inmediata y su médico no pudiera acceder a sus registros médicos porque no están disponibles en el momento.

2.1.3 Estándares y marco de trabajo de la seguridad de la información, norma ISO/IEC 27001

“ISO (Organización Internacional de Normalización) es una familia de estándares que proporciona organizaciones con un marco general para políticas y estándares

de seguridad de la información" (SGSI, 2015). Esta serie es útil para todas las organizaciones que deseen proteger los activos de información, como informes financieros, información de empleados, propiedad intelectual o detalles del cliente. El ISO 27000: 2013 es una serie que consta de cuatro documentos de estandarización. En primer lugar, la familia contiene la ISO 27001: 2013 que contiene los requisitos para una seguridad de la información sistema de gestión. ISO 27002: 2013 es el segundo documento de la serie y contiene una lista de código de prácticas que garantizan la seguridad. El tercer documento en esta familia es ISO 27003: 2010, que está diseñado para proporcionar orientación durante la etapa de implementación del sistema de gestión de seguridad. El cuarto en esta serie es ISO 27004: 2009 que abarca El análisis de las medidas requeridas para un sistema de seguridad de la información.

ISO 27001: 2013 es el estándar adaptado para ofrecer orientación a través de los procesos de Establecimiento, implementación, mantenimiento y mejora continua de la información como sistema de gestión de seguridad. La norma considera varios tipos de organizaciones e industrias que abarcan sus tamaños y mercados. Es un amplio y genérico documento y su adopción e implementación debe ser una decisión estratégica. El proceso de adaptación del estándar debe estar influenciado por las necesidades de la organización y alineado a sus objetivos comerciales. La junta y la gerencia ejecutiva tienen libertad para seleccionar 23 de las políticas de seguridad que son apropiadas para el estado actual de seguridad y pueden complementar estas políticas con más opciones, también denominadas conjuntos

de control extendido. La evaluación exhaustiva de los riesgos de seguridad de la información de la organización es fundamental para para hacer una selección adecuada de controles.

2.1.4 Cómo trabaja el estándar ISO/IEC 27001

La mayoría de las organizaciones tienen varios controles de seguridad de la información. Sin embargo, sin un sistema de gestión de seguridad de la información (SGSI), los controles tienden a ser algo desorganizado y desarticulado, implementado a menudo como soluciones puntuales a situaciones específicas o simplemente como una cuestión de convención. Controles de seguridad en funcionamiento normalmente aborda ciertos aspectos de TI o seguridad de datos específicamente; dejando fuera de TI activos de información (como papeleo y conocimiento de propiedad) menos protegidos en el todo. Además, se puede gestionar la planificación de la continuidad del negocio y la seguridad física de manera independiente a la seguridad informática o de la información, mientras que las prácticas de Recursos Humanos pueden hacer poca referencia a la necesidad de definir y asignar roles de seguridad de la información y responsabilidades en toda la organización.

ISO / IEC 27001 requisitos para la administración:

- Examinar sistemáticamente los riesgos de seguridad de la información de la organización, tomando cuenta las amenazas, vulnerabilidades e impactos.
- Diseñar e implementar un conjunto de información coherente e integral, controles de seguridad y otras formas de tratamiento de riesgos (como evitar riesgos o transferencia de riesgos) para abordar aquellos riesgos que se consideran inaceptables.
- Adoptar un proceso de gestión global para garantizar que los controles para la seguridad de la información continúen satisfaciendo las necesidades de seguridad de la información de la organización en una forma continua.

Los beneficios clave de ISO / IEC 27001 son:

- Puede actuar como la extensión del sistema de calidad actual para incluir la seguridad.
- Brinda la oportunidad de identificar y gestionar los riesgos para la información clave.
- Brinda confianza y seguridad a los socios comerciales y clientes; actúa como una herramienta de marketing
- Permite una revisión y garantía independiente sobre la seguridad de la información.

2.1.5 Norma ISO/IEC 27002

“ISO / IEC 27002: 2013 proporciona pautas para los estándares de seguridad de la información organizacional y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización” (ISO,2013).

Mientras que otros conjuntos de controles de seguridad de la información pueden usarse potencialmente dentro de un ISMS ISO / IEC 27001, así como ISO / IEC 27002 (el Código de Práctica para la gestión de la seguridad de la información), estos dos estándares se utilizan normalmente juntos en la práctica. Los dominios cubiertos por ISO 27002 incluyen:

1. Política de seguridad
2. Organización de la seguridad de la información.
3. Gestión de activos
4. Seguridad de recursos humanos
5. seguridad física y ambiental
6. Gestión de comunicaciones y operaciones.
7. Control de acceso

8. Adquisición, desarrollo y mantenimiento de sistemas de información.

9. Gestión de incidentes de seguridad de la información.

10. Gestión de la continuidad del negocio

11. Conformidad

Las organizaciones que implementan un conjunto de controles de seguridad de la información en de acuerdo con ISO / IEC 27002 es probable que cumplan simultáneamente con muchos de los requisitos de ISO / IEC 27001, pero puede faltar parte de la gestión general elementos del sistema. También está que un certificado ISO / IEC 27001 de cumplimiento garantiza que el sistema de gestión de información la seguridad está en su lugar, pero dice poco sobre el estado absoluto de la seguridad de la información dentro de la organización. Los controles técnicos de seguridad como antivirus y cortafuegos (Firewall) no son normalmente auditado en auditorías de certificación ISO / IEC 27001: la organización esencialmente se presume que ha adoptado todos los controles de seguridad de la información necesarios desde el ISMS está en su lugar y se considera adecuado al cumplir los requisitos de ISO / IEC 27001. Además, la administración determina el alcance del SGSI para la certificación propósitos y puede limitarlo a, por ejemplo, una sola unidad de negocios o ubicación.

Otros estándares en la familia de estándares ISO / IEC 27000 proporcionan información adicional orientado sobre ciertos aspectos del diseño, implementación

y operación de SGSI, para ejemplo sobre gestión de riesgos de seguridad de la información (ISO / IEC 27005).

2.1.6 Otros estándares y marcos de trabajos relacionados

BS7799

"Es el código de práctica del estándar británico para la gestión de la seguridad de la información, se publicó en febrero de 1995" (Fisk 2002). Es un documento se refiere a los responsables de implementar y mantener la seguridad de TI, y proporcionar una base sólida para la política de seguridad de TI de una organización. El estándar BS7799 aborda una serie de áreas, incluidos los activos a proteger, el enfoque de la organización para la gestión de riesgos, los objetivos y controles, el grado de garantía requerido, los programas de concienciación sobre la seguridad y el desarrollo de políticas y procedimientos de seguridad. El mismo proporciona exploración para la gestión de seguridad de la información. "Las organizaciones que solicitan esta certificación se evalúan de acuerdo con este documento" (Bisson & Sain-Germain 2005).

NIST SP 800-53

NIST, Instituto Nacional de Estándares y Tecnología de EE. UU, Fundado en el 1901. Ha establecido una amplia recopilación de normas de seguridad de la información y mejores prácticas. NIST SP 800-53 es un estándar maduro y muy

completo y bueno para grandes empresas y especialmente para empresas y negocios con conexión en los Estados Unidos.

Los marcos de otras agencias gubernamentales de EE. UU. Han evolucionado desde el estándar NIST SP 800-53. Si se utiliza NIST SP 800-53, se puede cumplir con la “Federal Information Processing Standards” (FIPS) 200 o estándar de procesamiento de Información federal. NIST 800-53 cubre todos los riesgos IPS, como los pasos del marco de gestión que abordan los controles de seguridad. NIST 800-53 es específico para las agencias del gobierno de EE. UU., sin embargo, el marco podría aplicarse a cualquiera otra industria y particularmente por las compañías que buscan construir una seguridad de la información programa. “Las organizaciones federales de EE. UU. Utilizan el NIST 800-53 para cumplir con los requisitos del SGSI” (SearchSecurity 2017).

COBIT

“Control Objectives for Information and Related Technology” es un marco orientado al riesgo de alto nivel. Originalmente, fue utilizado por profesionales de gobierno de TI para ayudar reducir los riesgos técnicos. Más tarde se convirtió en un estándar para alinear los objetivos comerciales de TI. COBIT mapea los procesos centrales de TI de una manera que permita a los organismos de este, como los negocios de los ejecutivos ejecutan políticas y procedimientos clave. Cuando ITIL e ISO 27002 están enfocando solo en seguridad de la información, COBIT incluye procesos de gestión de TI al alcance. COBIT no se sigue tan ampliamente como otros estándares

de seguridad de la información, sin embargo, es se utiliza principalmente en la industria financiera para cumplir con estándares, como Sarbanes-Oxley (SOX). Es útil al establecer planes de continuidad comercial (Origin, 2017).

En cuanto a las fortalezas de COBIT, se puede mencionar que COBIT es administrado por ISACA (Asociación de Auditoría y Control de Sistemas de Información) que mantiene el estándar actualizado con el desarrollo de las tecnologías. Es un estándar aceptado a nivel mundial y se centra en más allá del alcance de seguridad de la información al que se limitan otros estándares. En consecuencia, COBIT se puede implementar fácilmente también parcialmente sin requerir un análisis y compromiso de la organización.

La debilidad de COBIT es que, aunque tiene un alcance amplio, también puede ser un factor limitante durante la implementación. Por diseño no está limitado a un área única, a menudo puede generar lagunas en cobertura. Por lo general, lo que le falta son consejos prácticos informativos (Origin, 2017).

ITIL

Es un conjunto de conceptos de gestión de servicios de tecnología de la información (ITSM) y la mejor práctica para el desarrollo de TI y operaciones de TI. Consiste en varios libros que cubren Prácticas específicas de gestión de servicios de TI. Uno de esos libros se enfoca en lo mejor prácticas en seguridad de la información.

ITIL sigue un modelo de proceso para controlar y gestionar operaciones basadas en el ciclo Plan-Do-Check-Act (PDCA) acreditado por W. Edwards Deming.

Contiene ocho TI principales Componentes de estándares y mejores prácticas de gestión de servicios: soporte de servicio, Prestación de servicios, gestión de infraestructura de TIC, gestión de seguridad, aplicación Gestión, gestión de activos de software, planificación para implementar el servicio Gestión e implementación a pequeña escala (Almunawar y Tuan, 2011).

ITIL se ofrece en cinco publicaciones principales, cada una de las cuales se ocupa de diferentes etapas en la TI ciclo vital. Mediante el proceso ITIL, uno puede generar documentación de procesos, tareas y listas de verificación, que están creando una línea de base para implementar controles y medir el éxito. Los procesos de ITIL son genéricos y, como tal, independientes de la organización. (Una comparación de COBIT, ITIL, ISO 27002 y NIST, 2017).

PCI DSS

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un estándar mundial de seguridad de la información. Está definido por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago. Es un marco estándar de alto nivel, diseñado originalmente para las compañías de pago, como Visa y MasterCard, que manejan información de tarjeta de crédito.

El estándar PCI DSS se creó para prevenir el fraude con tarjetas de crédito en los procesos y pagos con tarjeta de organizaciones de la industria. Aumentó los controles sobre los datos y la exposición de transacciones de pago. Los requisitos del estándar se refieren a todas las organizaciones que mantienen, procesan o

intercambian información de titulares de tarjetas de cualquier marca de tarjeta de pago. “Las organizaciones deben evaluar su cumplimiento por un asesor independiente llamado por un Asesor de Seguridad Calificado (QSA) o en el caso de una empresa más pequeña a través de un Cuestionario de Autoevaluación (SAQ)” (Almunawar y Tuan 2011).

PCI DSS es muy específico para el sector de tarjetas de pago y solo es relevante para la parte de pago de un sistema comercial. Por lo general, PCI DSS se implementa en asociación con algún otro marco de seguridad.

2.2 Certificaciones relacionadas a la seguridad de la información

2.2.1 Introducción

La entrada al campo se puede lograr a través del autoestudio, la educación universitaria o a través del instituto InfoSec o SANS’ SEC401 Security Essentials. Muchos colegios, universidades y formación en las compañías ofrecen muchos de sus programas en línea. Las certificaciones GIAC-GSEC y Security + son ambas respetadas certificaciones de seguridad de nivel de entrada. La seguridad certificada de los sistemas de información profesional (CISSP) es una muy respetada certificación de seguridad de la información de nivel medio a superior. La

profesión de seguridad de la información ha visto una mayor demanda de profesionales de la seguridad que tienen experiencia en auditorías de seguridad de redes, pruebas de penetración e investigación forense digital.

2.2.2 CISM

CISM (Certified Information Security Manager)

“Es una certificación ofrecida por ISACA que valida su conocimiento y experiencia en la gestión de equipos de seguridad de la información empresarial. Obtener la certificación CISM lo pone en alta demanda con empleadores de todo el mundo que reconocen el logro y la capacidad que representa la certificación CISM” (JEFF PETTERS, 2018).

2.2.3 CISSP

CISSP (Certified Information Systems Security Professional)

“Es otra certificación de seguridad de la información de gran prestigio, ofrecida por (ISC) 2. La certificación CISSP demuestra que tiene la experiencia para diseñar, implementar y administrar un programa de seguridad cibernética” (JEFF PETTERS, 2018).

2.2.4 SSCP

SSCP (Systems Security Certified Practitioner)

“La certificación SSCP demuestra que tiene las habilidades y conocimientos técnicos avanzados para implementar, monitorear y administrar la infraestructura de TI utilizando las mejores prácticas, políticas y procedimientos de seguridad establecidos por los expertos en seguridad cibernética en (ISC) “(ISC2, 2018).

2.2.5 CRISC

Certified in Risk and Information Systems Control (CRISC)

“Es una certificación independiente del proveedor que valida las habilidades de un individuo en los campos de control de sistemas de información y gestión de riesgos” (Techopedia).

2.2.6 Tabla de apreciación salarial al poseer certificaciones en la seguridad de la información

"Los trabajadores de TI con certificaciones de seguridad tienden a tener salarios promedio significativamente más altos, alrededor del 15 por ciento más, que aquellos sin ellos, según un estudio global de habilidades y salarios de TI realizado por Global Knowledge" (Morgan S, 2019).

Certification	U.S. & Canada			EMEA		
	Mean	Median	Count	Mean	Median	Count
Certified in Risk Systems and Control (CRISC)	$127,507	$122,900	159	$82,959	$82,000	65
Certified Information Security Manager (CISM)	$122,448	$120,000	276	$71,534	$68,500	252
AWS Certified Solutions Architect – Associate	$119,085	$118,350	304	$62,169	$60,000	202
Certified Information Systems Security Professional (CISSP)	$118,179	$115,000	304	$77,208	$74,500	116
Certified Information Systems Auditor (CISA)	$110,634	$106,059	588	$66,897	$64,750	416
PMP®: Project Management Professional	$105,324	$100,000	293	$53,521	$52,000	50
Citrix Certified Professional – Virtualization (CCP-V)	$102,353	$97,000	153	$65,850	$61,875	182
Citrix Certified Associate – Networking (CCA-N)	$98,583	$92,000	163	$58,080	$52,850	128
VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV)	$96,309	$90,000	159	$57,332	$53,300	139
Citrix Certified Associate – Virtualization (CCA-V)	$96,231	$92,000	241	$58,190	$55,000	244
MCSE: Server Infrastructure	$94,921	$92,000	329	$54,305	$50,775	250
ITIL® v3 Foundation	$93,638	$88,000	891	$56,601	$52,000	664
CompTIA Project+	$92,593	$88,000	205	$48,275	$50,000	27
CCNP Routing and Switching	$90,945	$89,550	193	$37,114	$28,500	275
MCSA: SQL Server	$90,303	$83,750	188	$48,632	$45,000	125
MCSA: Windows Server	$89,941	$84,000	628	$50,042	$45,500	591
CompTIA Security+	$87,666	$83,000	678	$53,490	$46,944	101
CCNA Security	$84,652	$80,000	185	$38,193	$28,440	164
CCNA Routing and Switching	$80,873	$75,000	799	$32,873	$25,000	825
CompTIA Network+	$79,435	$75,000	760	$44,747	$38,498	140

Figura 2.2: Certificaciones que pagan más alto

Fuente: (Helpnetsecurity, 2019)

2.2.7 Demanda laboral para profesionales en la seguridad de la información

Cybersecurity Ventures predice que habrá 20 millones de empleos de seguridad cibernética quedarán sin cubrir para 2021, frente a 1 millón de vacantes en 2014.

Según Crane, C (2019) los 5 puesto de trabajo sobre seguridad de la información más demandado hoy en día son:

- **Analista / ingeniero de seguridad cibernética** - Planificar, monitorear, implementar o actualizar medidas de seguridad que protejan las redes de computadoras, la infraestructura electrónica y los archivos digitales.
- **Consultor de seguridad cibernética -** Evaluando los sistemas informáticos, las redes y el software en busca de vulnerabilidades, así como describiendo las mejores soluciones de seguridad cibernética para la implementación.
- **Administrador de sistemas** - Soporte técnico, monitoreo diario del sistema, respaldo de datos, administración de infraestructura de seguridad de TI y otras responsabilidades.
- **Ingeniero de sistemas** - Asegurando los niveles más altos de infraestructura y disponibilidad de sistemas al administrarlos, monitorearlos, probarlos y mantenerlos a través de una variedad de herramientas.

- **Analista de vulnerabilidad / probador de penetración** - Hurgando, presionando e intentando romper las defensas de una red o sistema para identificar vulnerabilidades que los ciberdelincuentes pueden explotar.

2.3 La seguridad de la información en el tiempo

2.3.1 La seguridad de la información a través del tiempo

Durante la Primera Guerra Mundial, el Sistema de clasificación de niveles múltiples se desarrolló teniendo en cuenta la sensibilidad de la información. Con el comienzo de la Segunda Guerra Mundial, se realizó la alineación formal del Sistema de Clasificación. En 1936, Alan Turing fue quien descifró con éxito la máquina Enigma, que fue utilizada por los alemanes para cifrar los datos de la guerra.

Durante los primeros años de la informática, los mainframes (Supercomputadoras) utilizados por los militares se conectaron a través de líneas telefónicas dedicadas para formar ARPANET, el precursor de la INTERNET moderna. Si bien esto permitió una fácil sincronización de la información entre los centros de datos, también proporcionó puntos inseguros entre los centros de datos y el público. Esta vulnerabilidad se soluciona asegurando ubicaciones físicas y hardware. Un grupo de trabajo formado por ARPA (Agencia de Proyectos de Investigación Avanzada)

para estudiar la seguridad de INTERNET en 1967 encontró que este método era inadecuado, y el Informe Rand R-609 determinó que se deben tomar medidas adicionales para mejorar la seguridad. Este informe marcó una etapa importante en el desarrollo de la seguridad de la información actual.

Algunos de los primeros esfuerzos de seguridad se centraron en el sistema operativo mainframe. MULTICS (Servicio multiplexado de información y computación) fue un esfuerzo del MIT, Bell Labs y General Electric para incorporar la seguridad en los sistemas operativos de mainframe utilizando múltiples niveles de seguridad y contraseñas. Se volvió obsoleto cuando llegó la era de las computadoras personales.

En 1989, la Universidad Carnegie Mellon estableció el Instituto de Redes de Información, el primer centro estatal de investigación y educación dedicado a la creación de redes de información. De la academia surgieron disciplinas de seguridad informática, seguridad de la información y aseguramiento de la información junto con numerosas organizaciones profesionales durante los últimos años del siglo 20 y los primeros años del Siglo 21.

Las personas encontraron diferentes formas de penetrar las primeras redes telefónicas y computadoras. En la década de 1970, los "phreakers" explotaron vulnerabilidades en la red telefónica para hacer llamadas telefónicas gratuitas de larga distancia. El FBI arrestó a un grupo de seis adolescentes en Milwaukee a principios de la década de 1980 por piratear 60 redes informáticas diferentes. Los

Milwaukee 414 (nombrados por su código de área) lo hicieron por un desafío, pero cuando el “First National Bank of Chicago” fue pirateado por $ 70 millones de dólares, quedó claro que esto no era solo un pasatiempo para los niños.

Más computadoras se convirtieron en objetivos en la década de 1990 a medida que más personas pusieron su información personal en línea. El crimen organizado descubrió que la piratería informática podría proporcionar una fuente lucrativa de ingresos. Para el año 2000, INTERNET se convirtió en una multitud de redes no seguras, cada una de las cuales ofrecía un posible “exploit”. Esta red no segura continúa creciendo. Las amenazas ahora provienen del crimen organizado, de empresas que usan técnicas de "sombrero negro" y de estados extranjeros que desean robar información clasificada del gobierno. Incluso se sabe que algunas corporaciones piratean las redes de sus competidores para robar o sabotear información vital.

2.3.2 La seguridad de la información hoy

Un estudio realizado por Karpesky Lab (2018) “dirigido a 7,993 empleados de tiempo completo preguntó sobre las políticas y responsabilidades para la seguridad de TI corporativa y también reveló que 24% de los empleados cree que no hay políticas establecidas en sus organizaciones en absoluto. Curiosamente, parece que el desconocimiento de las reglas no es excusa, ya que aproximadamente la

mitad (49%) de los encuestados piensa que todos los empleados, incluidos ellos mismos, deberían asumir la responsabilidad de proteger los activos de TI corporativos contra las amenazas cibernéticas".

Los consumidores en línea de hoy en día lidian habitualmente con spyware, adware y malware, que presentan amenazas que van desde la simple molestia hasta el robo de contraseñas. Tomar medidas para aumentar la seguridad de los datos personales, limitar la exposición de datos y compartir información sobre amenazas en línea es una forma en que la seguridad de la información personal ha evolucionado. El mayor uso del software antivirus es otro. Las agencias gubernamentales y las empresas invierten habitualmente millones de dólares para estudiar las amenazas mientras prueban y mejoran constantemente la seguridad de la información.

¿Qué amenazas hay en el horizonte? La piratería patrocinada por el estado ya es una industria en sí misma. La privacidad individual puede disminuir a medida que los gobiernos y los organismos encargados de hacer cumplir la ley supervisan de forma agresiva el correo electrónico y la comunicación personal. Es probable que las aplicaciones móviles y los proveedores de servicios también estén bajo un número creciente de ataques.

Estos problemas son molestos por la mentalidad de muchos grupos que creen que las leyes de derechos de autor y propiedad intelectual representan una limitación o infracción de sus derechos.

2.4 Manejo del Riesgo

2.4.1 El riesgo

"La gestión de riesgos es el proceso de identificar vulnerabilidades y amenazas a los recursos de información utilizados por una organización para lograr los objetivos del negocio, y decidir qué contramedidas, si las hay, tomar para reducir el riesgo a un nivel aceptable, basado en el valor del recurso de información a la organización " (Whitman & Mattord, 2008). En este proceso se le otorga a la organización el equilibrio entre sus operaciones y costo financiero de medidas de salvaguarda y lograr su objetivo de misión. No está limitado por la tecnología de la información y la regla de seguridad. Es un proceso que ayuda a las empresas a cumplir sus objetivos y proteger los activos de la organización. Ayuda a identificar, controlar y reducir el impacto de las vulnerabilidades.

El objetivo principal de este proceso es minimizar el riesgo mientras realizar pocas actividades o funciones que puedan ser aprobadas por la alta gerencia. La naturaleza omnipresente de las tecnologías de comunicación e información significa que los riesgos pueden convertirse en una complicada malla de interdependencias inmanejables.

De acuerdo con koronios (2006) hay principalmente cinco procesos en la gestión de riesgos que son:

- Identificar los peligros.
- Evaluar esos peligros
- Desarrollar controles y tomar decisiones de riesgo
- Implementar controles
- Monitorear y evaluar la situación

Este patrón se refleja en una serie de modelos más formales del proceso. Por ejemplo, Koronios (2006) sugirió los siguientes pasos:

- Recopilar información sobre el riesgo.
- Preparar alternativas.
- Tomar decisiones.
- Tomar acción.
- Mirar lo que pasa.

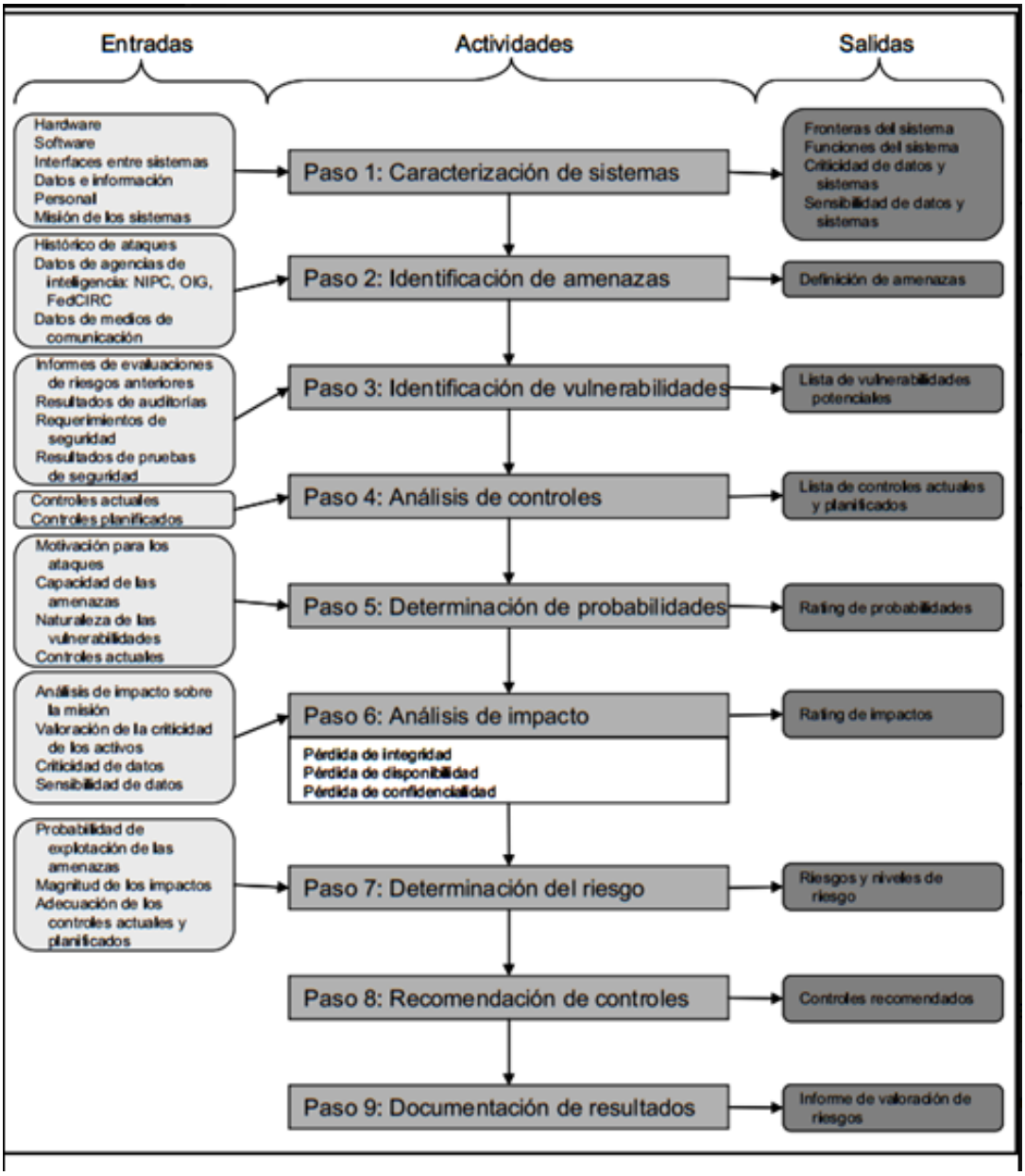


Figura 2.3: Diagrama de flujo de metodología de evaluación de riesgos

Fuente: (National Institute of standards and technology, 2002)

2.4.2 Identificación del riesgo

"El primer paso para identificar los riesgos es comprobar todos los elementos, activos y recursos que pertenecen al sistema informático o que son necesarios para su funcionamiento y que, por lo tanto, podrían estar en riesgo" (Whitman y Mattord, 2008). Las clasificaciones del sistema son las siguientes:

- **Hardware**, Procesador, unidades de disco magnético, terminales, módems, gabinetes de almacenamiento.
- **Software**, Sistema operativo, compiladores, programas de aplicaciones, rutinas de auditoría, volcados de seguridad, copias de seguridad.
- **Datos y medios**, Archivos maestros, datos de entrada, archivos de salida, documentación de software, documentación de procedimientos operativos, paquetes de discos, cintas magnéticas, tarjetas.
- **Comunicaciones**, Circuitos telefónicos, servicios postales, servicios privados de transporte de datos, redes, etc.
- **Medio ambiente**, Estructura y accesorios del edificio, fuentes de alimentación, planta de aire acondicionado, servicios de limpieza, instalaciones de restauración, servicios de ascensor.
- **Organización**, Política y estructura de gestión, personal (TI, técnico, administrativo y secretariado).

- **Apoyo**, Personal de mantenimiento, auditores, consultores, servicios de entrega.

"Después de haber preparado la lista que cubren todos los elementos en riesgo, cada elemento, activo o recurso debe considerarse en relación con los tipos de riesgo (por ejemplo, destrucción accidental, divulgación deliberada, etc.) y los factores de riesgo (por ejemplo, incendio, inundación, daño malicioso, acción industrial, etc.)" (Nicholas, 2002). Además, al considerar los posibles riesgos, debe tenerse en cuenta que un solo evento puede poner en riesgo más de un elemento y puede resultar de la interacción en ocurrencia de riesgos con los diversos elementos que constituyen un sistema informático en conjunto. El riesgo puede clasificarse en términos generales de la siguiente manera:

- **Pérdidas de propiedad**, Destrucción, daño, pérdida, robo, contaminación.
- **Pérdidas de responsabilidad**, Incumplimiento de contrato, incumplimiento de derechos de autor, difamación, calumnia.
- **Pérdidas de personal**, Lesiones por muerte, enfermedad, acción industrial, renuncia, licencia.
- **Pérdidas finales**, deudas incobrables, empleados deshonestos.
- **Pérdidas por interrupción de negocios**, flujos de efectivo retrasados, aumento del costo de trabajo, cláusulas de penalización.

2.4.3 Análisis y evaluación de riesgos

"El análisis de riesgos se refiere a evaluar la posibilidad y la magnitud del riesgo. Se utiliza para reducir la posible aparición de un riesgo, las consecuencias del riesgo y los métodos utilizados para manejar cada una de esas consecuencias individuales" (Stulz, 2003). Esto implica un medio de evaluar o medir el riesgo y las consecuencias de su ocurrencia. Existen varias técnicas para hacerlo, algunas cualitativas y otras cuantitativas.

Un valor cuantitativo, que puede derivarse para un riesgo particular, es el de la pérdida esperada. Se puede expresar en unidades monetarias, como dólares por año, y se obtiene multiplicando el valor medio de la pérdida en términos monetarios por la frecuencia con la que se espera que ocurra el riesgo por año. Aunque generalmente se elige un intervalo de tiempo de un año por razones obvias de conveniencia, se pueden usar otros intervalos de tiempo según corresponda. Si se utiliza la pérdida esperada para establecer tanto la gravedad del riesgo como la necesidad resultante de contramedidas, entonces los valores de las dos cantidades involucradas “pérdida” (también conocida como impacto) y “frecuencia” son obviamente críticos. Una vez que los valores de la pérdida esperada se han estimado para cada riesgo, los riesgos deben enumerarse en orden de disminución del valor de la pérdida esperada.

Como regla general, cuanto mayor sea el valor de la pérdida esperada, más importante es contrarrestar el riesgo correspondiente. Sin embargo, al seleccionar

las contramedidas apropiadas, se debe tener en cuenta su eficacia para reducir la pérdida esperada y su costo de implementación. Lo que se debe buscar es un conjunto de contramedidas que, teniendo en cuenta la cantidad de dinero disponible, se reduzca al mínimo el valor de la suma de las pérdidas esperadas debido a todas las ocurrencias de riesgos y el costo de las contramedidas.

Habiendo considerado los posibles riesgos y evaluado la probabilidad de que ocurran y la gravedad de sus consecuencias, se debe prestar atención a las posibles formas de abordar la situación. “Las medidas deben seleccionarse para manejar los riesgos individuales y cumplir con las contingencias. Las formas en que estas medidas deben implementarse, monitorearse, revisarse y, cuando sea necesario, actualizarse, también deben decidirse" (O'Harrow, 2003).

2.4.4 Norma ISO/IEC 27005

El estándar ISO / IEC 27005 es la referencia principal de este documento para el riesgo de seguridad de la información gestión en una organización, proporcionando pautas para los requisitos de un SGSI de acuerdo con ISO / IEC 27001.

“De acuerdo con este estándar, el proceso de gestión de riesgos en seguridad de la información puede aplicarse a una organización completa como parte de la organización (es decir, departamento, servicio, ubicación), sistema de información

(existente o planificado), así como aspectos particulares de control (es decir, plan de continuidad del negocio)” (ISO, 2011).

Un enfoque repetitivo en la realización del proceso de evaluación de riesgos puede aumentar la profundidad y los detalles de evaluación en cada iteración. "Esta norma define un proceso de gestión de riesgos de seguridad de la información de Plan, Do, Check, Act, que consta de los siguientes pasos" (ISO, 2011):

Plan

- Establecer el contexto para la gestión de riesgos de seguridad de la información. Esto incluye seleccionar criterios para evaluar el riesgo, determinar el impacto y aceptar el riesgo; definir el alcance del activo y los límites sobre los cuales se llevará a cabo la gestión de riesgos (por ejemplo, qué aplicaciones se evaluarán); y determinar la estructura organizativa, los roles y las responsabilidades para realizar la gestión de riesgos.
- La evaluación de riesgos implica realizar un análisis de riesgos para identificar los riesgos en términos de activos y su valor, amenazas, controles existentes, vulnerabilidades que podrían explotarse y consecuencias debidas al impacto y la pérdida en caso de que los riesgos se realicen. La magnitud de las posibles consecuencias se estima en términos cualitativos, cuantitativos cuando sea posible, teniendo en cuenta la probabilidad de ocurrencia de incidentes. los riesgos se priorizan frente a criterios de evaluación y objetivos organizacionales.

- Desarrollar un plan de tratamiento de riesgos que identifique los controles necesarios para reducir, retener, evitar o transferir los riesgos identificados. Los controles se seleccionan realizando un análisis de costo / beneficio, teniendo en cuenta los criterios. El riesgo residual cae dentro de tolerancias de riesgo aceptables.

- La decisión de aceptar los riesgos identificados y las responsabilidades de cada decisión se documentan formalmente. Los gerentes responsables revisan y aprueban los planes de tratamiento de riesgos propuestos. La información sobre el riesgo se comparte entre los tomadores de decisiones y las partes interesadas clave para proporcionar seguridad y apoyar la toma de decisiones continua.

Hacer

- Implementar el plan de tratamiento de riesgos.

Chequear

- Controlar y revisar continuamente los riesgos, incluidos todos los factores relevantes (incluido el valor de los activos, los impactos, las amenazas, las vulnerabilidades y la probabilidad). Identificar y actuar sobre cualquier cambio que agregue nuevos activos, amenazas y vulnerabilidades o que actualice las dimensiones de riesgo existentes, las prioridades y el tratamiento.

Actuar

• Mantener y mejorar el proceso de gestión de riesgos de la información a través del monitoreo continuo y revisión.

“Según esta norma, todas las actividades de gestión de riesgos deben estructurarse de la siguiente manera” (ISO,2011):

- **Entrada**: identificación de la información necesaria para realizar la actividad.
- **Acción**: describe la actividad.
- **Guía de implementación**: proporciona una guía sobre cómo realizar la actividad. Es necesario que se considere que la orientación propuesta no se ajusta a todos los casos.
- **Salida**: identificación de cualquier información derivada de la actividad de ejecución.

2.5 Controles y sus implementaciones

2.5.1 Los controles

El control puede definirse como la evaluación y medición de efectividad de los protocolos activos dentro de un sistema, organización y entidad. Los mismos sirven

para detectar posibles desvíos o fallas respecto de lo planteado. Asimismo, estos desvíos serán corregidos mediante la utilización de un sistema o contramedida determinada cuando los mismos excedan los límites admitidos.

Los controles también pueden definirse como la regulación de actividades de acuerdo con los requerimientos que se han planteado. No obstante, todas estas regulaciones son establecidas y determinadas por un equipo de personas con la capacidad lógica y coherente de pensar a futuro en cuanto a riesgos y prevención de los mismo se refiere. Ante todo, lo antes planteado, es claro destacar que los controles sin importar el los rigurosos que sean comparten un objetivo en común, asegurar el cumplimiento de los demás objetivos básicos de un sistema u organización.

Para que los controles sean efectivos se necesita tener total conocimiento de las acciones ejecutadas dentro de los protocolos a seguir, la correlación existente entre estas acciones respecto al objetivo y la eliminación de los obstáculos que puedan trabar el logro de las metas establecidas.

Los controles pueden adquirir diversos significados dependiendo del contexto en que se apliquen, es por ello que a continuación veremos los diferentes ambientes donde pueden ser implementados:

Organizaciones: Como bien conocemos las mismas son una estructura de personas y bienes que persiguen una meta en común. Dentro de estas los controles pueden ser:

Control coercitivo (físicos): Cuando a la hora de aplicar la sanción o contramedida afecta directamente al cuerpo humano dentro de esta.

Control utilitario (materiales): Si al momento que se cumplen los objetivos previamente planteados se utilizan recompensas ya sean monetarias o con objetos que posean algún valor tangible. los mismos no se entregan si no se cumplen con las metas establecidas. Su principal símbolo es el dinero.

Control normativo (simbólicos): Dentro de este se busca el seguimiento de las reglas o protocolos implantados a través de la adhesión de los individuos a un credo, ideales u otros símbolos.

Área de administración: Describimos administración como el conjunto de tareas o funciones que se llevan a cabo para dirigir y marchar en la dirección más conveniente. En cuanto al control en la administración se refiere, posee tres elementos principales:

Normas que representan una actuación deseada: Estas reglas pueden ser tangibles o intangibles, específicas o vagas. Sin embargo, si las personas correspondientes no entienden los resultados que se desean obtener, las mismas no sirven de nada.

Comparación de los resultados efectivamente logrados contra las normas: De esa comparación surge una evaluación, la cual es realizada por alguien competente que posteriormente informa a la Dirección Superior con autoridad para tomar las decisiones correctivas.

Acciones correctivas: Que como resultado de la evaluación realizada se rectifican los errores detectados para obtener los resultados planeados. Estas acciones pueden ser a corto, mediano y largo plazo.

Este último tipo de control, si bien refleja aspectos de los controles "Normativos" por el tipo de sanción que implican los incumplimientos, en definitiva, es "Utilitario" y refleja el concepto del control administrativo en su forma más amplia. En este caso, primero existe una norma, luego una comparación entre plan y acción, una evaluación de los desvíos y luego la corrección por parte de la autoridad competente.

Área cibernética: Considerada como la ciencia de la comunicación entre humanos y máquinas, este apartado no difiere mucho de las otras definiciones anteriores. Se entiende que como todo control hay normas o conductas a seguir, asimismo, un mecanismo o sistema que detecta cuando las mismas no son cumplidas y por último se aplican las contramedidas o correcciones correspondientes.

Elementos del control.

Fuente anónima, de los conceptos anteriores surge que podemos concebir al control como parte de un todo, o como un subsistema dentro de un sistema mayor, superando al concepto clásico, estático, como una etapa más dentro del proceso administrativo típico de planificar, administrar y controlar.

A partir de esta concepción del control que lo coloca como un subsistema dentro del sistema administrativo de una organización, a partir de ahí podemos sacar a relucir los elementos que componen este subsistema:

Variables para controlar: Es el punto básico de todo monitoreo o control pues sin las mismas no tendríamos algo que controlar realmente. Cuando un sistema marcha en perfecto estado es en el momento que cumple con todos sus objetivos, y para poder controlar dicho sistema hay que seleccionar del total de operaciones que corren dentro del sistema, aquellas más relevantes, cuya medición trace las pautas del funcionamiento total del sistema.

Mecanismo o sistema de monitoreo: El mismo debe ser totalmente capaz de medir las variables puesta bajo su control en los intervalos de tiempo seleccionados por el propio administrador del sistema.

Comunicación: Conocida como el intercambio de información entre dos o más participantes, es parte fundamental para nuestra vida y en un sistema de control no sería la excepción. La misma es primordial a la hora de la detección de los errores, ya que, estos necesitan ser notificados para su pronta intervención. Ya que, el control es para evaluar y corregir, es clave que, a la hora de diseñar la red de comunicación, se tomen en cuenta sus dos grandes desafíos; la longitud y la rapidez en el flujo de la información pertinente.

Unidad central de control: La misma es utilizada para comparar lo planeado con lo ejecutado, de esta manera se detecta la magnitud y el sentido de los desvíos.

(Fuente anónima) La determinación de las causas y la adopción de las medidas correctivas son actividades de los centros de planeamiento y dirección, no del centro de control. cabe destacar que algunos sistemas de control implementan un subsistema o instrumento corrector para que el sistema vuelva al rango de los parámetros planeados, a esto se denomina sistema de control automático.

Importancia.

Ihndira Elena Fontt Establece que, las medidas para corregir las actividades, de tal forma que se alcancen los planes exitosamente. Se aplica a todo: a las cosas, a las personas y a los actos. Determina y analiza rápidamente las causas que pueden originar desviaciones para que no vuelvan a presentarse en el futuro. Localiza los sectores responsables de la administración, desde el momento en que se establecen medidas correctivas. Proporciona información acerca de la situación de la ejecución de los planes, sirviendo como fundamento al reiniciarse el proceso de la planeación. Reduce costos y ahorra tiempo al evitar errores. Su aplicación incide directamente en la racionalización de la administración y consecuentemente, en el logro de la productividad de todos los recursos de la empresa.

2.5.2 Tipos de control y sus objetivos

Después de una basta definición y clasificación de sus elementos, es propicio tipificar los controles existentes en la seguridad de la información. Son tres principales vertientes:

Controles preventivos o preliminares: Estos reducen la frecuencia con que ocurren las causas propias del riesgo. Este tipo de control tiene como característica principal que incluye la creación de políticas, procedimientos y reglas diseñadas para asegurar que las actividades planeadas serán ejecutadas con propiedad. Dentro del mismo se permite cierto margen de violación antes de ejecutar la acción correctiva.

Controles detectives: Según Sixto Ronquillo, son aquellos que no evitan que ocurran las causas del riesgo, sino que los detecta luego de ocurridos. Por otro lado, son los más importantes para un auditor. Los mismos, sirven para evaluar la eficiencia de los controles preventivos.

Controles correctivos: Estos ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectives sobre los controles correctivos. Esto último debido a que la corrección de errores es por sí misma una actividad altamente propensa a generar más errores.

2.6 Ataques informáticos

2.6.1 ¿Qué es un ataque informático?

Ataques, los podemos presenciar de diferentes maneras, escalas y contextos, ya sea en el ámbito militar, médico o informático (en el cual nos enfocaremos). Sin embargo, todos poseen una cualidad en común; emprender una ofensiva, perjudicar o destruir un objetivo previamente establecido. Una vez teniendo claro lo antes dicho, tenemos como definición plana que un ataque ¨Es la acción y efecto de atacar y el concepto suele utilizarse para nombrar una hostilidad o agresión¨. (Merino., 2010). No importa cuál sea el ambiente en el que estemos presentes, somos más vulnerables a diversos ataques de lo que en ocasiones podemos imaginar.

Tal vez en este momento se estén diciendo a sí mismos o preguntando ¨si, pues claro que sabemos que es un ataque. Pero ¿Cómo surgen? ¿Cómo los puedo evitar? O la clásica y más común de todas ¿Por qué a mí? ¨. Pues, es de esperarse, un día estás tomando aquella taza de café que tanto disfrutas y al día siguiente estás siendo atacado por una persona al otro lado del mundo la cual se lleva toda la información de tus clientes. Ya sea de manera interna o externa por algún agente malicioso o entidad los ataques y más aún los informáticos son más frecuentes de lo que muchos de ustedes piensan.

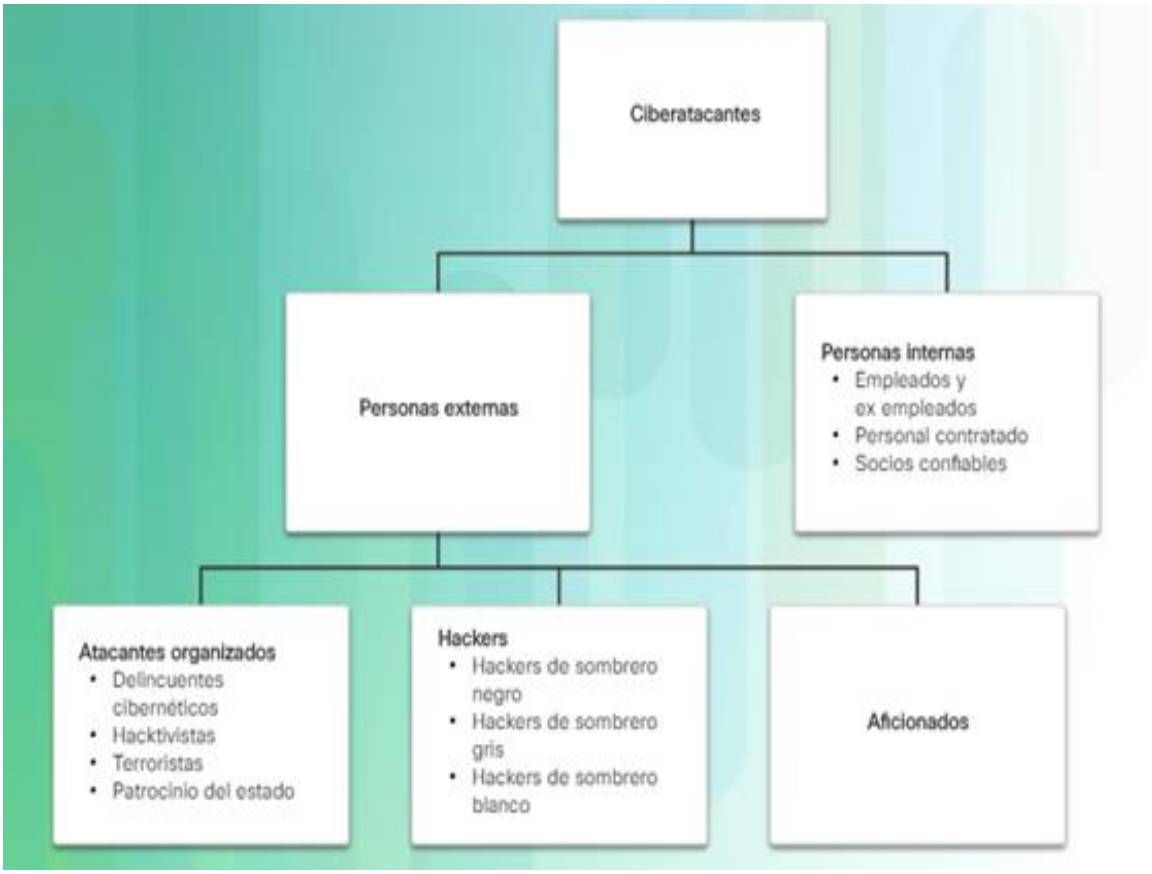


Figura 2.4: Diagrama de Ciberataques

Fuente: (Cisco Netacad)

Ciberataque (ataque informático), el Instituto Español de Estudios Estratégicos lo define como: actos que los delincuentes informáticos llevan a cabo como parte de sus actividades delictivas virtuales. No obstante, un ataque informático no siempre ocurre de manera virtual, pues también tenemos uno de los eslabones más débil en la cadena de la seguridad de la información; el factor humano.

Si hay algo que se debe poner en práctica y de preferencia antes de que el ataque informático toque la puerta, son las medidas para evitarlo o contenerlo de cierta manera. Teniendo claro que la prevención en todos los aspectos es más factible que la intervención violenta a la hora de ejecutar una contramedida. Partiendo de esto y ubicando en el contexto deseado, podemos describir medida como: ¨disposición, normativa implementada para evitar, contrarrestar o eliminar una acción o suceso no deseado¨.

2.6.2 Objetivo de los ataques informáticos

Si eres de los que piensan que un grupo de ¨nerds¨ informáticos irá tras de ti o tu organización solo por ver cómo te vuelves loco mientras ellos lo disfrutan, probablemente estés equivocado. Según el Ponemon Institute of Michigan, 70 % de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017. Y no es para menos, día tras día los factores de riesgo se van actualizando en todas las organizaciones; considerando que, según el portal ZDNET, a una compañía le toma entre 6 meses o 197 días, detectar una brecha de seguridad. Entonces, ¿Cómo estás tan seguro de que tu organización no posee ninguna brecha de seguridad en estos momentos?

Tal vez aún estés procesando la información anterior, pero a continuación vamos a apreciar y conocer más a fondo algunos de los objetivos más comunes.

Datos e información: Sin duda alguna lo más importante en el mundo actual en que vivimos, no es para menos que ocupe el primer lugar. Pero dejémonos de rodeos, la técnica superior en programación y analista de sistemas computarizados, Patricia Dip, en su artículo ¨tecnología e informática¨ publicado en 1 de agosto del 2009 dice que, los datos son números, letras o símbolos que describen objetivos, condiciones o situaciones. También, pueden ser descriptos como el conjunto básico de hechos referentes de una persona o cosa que posteriormente son utilizados para la toma de decisiones. Partiendo de esto en la computación, los datos se representan como pulsaciones electrónicas a través de la combinación de circuitos, denominados señal digital y pueden ser:

- Alfabéticos (A-Z)
- Numéricos (0-9)
- Caracteres especiales (%, *, /, $, #)

¿Por qué tus datos e información son un objetivo? Fácil, si un agente malicioso los obtiene, puede cambiar su identidad en línea, cometer delitos informáticos bajo tu nombre y peor aún robarte de una manera rápida y efectiva, sin dejar rastros. Así que, ya sabes porque ataques a organizaciones no tan ¨lucrativas¨ son tan importantes, si, por la información almacenada sobre sus clientes.

Dinero: ¿Qué haríamos sin él? Desde satisfacer nuestras necesidades básicas hasta poder adquirir nuestro propio avión privado, sin duda alguna mueve al mundo por completo. Tal vez en estos momentos están pensando ¨bueno, la gran parte de

las organizaciones lo conservan en la bóveda súper segura ubicada tres pisos bajo tierra¨, pues tengo para decirles que están equivocados. Según Brett Scott en su artículo ¨La guerra contra el dinero en efectivo¨ establece que, la cantidad de dinero en efectivo circulando por las calles se calcula entre el 1 % y un 8 % ¿Dónde se encuentra todo el dinero restante? Pues sí, es totalmente electrónico, así que no es de sorprender que un grupo de hackers quiera agregar unos cuantos ceros a sus cuentas bancarias.

Ideales religiosos: Si, sé que suena extraño, un grupo de hacker que ¨profesan la palabra de Dios¨ ¿Cuándo llegamos a esto? Sin embargo, existe, recordando que cada persona tiene sus propias creencias, es común que alguien quiera llevar sus ideales al siguiente nivel. Atacando páginas web con publicidad o tratar de reclutar personas vía las mismas, son las formas más comunes.

Diversión: ¿Qué? ¿Acaso pensaron que esos chicos\as que llaman ¨Nerds¨ solo se entretienen viendo su serie favorita y jugando videojuegos? Tal vez sí. Sin embargo, para algunos reírse a carcajadas luego de robar información privilegiada de una empresa multinacional suena mucho más interesante que solo sentarse durante horas frente a la tv un sábado por la noche. Por lo tanto, la diversión no deja de ser de los fines más comunes en este ámbito.

Venganza: suponiendo que todos la hemos sentido en nuestro interior en más de una ocasión, por consiguiente, es necesario marcarla como motivo u objetivo suficiente para cometer un ataque. La misma ha sido precursora de innumerables

atentados contra la seguridad de la información a través de los años. A continuación, un pequeño ejemplo:

Un sujeto X y su familia viven tranquilamente en una de las mejores zonas residenciales de la ciudad, poseen una casa amplia y con un gran jardín, sus hijos se la pasan de maravilla. El bloque donde residen está siendo adquirido lentamente por una gran constructora internacional, la cual poco a poco ha ido comprando las casas y terrenos aledaños para la construcción de un gran centro comercial. Al final de un largo proceso legal la compañía constructora consigue desalojar al sujeto X y su familia de su hogar de una manera para nada legitima y con mucho dinero de por medio. En los tres meses siguientes y viviendo en un departamento dos veces inferior, el sujeto X emprende un plan para dañar de cierta manera aquella compañía constructora que le arrebató su lugar feliz y el de su familia. Un ataque de ingeniería social, consiguiendo nombres y claves de acceso de usuarios categoría 1, al cabo de 6 meses la compañía es atacada desde adentro y uno de los administradores de los sistemas figura como único y principal responsable, pero ya el daño está hecho, las pérdidas son millonarias.

Hacktivismo: Según Paula Rochina, no es más que una forma de protesta realizada por aficionados o profesionales de la seguridad informática (Hackers) con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general (ejemplo: cambio climático), haciendo uso de los fallos de seguridad de las entidades o sistemas gubernamentales. Es decir, surge como un nuevo fenómeno cuya base ideológica es el intercambio y apertura del conocimiento

y la vulneración de derechos de propiedad intelectual que aprisionan el desarrollo del conocimiento.

Los mismos tienen como fin normalmente temas políticos y sociales, por lo habitual situaciones creadas por gobiernos. Las personas que toman este tipo de acciones en gran medida han intentado por diferentes vías llevar su mensaje, pero ha sido totalmente fallido. no tienen que ser personas asociales y mucho menos excluidos de la sociedad, una persona Hacktivista puede estar compartiendo con nosotros en cualquier momento, pero siempre con su idea firme e incorruptible.

2.6.3 Metodología de los ataques informáticos

Análisis, inspección y clasificación del objetivo: En este proceso sacamos a relucir todos los métodos que se pueden tener a mano para clasificar al objetivo de acorde a sus características. Siempre que hagamos una correcta distribución de las peculiaridades del blanco podemos estar casi seguros de que el método o vector a utilizarse será bastante efectivo a la hora del ataque. Es por ello que, es bastante importante poner tanto énfasis en este apartado; de lo contrario, no sería posible un ataque exitoso.

La fase de análisis o reconocimiento la podemos subdividir en dos principales vertientes: pasivo y activo.

Reconocimiento pasivo: requiere la compilación de datos o información sobre el objetivo seleccionado, pero, sin tan siquiera la sospecha de la persona o entidad afectada. De esta manera, esta opción sería bastante factible; ya que, la recopilación se realiza de manera incógnita.

Reconocimiento activo: Este se caracteriza porque para el mismo, se realiza una búsqueda de datos e información más agresiva. Por lo tanto, el mismo conlleva mayor factor de riesgo que el anterior.

Escaneo, codificación y alineamiento del objetivo: Este paso de caracteriza por ser vital a la hora de su ejecución, pues dentro del mismo se llevan a cabo las acciones necesarias para posteriormente saber con qué vector se realizará el ataque o mejor aún, de qué manera se utilizará dicho vector a la hora del ataque. Así que lo podemos definir llanamente como: adquirir toda información recopilada durante el reconocimiento y así de cierta manera alinear, preparar y probar toda herramienta que se considere eficaz para el ataque. Destacando con la peculiaridad que cualquier mínima información que se obtenga en esta fase del objetivo puede ser crucial para todos los procesos restantes.

Obtener el acceso e infiltración: O como le quieran llamar, sin duda alguna, la más esperada por todo agente malicioso. Puesto que, aquí es donde se evidenciará si todo el trabajo previo valió la pena. En esta, toda vulnerabilidad expuesta en las dos fases anteriores ahora es explotada a merced del atacante. Teniendo en cuenta que, se pueden identificar infinitas formas de penetrar el objetivo. Ya sea física o

virtual, de toda manera si el trabajo previo es concreto, los daños serán significativos.

Mantener el acceso e infiltración: Cuando nos pasamos largos meses de espera para obtener el vehículo que por tanto tiempo habíamos soñado, no queremos perder las llaves al tercer día de usarlo. Del mismo modo los agentes maliciosos no desean pasar largas horas de análisis para llevar a cabo una infiltración y que luego la misma sea detectada y bloqueada. Por esa razón, la fase de mantener el acceso es de suma importancia para los mismos. Este proceso también es uno de los más importantes a tomar en cuenta a la hora de mitigar un ataque, pues si se detecta a tiempo las organizaciones pueden frenar el daño.

Cubrir los pasos o las huellas: ¿Aún recuerdan cuando eran apenas unos niños y rompían algo y lo mantenían a escondidas de sus padres? De esta misma manera los agentes maliciosos una vez han sido capaces de obtener y mantener el acceso, cubren sus huellas para evitar una futura detección por parte del personal encargado.

Figura 2.5: Fases del Hacking.

Fuente: (Ehack, 2019)

2.6.4 Estadísticas y casos de ataques informáticos

- Según el blog Accenture, Los dos ataques más frecuentes son los ataques de malware y aquellos basados en la web. Las empresas gastan un estimado de $2.4 millones en defensa.
- Cybersecurity Ventures dice que, se proyecta que el daño relacionado a ciberataques llegará a los $6 trillones de dólares anuales para el 2021.

- El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos. (Blog Accenture).
- Según Verizon, sé que reporta que usuarios estadounidenses abren un 30% de todos los correos maliciosos y un 12% de ellos dan clic al enlace peligroso.
- Según el website **KnowBe4** 91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones.
- El FBI asegura que ocurren más de 4,000 ataques de ransomware por día.
- Según el website **Vanson Bourne**, 90% de los hackers cubren sus rastros utilizando encriptación.
- En 2016, Uber informó que hackers robaron la información de más de 57 millones de conductores y pasajeros.
- En 2018, Under Armour informó que su aplicación “My Fitness Pal” fue hackeada, afectando a 150 millones de usuarios.
- En el 2016, 3 mil millones de cuentas de Yahoo! fueron pirateadas en uno de los mayores ataques cibernéticos de todos los tiempos.
- Según el website TbSEK, el costo promedio por delitos informáticos aumentó en más de un 27% durante el 2017. Se espera que el incremento del costo promedio sea aún mayor en los próximos años.

- Información preliminar por parte de Google & Apple, la información que las Apps filtran con mayor frecuencia son los números telefónicos y la ubicación del dispositivo. Cada día, de las tiendas de Apple Store y Google Play son bloqueadas cerca de 24 mil aplicaciones maliciosas.
- Según el website TbSEK los archivos de Microsoft Office como Word, Excel y Power Point confirman el grupo más frecuente de archivos que incluyen malware, con un 48% del total.

2.7 Vectores de ataque en la seguridad de la información

2.7.1 ¿Qué es un vector de ataque?

Según Alexander Guedez, un vector de ataque es un agujero o falla presentada en una defensa o medida previamente establecida. Por consiguiente, en el tema de la ciberseguridad, son las formas, medios o debilidades que permiten el acceso de agentes maliciosos a un determinado objetivo. Los cuales, mueven el juego a su favor para explotar una o varias vulnerabilidades que posee la persona o entidad que se le realizará el ataque.

Hablando un poco de donde proviene el término ¨vector de ataque¨, es necesario destacar que su origen es completamente militar. En este ámbito, las tropas

enemigas clasificaban ¨ataque¨ como la acción a ejecutarse y ¨vector¨ como el medio a utilizarse para arremeter contra el enemigo. Del mismo modo, podemos introducir esta expresión al contexto de la tecnología de la información. Ya que, los mismos sacan a relucir una estrecha relación en su terminología y contexto.

Finalmente, sé que pueden pensar que un vector de ataque siempre debe venir en grandes medidas y recursos, pero no es así. El vector puede ser cualquier medida o forma que interfiera directamente con las vulnerabilidades previamente evaluadas por el o los agentes maliciosos. De esta manera, hasta la más simple acción puede afectar grandemente.

2.7.2 Vectores de ataque en la seguridad de la información

Como ya le hemos mencionado previamente, podemos encontrar una cantidad bastante extensa de todo tipo de vectores de ataques. Los mismos son la flecha lanzada por el atacante con el fin de cumplir su objetivo pensado. A continuación, los vectores de ataques más utilizados:

- Correos electrónicos.
- Mensajes de texto.
- Llamadas telefónicas.
- Concursos ficticios.

- Interacción personal.
- Redes sociales.

2.8 Ataques informáticos recientes

2.8.1 Marriot

Este caso nos recuerda que incluso aquel lugar que nos hace sentir como en casa en nuestros viajes de negocios puede ser comprometido al más alto nivel. sucede que la cadena de hoteles Marriott notificó acerca de una de las mayores violaciones de la información en la historia, si, así como lo leyeron, en la historia. a la organización se le fueron violentadas informaciones personales y financieras de más de 500 millones de clientes alrededor de todo el mundo. Sin embargo, lo peor de todo es que la brecha de seguridad se origina en el año 2014 y no es hasta el 19 de noviembre del 2018 que la cadena hotelera se da cuenta de este gravísimo error.

Si creyeron que no podría empeorar, Marriott admite que dentro de los datos hurtados se encuentra: combinaciones de nombres, sexo, fecha de nacimiento, numero de pasaporte, número telefónico, dirección postal y hasta la fecha de reserva con entrada y salida. Asimismo, como información de las tarjetas de crédito utilizadas para el pago del hospedaje correspondiente y como si fuera poco no se

descarta la sustracción de las claves adjuntas a dichas tarjetas. Entonces, nos queda claro que puedes estar tomando una copa de vino en tu cena de negocios mientras que todos tus datos personales y financieros hasta el momento son robados y manipulados por agentes maliciosos.

2.8.2 Google+

Apenas lanzada en el año 2011 y propiedad del mismísimo gigante de la INTERNET Google, esta red social se proyectaba para hacer una competencia directa a sitios web como facebook, instagram y twitter. La misma fue diseñada bajo el objetivo principal de enlazar los productos blogger y youtube, ambos pertenecientes a google. Pero esta pequeña belleza del buscador se vino abajo más rápido de lo previsto y no es para menos, después que un nuevo bug comprometiera de manera directa la información de más de 52 millones de usuarios a consecuencia de esto, prácticamente se le quedaron los días contados. Un aspecto importante a resaltar es que la vulnerabilidad se mantuvo sin ser observada desde el año 2015 hasta marzo del 2018.

El error dentro de la red social permitió el acceso a la información privada en el perfil de usuario de Google+, la cual incluye detalles como direcciones de correos electrónicos, sexo, fecha de nacimiento, imagenes y videos de los usuarios, ocupación profesional y hasta los lugares vividos o visitados por los usuarios. Sin

duda alguna, un caso que nos recuerda que hasta en las más grandes compañías a nivel global pueden existir debilidades a la hora de salvaguardar la información.

Según un informe publicado en Wall Street Journal, la compañía demoró bastante en revelar dicha brecha en la seguridad por posibles daños a su reputación. Pero más caos aún vino cuando en diciembre del 2018 se reveló que había un nuevo fallo el cual permite la información completa de los perfiles pueda ser reflejada. aunque Google aseguró que este bug fue resuelto en una semana, el gigante tomó la decisión de cerrar la red social a los usuarios comunes o civiles en abril del 2019.

2.8.3 OpenSSH

Antes que nada, es pertinente saber que OpenSSH, es un conjunto de aplicaciones desarrolladas para realizar comunicaciones cifradas mediante una red. las cuales utilizan el protocolo SSH, el mismo tiene como función principal el acceso remoto a un servidor por medio de un canal seguro. OpenSSH es bastante utilizado en los sistemas operativos Linux, Mac y en el último tiempo Windows.

La brecha de seguridad que vamos a tratar a continuación sobresale de las demás debido a su duración presentada, 19 años. La misma se trata de un fallo en la enumeración de los nombres de usuario, la cual permite a un agente malicioso de manera remota adivinar los nombres de usuario registrados en un servidor OpenSSH. El escenario de ataque se basa principalmente en que un agente

malicioso intenta autenticarse en un endpoint de OpenSSH a través de una solicitud de autenticación mal formulada, la cual puede estar compuesta de un paquete truncado. Luego, el servidor OpenSSH vulnerable puede reaccionar de dos maneras diferentes: En caso de que el nombre de usuario en la autenticación mal formada no exista en la base de datos, el servidor responderá con el simple error de fallo en la autenticación, en cambio, en el caso de estar ya registrado simplemente se cerrará la conexión sin dar ninguna respuesta.

El bug fue reparado en las versiones estables, pero un gran número de dispositivos se vieron expuestos a un posible e inminente ataque masivo ya que OpenSSH es una de las tecnologías mayormente utilizadas en el mundo cuando se trata de acceso remoto y se usa en millones de dispositivos grandes y pequeños.

2.8.4 GitHub ataque DDoS

Para los que no saben acerca de GitHub, es una plataforma para desarrollo colaborativo, la cual se utiliza para alojar proyectos con la implementación del sistema de control de versiones Git. En el mismo, puedes controlar y gestionar los diversos cambios que se realizan sobre los elementos de un producto en desarrollo. En este caso el servicio de GitHub sufrió el mayor ataque de denegación de servicio antes visto, 1,35 terabits por segundo (126,9 millones de paquetes informáticos por segundo).

Como sabemos los ataques de DDoS sobrecargan los recursos computacionales de la organización que sirve como objetivo, toda esta sobrecarga se ejecuta hasta que los servidores quedan inaccesibles debido a la saturación de información. En el caso de GitHub el volumen de datos sobrepasó los ordenadores, provocando que dejaran de responder y se pongan en estado offline. Un lado positivo a resaltar es que la confidencialidad e integridad de los datos de los usuarios nunca estuvo en riesgo.

2.8.5 Quora

Tal vez este nombre no sea muy conocido, pero es uno de esos tantos éxitos silenciosos que no encontramos en INTERNET. Con millones de usuarios en la web, es una de las mayores fuentes de información junto a Wikipedia. y como es de esperarse, al ser de tan gran envergadura está en el ojo por parte de los agentes maliciosos. En este caso se puso en riesgo a 100 millones de usuarios.

Quora admite que se realizó un acceso no autorizado en el cual se comprometió la información personal de los usuarios, tales como: Nombres, dirección de correos electrónicos, datos vinculado a redes sociales como Facebook y Twitter, etc. aunque la entidad asegura que tomó las medidas pertinentes para para evitar y mitigar estos ataques en el futuro, es de relevancia destacar que prevenir es de mayor importante

y menos gasto económico que una corrección agresiva. Lo cual nos recuerda que es de importancia invertir más en el tema de la seguridad.

CAPÍTULO III:

TIPOS DE ATAQUES Y VECTORES EN LA SEGURIDAD DE LA INFORMACIÓN.

3.1 Tipos de ataques en la seguridad de la información.

3.1.1 Ingeniería social

“La Ingeniería Social está utilizando medios no técnicos para obtener acceso no autorizado a la información o al sistema” (Chandra, 2011). Normalmente, los hackers utilizan vulnerabilidades de los sistemas y ejecutarán scripts para obtener acceso. Cuando los hackers implementan ingeniería social, explotan la naturaleza humana. La ingeniería social está representada por la construcción de relaciones de confianza con las personas que trabajan en el interior de la organización para obtener acceso o que tienen el privilegio de información confidencial como nombres de usuario, contraseñas y códigos de identificación personal que son necesarios para obtener acceso a redes, información y equipos.

Los sitios web de redes sociales son los lugares más populares en la actualidad. El número de usuarios crece a pasos agigantados. Proporcionan excelentes servicios para hacer nuevos amigos, encontrar viejos amigos y compartir fotos y videos. Estos sitios web se han convertido en una de las herramientas más entretenidas en INTERNET. Los usuarios registrados deben compartir información básica sobre sí mismos, pero tienen opciones para compartir información personal y familiar de forma ilimitada en INTERNET. Comparten estas informaciones con sus amigos y familiares y hacen que sus páginas web sean interesantes y divertidas.

Los ingenieros sociales usan estos sitios web para aprovecharse de posibles objetivos. Los ataques de ingeniería social son fáciles de intentar, tienen bajo costo y muy difícil de rastrear. Estos ataques en línea suelen ser variantes de programas tradicionales de piratería de seguridad de la información, como malware, gusanos, etc., pero en caso de un sitio web de redes sociales ingenieros sociales explotan el factor de confianza entre víctimas y amigos de la víctima para obtener información sensible y valiosa.

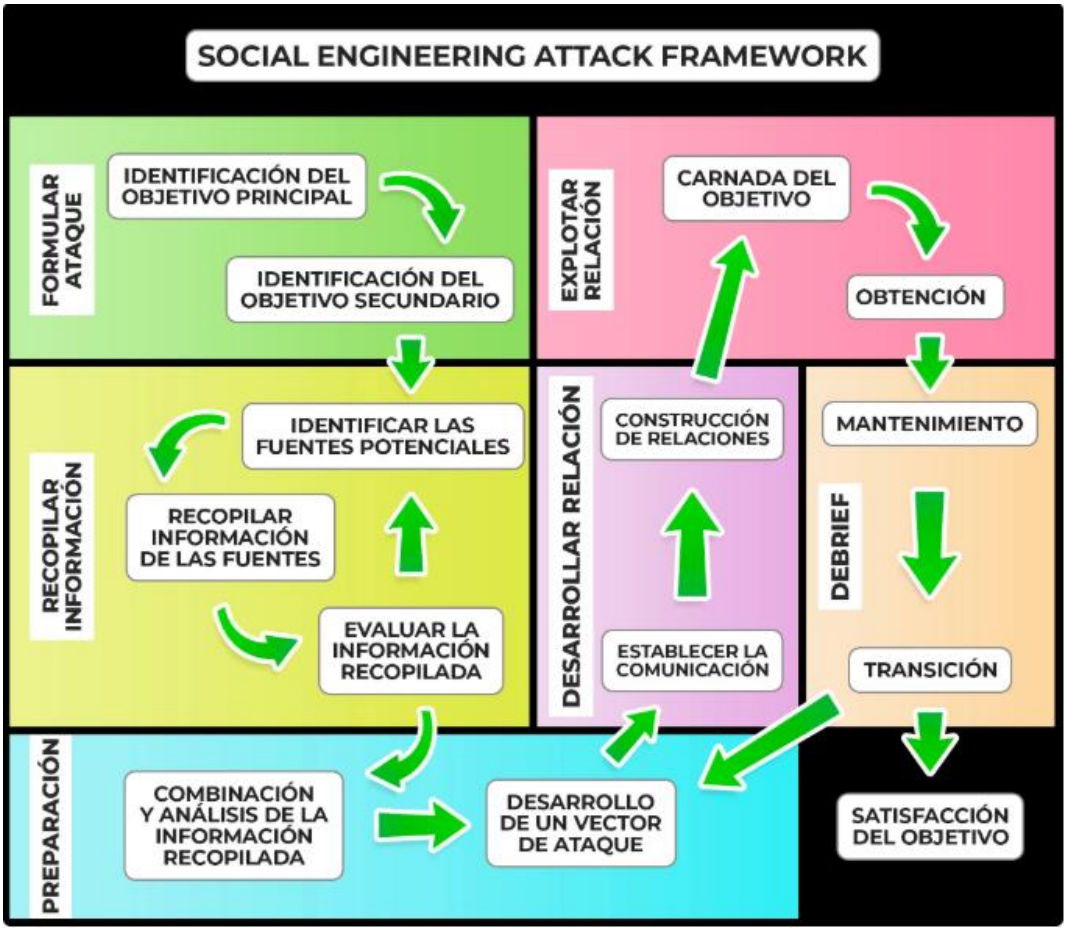


Figura 3.1. Esquema de un ataque de ingeniería social

*Fuente: (**Tahiri Dikovec** 2019)*

3.1.2 Phishing

“El término Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.” (Rivero. M, 2008). Estos ataques generalmente se aprovechan de la amabilidad y la escasez de las condiciones humanas. El phishing se intenta más comúnmente a través del correo electrónico, pero también puede presentarse en forma de mensaje instantáneo, llamada telefónica o incluso en persona. En casi todos los intentos, el atacante se hace pasar por alguien para explotar la idea de autoridad y ganar la confianza y la aceptación de la víctima.

Incluso esta extensión del phishing, el Spear-Phishing, en el que el ataque se dirige a un objetivo o un grupo específico dentro de un departamento. Es mucho más sofisticado el enfoque, ya que su información personal y actividades relacionadas que son esenciales para hacer engaño creíble. Para llevar a cabo un ataque de este tipo es necesario tener una mejor comprensión del objetivo, siendo la información obtenida más específica y detallada. Además, en este caso, el mensaje de correo electrónico puede contener hipervínculos que pueden forzar a un miembro del personal a violar la empresa de seguridad.

3.1.3 Vishing

Según BBVA (2013) el “vishing” es una nueva estafa que pretende suplantar la identidad del afectado a través de VoIP (Voice over IP), recreando una voz automatizada semejante a la de las entidades bancarias”. La empresa de seguridad Symantec (2018) advirtió que por las redes sociales circulan un sin número de aplicaciones no verificadas que tienen la intención de instalar este tipo de Malware y con el mismo se dedican a interceptar las llamadas de los usuarios hacia sus bancos, etc. y redireccionarlos a las centrales de los estafadores, para conseguir acceso a sus cuentas e información personal. La misma empresa también informa a través de su blog que al menos 22 aplicaciones móviles falsas, que se encuentran en mercados de Android de terceros, están dirigidas a clientes de bancos coreanos con el Malware. Fakebank normalmente recolecta mensajes SMS bancarios, graba llamadas telefónicas a los bancos y muestra una interfaz de usuario de inicio de sesión bancaria falsa para las víctimas; La capacidad de interceptar llamadas entrantes y salientes es una nueva capacidad.

3.1.4 Baiting

“Es en muchos sentidos similar a los ataques de phishing. Sin embargo, lo que los distingue de otros tipos de ingeniería social es la promesa de un artículo o un bien que los hackers usan para atraer a las víctimas. Los Baiters pueden ofrecer a los usuarios descargas gratuitas de música o películas, si entregan sus credenciales de inicio de sesión a un sitio determinado” (Bisson D, 2015). El término también es llamado “Carretera de Manzanas” (Road apples), son ataques de phishing que invitan a los usuarios a hacer clic en un enlace para obtener cosas gratis. Actúan como virus Troyano donde el ataque se realiza mediante la explotación de materiales informáticos no seguros, como medios de almacenamiento o unidades USB que contienen malware en una cafetería que las víctimas pueden encontrar. Cuando las víctimas conectan la unidad USB a sus computadoras, la unidad actúa como un caballo de Troya del mundo real y ataca la computadora. Este ataque realiza acciones maliciosas en segundo plano sin que las víctimas lo noten.

3.1.5 Shoulder surfing

“El Shoulder surfing es el acto de ver lo que alguien está escribiendo o haciendo en la computadora mirando la pantalla (o el teclado) con o sin el conocimiento de la víctima” (Robinson, 2007). El acto de Shoulder surfing en sí no es una verdadera

forma de ingeniería social, ya que el atacante no está involucrando activamente a la víctima. Aun así, se utilizan otros métodos de ingeniería social para llevar a este ataque, ya que el atacante necesita la confianza de la víctima y debe hacer que la víctima se sienta cómoda para permitir que el atacante se acerque tanto.

A los atacantes les resulta difícil caminar y hacer Shoulder surfing sin un sentido de confianza por parte de la víctima. Esta acción seguramente hará que la víctima potencial pregunte cuál es el motivo del atacante y por qué el atacante está detrás de ellos. Ganarse la confianza de la víctima, involucrar a la víctima en una conversación y encontrar (o crear) similitudes entre el atacante y la víctima aumentará las posibilidades de que este ataque tenga éxito. A medida que la víctima cae en un falso sentido de confianza alrededor del atacante, será menos probable que note o se preocupe si el atacante observa lo que está escribiendo en la computadora. Una vez que se establece esta confianza, el atacante solo necesita estar atento a los nombres de usuario, contraseñas u otra información valiosa, y luego desaparecer. Una vez más, la víctima no tiene idea de que se haya producido un ataque.

3.1.6 Hunting

Este tipo de ataque busca ejecutar la ingeniería social a través de una interacción mínima con el objetivo. Una vez que se logra el objetivo especificado y se establece

la violación de seguridad, es probable que se termine la comunicación. Esta es la metodología más utilizada para soportar ciberataques y, por regla general, el modus operandi implica un solo encuentro.

3.1.7 Pharming

Según Karpersky lab “el pharming” es una combinación de los términos "phishing" y "farming", es un tipo de cibercrimen muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial”. Este es un ejemplo de ataque pasivo donde la víctima acude al atacante. El atacante hace una recreación de un sitio web legítimo, como un banco o un minorista en línea. El objetivo es engañar a la víctima para que piense que está en un sitio real y legítimo y que la víctima ingrese información confidencial. Dependiendo del tipo de sitio web, este podría ser el número de seguro social, la información de la tarjeta de crédito o el nombre de usuario y contraseña de un sitio web legítimo.

3.1.8 Virus y Gusano

Los virus y gusanos son “programas informáticos que no permiten que los sistemas informáticos funcionen correctamente. Ambos programas pueden replicarse a sí

mismos, sin embargo, una pequeña diferencia entre ambos programas es que los virus no pueden viajar por sí mismos y requieren una red para conectarse y realizar su función, mientras que los gusanos pueden viajar por sí mismos y funcionar de manera independiente" (Hadnagy, 2010). El objetivo de estos es que funcione mal el sistema de trabajo. En los últimos años, los virus se propagan a través de disquetes o CD, pero ahora los virus se propagan a través de INTERNET, que llega a millones de sistemas informáticos en un instante. Si el virus ingresa a una red organizacional, todos los sistemas conectados a la red se verán afectados en minutos, creando así una pérdida de millones de dólares para la organización.

3.1.9 Malware

Según Joseph Regan (2019) El termino de malware "es una contracción de software malicioso. En pocas palabras, el malware es cualquier pieza de software que se desarrolló con la intención de dañar dispositivos, robar datos y, en general, causar un desastre. Los virus, troyanos, Spyware y Ransomware se encuentran entre los diferentes tipos de malware".

El desarrollo y la propagación de estos softwares malintencionados se han convertido en un problema real para todos los usuarios en la red hoy en día. El mismo se vuelve cada vez más problemático, ya que las computadoras, los teléfonos inteligentes y otros dispositivos inteligentes están constantemente

conectados en INTERNET. Las víctimas potenciales de ataques maliciosos son más que nunca. Además, la "fama" de la exposición de las agencias de noticias y las redes sociales a las diversas amenazas y ataques cibernéticos atrae el interés de más programadores para desarrollar software con los mismos fines maliciosos.

Sin embargo, el software malicioso existe desde hace bastante tiempo. A pesar de que las primeras implementaciones de los sistemas de información eran mucho más vulnerables, los ataques maliciosos no eran una preocupación. Fue porque durante esos primeros años, muy pocas personas pudieron comprender profundamente cómo funcionan los sistemas de información y, por lo tanto, explotarlos.

Según una estadística desarrollada por Kaspersky Security (2016), los países latinoamericanos, al menos 12 ataques por segundo son registrados por usuario conectado a

INTERNET. Dentro de los países más afectados del área están:

Intentos de ataque por usuarios conectados	
País	**Porcentaje**
Brasil	49,9%
Perú	41,9%
Bolivia	41,8%
Chile	40,0%
México	39,9%
Colombia	39,3%
Guatemala	37,5%
Ecuador	36,1%
Venezuela	36,0%
Uruguay	30,0%
Argentina	29,5%

Figura 3.2: Intentos de ataque a usuarios conectados.

Fuente: (BBC, 2016)

3.1.10 Troyano

"En informática, un Troyano es un programa descargado e instalado en una computadora que parece inofensivo, pero de hecho es malicioso. Los cambios inesperados en la configuración de la computadora y la actividad inusual, incluso

cuando la computadora debe estar inactiva, son fuertes indicios de que un troyano reside en una computadora.” (Rouse, M 2019). Los ataques del Troyano, también conocidos como " “gimmies", tienen como objetivo explotar la curiosidad de la víctima. Los ataques del Troyano son únicos, ya que es posible que nunca requieran contacto (directamente en persona o indirectamente por correo electrónico) para llevarse a cabo. El ataque se realiza dejando algo que la víctima encontrará tan valioso como un CD o una unidad flash.

Si bien a primera vista parece no ser más que una pieza inofensiva de tecnología es el software contenido el que es un peligroso. Antes de plantar el dispositivo en un lugar donde la víctima lo encuentre, el atacante cargará cualquier cantidad de utilidades de Malware en él. Estas utilidades incluyen Keyloggers (registradores de claves), virus de spyware, kits de raíz, etc. Una vez que la víctima encuentra el artículo y lo inserta en su computadora, el software se instalará y se activará automáticamente sin el consentimiento o conocimiento de la víctima. Cuando la víctima recoge el artículo después de haber guardado lo que buscaba, el troyano se aloja en un espacio discreto. La curiosidad de la víctima explota cuando está coloca el dispositivo en su computadora para ver los datos del dispositivo.

3.1.11 Spyware

“Spyware es software malicioso que infecta ordenadores y otros dispositivos conectados a INTERNET, y graba secretamente sus datos de navegación, las páginas web que visita y sus compras online” (Moes T, 2019). Este tipo de software se puede instalar en una computadora de diferentes maneras: troyanos, que se instalan sin el consentimiento de los usuarios, visitan sitios web que contienen ciertos controles como ActiveX o código malicioso que explota vulnerabilidades en el navegador web, aplicaciones como Shareware o Freeware que incluyen Spyware en el paquete de instalación. En general, el software espía se puede instalar con o sin la aprobación del usuario y es posible que no informe sobre el tipo de información recopilada por el software y cómo se utilizará.

El tipo más común de información monitoreada por el Spyware en los usuarios promedio es la dirección de los sitios web más visitados, los sitios web de los motores de búsqueda utilizados por el usuario, la versión del sistema operativo, el software que se utiliza en las computadoras infectadas y el correo electrónico del usuario. Después de que la información se procesa, se vende a compañías externas que utilizan el correo electrónico y los patrones de comportamiento del usuario para anunciar productos similares o para enviar correos electrónicos maliciosos que intentan dirigir a los usuarios a sitios web falsos y solicitar información bancaria confidencial utilizando técnicas de phishing.

3.1.12 Adware

De acuerdo con Panda Security (2019) Adware, o Malware respaldado por publicidad, “es un término utilizado para describir el software no deseado que muestra anuncios en un dispositivo. Un virus adware se considera un PUP (programa potencialmente no deseado), lo que significa que es un programa que se instala sin el permiso expreso del usuario”. Este tipo de software limita la experiencia de navegación del usuario con anuncios excesivos, ventanas emergentes, pancartas, enlaces en texto y video comerciales de reproducción automática.

3.1.13 Ransomware

“Es un software malicioso que infecta un dispositivo y brinda a los ciberdelincuentes la capacidad de bloquear el mismo desde una ubicación remota y encriptar los archivos para controlar toda la información y los datos almacenados.” (Panda Security, 2013). En el año 2016, el FBI declaró que las pérdidas debidas a ataques de ransomware fueron de aproximadamente $ 1 mil millones, lo que indica el inmenso daño financiero que un ransomware puede causar a las empresas. Las ramificaciones de un ataque de ransomware pueden ser más caras que el rescate en sí. Las empresas afectadas pueden sufrir los resultados de este tipo de ataque

durante años debido a la pérdida de negocios, clientes, datos y productividad.

3.1.14 Man in the middle

Un ataque Man-in-the-middle “es un nombre genérico para cualquier ataque cibernético en el que alguien se interpone entre el usuario y lo que sea que esté haciendo en línea, ejemplo entre usuario y su banca en línea o entre usuario y su conversación con sus familiares o entre los correos electrónicos del trabajo y la persona destinada a enviarlos / recibirlos o entre usuario y la casilla donde ingresa sus datos de pago, Etc” (Torres G, 2018).

La idea básica es que un atacante se interpone entre dos partes que se comunican y comienza a controlar su comunicación. Supongamos que “A” quiere comunicarse con “B”. Si una entidad maliciosa, llamada “C”, logra insertarse en el camino de la comunicación entre ‘A y B”, entonces se convierte en el Man in the middle, lo que significa que es capaz de leer y cambiar mensajes en la comunicación. Desde este momento existen dos canales de comunicación, uno entre “A y C” y el otro entre “C y B”. Cada mensaje enviado entre A y B pasa por C y puede ser manipulado sin que ningún lado lo note.

3.1.15 Ataque DDoS

“La denegación de servicio es un ataque que derriba la red objetivo y hace que deniegue o limite el servicio a usuarios legítimos. Para realizar un ataque DoS, el atacante no necesita ser un experto; Este ataque se puede realizar con un simple comando ping. Los hackers experimentados, que desean realizar el ataque DoS, no lo harían desde su propio sistema” (Shoniregun C, 2005). un pequeño programa conocido como “Zombies” está instalado en algunas computadoras que tienen acceso de nivel intermedio en una red. Cada vez que sea necesario realizar el ataque, el programa “Zombies” se ejecutará de forma remota y las computadoras que tenga el mismo instalado, estos lanzan los ataques de forma simultáneamente.

El atacante no necesita nombre de usuario o contraseña en estos casos. Una debilidad o vínculo conocido en el sistema puede brindar la oportunidad de tales ataques. Estos ataques generalmente desactivan la red o corrompen la información crítica. El sistema destino se bloquea o entra en un estado en el que no puede funcionar de manera eficiente y los servicios proporcionados por el sistema se detienen.

3.1.16 Keyloggers

“Los keyloggers son programas de spyware que registran las pulsaciones del teclado conectado al ordenador infectado” (Moes T, 2019). La actividad en tiempo real de un usuario en la computadora, incluidos los golpes de teclado que se presionan, los sitios web visitados, los programas en ejecución, los mensajes instantáneos y otras actividades relacionadas con la computadora. El usuario puede saberlo o el keylogger está oculto para el usuario con fines maliciosos.

Si un keylogger está instalado en un sistema, se puede configurar para que se inicie cada vez que se enciende la computadora. Después de instalar el keylogger en un sistema informático, el sistema puede ser monitoreado activamente.

3.1.17 Inyección de SQL

La inyección de SQL “es un tipo de ataque que puede dar a un adversario un control completo sobre la base de datos de su aplicación web mediante la inserción de código SQL arbitrario en una consulta de base de datos.” (Porup J, 2018).

Este tipo de ataque es una de las amenazas más peligrosas y comunes para las bases de datos y las aplicaciones web. Por lo general, implica actualizaciones maliciosas, modificaciones de la entrada de SQL del usuario, ya sea cambiando la

estructura de una cláusula existente o agregando cláusulas adicionales. El mismo permite a los atacantes acceder, eliminar o modificar información crítica en una base de datos sin la autorización adecuada y convertirse en la razón de los ataques de Inyección de SQL.

Algunos ejemplos de casos sucedido en los últimos años:

En 2017, NextGEN es un complemento de galería más popular que fue atacado con Inyección de SQL para acceder a la base de datos que almacena detalles de usuarios muy confidenciales y luego los investigadores dijeron que los atacantes usaron dos escenarios para robar datos de usuarios (Vatu, 2017).

En 2017, Airsoft GI es una empresa con sede en California. Los hackers atacaron el foro Airsoft GI y robaron unas 65,000 cuentas que incluyen detalles personales de usuarios registrados. Los hackers habían robado 40,000 cuentas de Gmail, 2,500 cuentas de Outlook, 3,000 cuentas de Yahoo, 2,500 cuentas de hotmail. Este ataque se ha iniciado a través de Inyección de SQL. (Amir, 2017).

3.1.18 Rootkit

Los Rootkits “son las cajas de herramientas del mundo del Malware. Se instalan como parte de alguna otra descarga, puerta trasera (BACKDOOR) o gusano. Luego toman medidas para evitar que el propietario detecte su presencia en el sistema. Una vez instalados, los Rootkits proporcionan a un mal actor todo lo que necesitan

para tomar el control de su PC y usarlo para DDoS o como una computadora zombie.” (Petters J, 2018).

El término "rootkit" proviene de los términos "root", el usuario más poderoso en un sistema UNIX, y "kit", un conjunto de programas y código. La calidad de identificación de los rootkits es que ocultan su presencia en un sistema infectado. Los rootkits no son maliciosos por naturaleza, pero lo son cuando se ejecutan con intención maliciosa. Por ejemplo, los rootkits a menudo ocultan malware. El término "malware" antes mencionado es un compuesto de "software malicioso" y describe un código que modifica el comportamiento de un sistema sin el conocimiento o consentimiento del usuario.

3.1.19 LokiBot

Según, Kaspersky Lab (2018) determina el objetivo clave del malware Loki Bot “es robar contraseñas de navegadores, aplicaciones de mensajería, clientes de correo y FTP y billeteras de criptomonedas. Loki Bot envía todo su botín a los propietarios del malware”. Este tipo de software malicioso puede por ejemplo simular la aplicación de una entidad bancaria, donde el usuario introduce sus credenciales y estos datos son enviados directamente al atacante del software. El mismo puede simular notificaciones como redes sociales, con el objetivo de captar información personal de la víctima.

3.1.20 Escaneo de puertos

“Según el Instituto SANS, Port Scanning es una de las técnicas más populares que usan los atacantes para descubrir servicios que pueden explotar para entrar en los sistemas. Aunque Port Scanning no es intrínsecamente hostil, a menudo es el primer paso de reconocimiento utilizado por los piratas informáticos cuando intentan infiltrarse en una red o robar / destruir datos confidenciales.” (Williams J, 2018).

El escaneo de puertos se consideraría un tanteo directo. Los escaneos de puertos permiten que un atacante trabaje desde una ubicación remota para determinar si una computadora está ubicada en una dirección en particular, qué servicios está ejecutando e incluso qué sistema operativo está usando. Un escaneo de puertos consiste en un intento de conexión a cada puerto en una computadora de destino para determinar qué puertos están abiertos y, por lo tanto, qué servicios se están ejecutando.

Dada una intranet, las computadoras pueden ubicarse en este espacio de direcciones a través de un círculo de ping, lo que significa hacer ping a cada dirección ip en el espacio de direcciones para determinar si una computadora está viva en el otro extremo. Una solicitud de ping consiste en un paquete de Protocolo de mensajes de control de INTERNET (ICMP) encapsulado dentro de un paquete de Protocolo de INTERNET (IP). Como el núcleo del sistema operativo maneja los paquetes ICMP en la capa de red, no se accede a ningún puerto de servicio en la

máquina de destino y, por lo tanto, ninguna aplicación registra la solicitud de eco / respuesta de eco. Sin embargo, un círculo de ping solo puede determinar que hay una respuesta de una dirección en particular. No puede determinar qué servicios están disponibles en la máquina.

Dada una computadora o red de destino, se puede usar un escaneo de puertos para determinar los puertos que están abiertos y, por lo tanto, los servicios que probablemente estén activos. Los escaneos de puertos se pueden clasificar por el objetivo del escaneo y por el conjunto de banderas (flags) del Protocolo de control de transporte (TCP). Hay cuatro tipos de escaneos, que son definidos por la información del objetivo que se recuperará:

Escaneos verticales, un escaneo vertical se refiere al escaneo de todos los puertos en un solo sistema para determinar qué servicios está ejecutando un sistema.

Escaneos horizontales, un escaneo horizontal es aquel en el que se verifica un solo puerto en una gran parte de los sistemas de una red.

Exploraciones estroboscópicas (Strobe Scans), una exploración estroboscópica es similar a una exploración horizontal, sin embargo, comprueba algunos puertos en lugar de un solo puerto. Esto lleva el nombre del software Strobe, que sondeó puertos de uso común como 21, 22, 23 y 80.

Escaneos en bloque, un escaneo en bloque combina escaneos verticales y horizontales en un escaneo grande que verifica todos los puertos en todos los sistemas.

3.2 Vectores de ataque en la seguridad de la información.

3.2.1 Correo Electrónico

Sus antecedentes se remontan al año 1965 y es específicamente en el Instituto Tecnológico de Massachusetts (MIT) donde comienza todo, allí es donde se registra el primer uso de un sistema de correo electrónico. Con el objetivo de expandir aún más esta nueva herramienta en el año 1971 Ray Tomlison, creó la primera aplicación de correo electrónico sobre la red ARPANET (precursora de INTERNET). En efecto, esta aplicación llamada SNDMSG era capaz de enviar mensajes a otras personas vía red. A Tomlison le conoce históricamente como el padre del correo electrónico.

El funcionamiento del correo electrónico se acerca bastante al sistema de correo postal. Es decir, ambos son usados para recibir y transmitir mensajes utilizando buzones de correo intermedios (en este caso llamados servidores) donde los mensajes son almacenados temporalmente antes de enviarse a su destino. Asimismo, como los grandes almacenes de paquetes y correo en las grandes ciudades, los servidores de correo electrónicos son los repositorios de almacenamiento de todos los mensajes recibidos y transmitidos para una cuenta de correo específica.

Luego de ver un tanto de la historia de esta herramienta indispensable hoy en día, tal vez se pregunten ¿Qué la hace tan común a la hora de ser utilizada en ataques de la información? Pues no es para menos, con aplicaciones tan conocidas como lo son Outlook, Gmail, Yahoo, Icloud y con más de 5,000.000.000 millones de usuarios registrados en el año 2019, no es sorpresa que sea el vector más utilizado por los agentes maliciosos. A continuación, algunos datos a relucir sobre el correo electrónico utilizado como vector de ataque:

- El 58% de los casi 80 millones de amenazas bloqueadas e identificadas como ransomware por Trend Micro (empresa dedicada a soluciones de seguridad informática) durante enero-junio 2016 se han transmitido por correo electrónico.
- Mientras las infecciones ransomware comienzan normalmente a través de correo electrónico, el 71% de las familias de ransomware conocidas entra a través de correo no deseado.
- Utilizando ingeniería social, para diseñar un correo perfecto para que el usuario haga clic y ejecutar cualquier tipo de ataque vía su correo electrónico de entrada.

Por estas razones y más, es importante que las empresas y administradores de TI se enfoquen bastante en la orientación y prevención contra ataques ejecutados vía correo electrónico.

Ejemplo:

Los ciber criminales tienden a intentar engañar a los usuarios de páginas de compra en línea (como Amazon) con emails falsos enviados desde cuentas falsas que parecen legítimas a primera vista. Estos emails (phishing) pueden ser usados para robarle el dinero a las víctimas o enviar un archivo adjunto email que puede traer consigo un serio virus de ordenador.

Según el sitio web “Losvirus”, Algunos estafadores estuvieron usando la dirección email **auto-shipping@amazon.com** para enviar miles de emails que contenían el ransomware Locky. Estos emails incluían un título como: “Your Amazon.com Order Has Dispatched (#order_number)” y contenían un archivo adjunto ZIP que traía un malicioso archivo JS el cual, una vez abierto, descargaba el ransomware desde una página web.

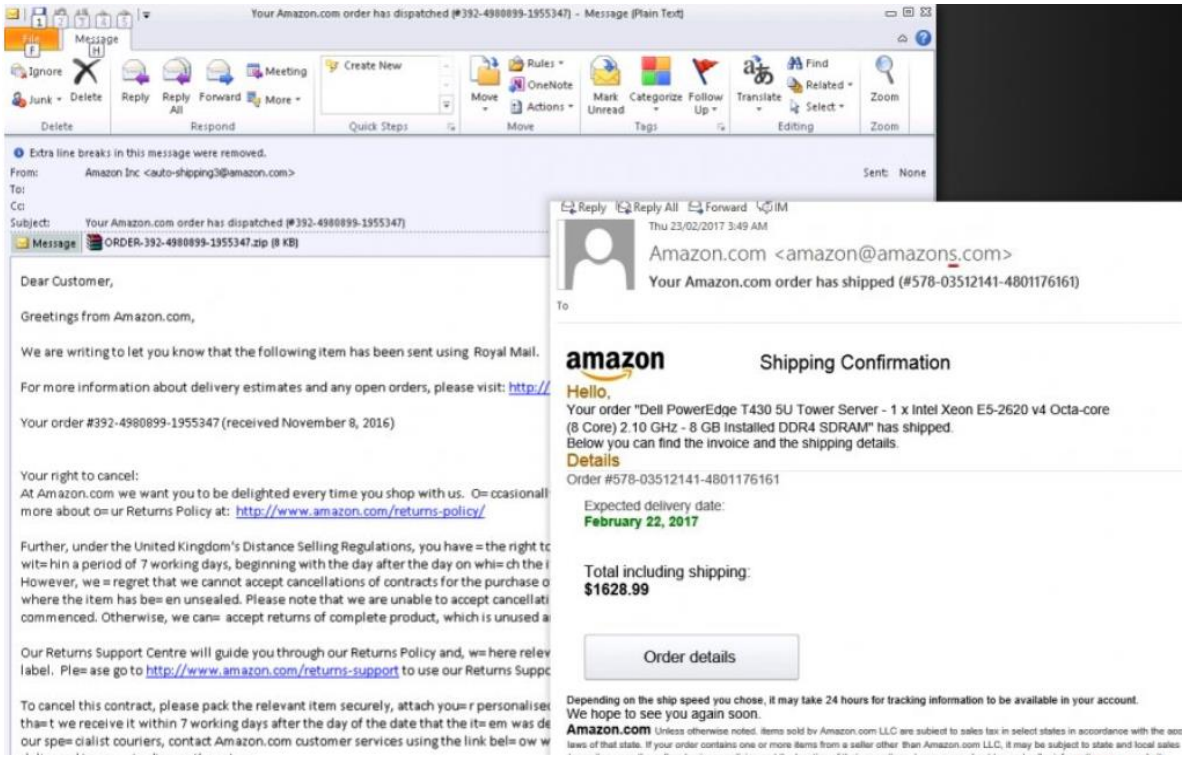


Figura 3.3: Ejemplo correo sospechoso

Fuente: (Los Virus)

3.2.2 Llamadas telefónicas

Sin duda alguna hemos entrado en la era digital, sin embargo, el teléfono sigue siendo el arma de preferencia de muchos de los estafadores (agentes maliciosos). Según Federal Trade Commission (FTC, Comisión Federal de Comercio) tan solo en el año 2018 recibió más de 940,000 quejas de fraude en las que se identificó un método de contacto, y en un 69% de los casos, las llamadas fueron el método que usaron los estafadores. Con el fin de conseguir su objetivo una vez que te tienen en

la línea telefónica, los victimarios realizan promesas dudosas, ventas agresivas y amenazas falsas para obtener la información que necesitan para robar tu dinero, tu identidad (o ambos).

A sabiendas de que las personas pueden tener ciertas dudas y sospechas, es habitual que los estafadores se hagan pasar por representantes de **agencias gubernamentales** o por compañías de **tecnología**, de **viajes**, de ventas minoristas y financieras muy conocidas, que te llaman con supuesta información importante por ofrecer.

Si se preguntan ¿Por qué razón hacen este tipo de acciones? aquí les va el siguiente dato, La FTC informa que en el 2018 la pérdida promedio de una estafa telefónica fue de $840, más del doble de la pérdida promedio de todos los tipos de fraude. Y si creyeron que los agentes maliciosos tienen que marcar manual cada llamada, otra vez se equivocan, pues la nueva tecnología está facilitando este trabajo ilícito. Con los marcadores automáticos, los mismos pueden hacer millones de llamadas automatizadas por solo unos pocos dólares al día.

Ejemplos de los pretextos más utilizados:

Podría ser con buenas noticias cómo: ¡Calificas para un gran premio en efectivo! o ¡Has sido preseleccionado para esta gran oferta de vacaciones!

También ser con malas noticias: Debes impuestos atrasados o Hay un problema con tu cuenta de tarjeta de crédito.

Sin importar cual sea el problema, normalmente dicen que se puede resolver si, por ejemplo, simplemente proporcionas tu número de seguro social o realizas un pago de inmediato.

Los estafadores telefónicos pueden incluso hacerse pasar por recaudadores de fondos para entidades benéficas (sin duda alguna son chicos malos). Y si pensaron que estas cifras y circunstancias disminuirían pues error otra vez ya que según un análisis de datos realizado por la firma de seguridad de telecomunicaciones First Orion, en el 2019, más del 44% de las llamadas a teléfonos móviles serán fraudulentas.

A continuación, algunos consejos que podemos hacer:

- Cuelga las llamadas automatizadas.
- Tómate tu tiempo y hazle preguntas a la tele vendedores, ya que Las empresas y organizaciones benéficas legítimas responderán tus preguntas y te darán tiempo para considerar una compra o donación.
- Investiga más a fondo las ofertas de viajes, organizaciones benéficas y las oportunidades de negocios e inversión que te ofrecen por teléfono.
- Considera usar una aplicación móvil o dispositivo que pueda detectar y bloquear las llamadas fraudulentas.
- No devuelvas llamadas de números desconocidos que solo timbren una vez.

- No pagues cargos de registro ni de envío para obtener un producto o premio que se supone que es gratis.
- No hagas pagos con tarjetas de regalo, tarjetas de débito prepagadas o por transferencia bancaria.

3.2.3 Mensajes de texto

Un agente malicioso puede enviar un mensaje de texto o SMS por medio del cual solicita que se envíe información confidencial, personal y/o financiera a través de un enlace web o un sitio web falso, o por medio de un número de teléfono. Puede parecer que los mensajes provienen de una compañía u organización confiable, o de alguna otra entidad con la que puedes estar realizando operaciones comerciales.

Teniendo en cuenta que las compañías y organizaciones de renombre nunca solicitará que "confirmes" o "verifiques" información personal confidencial en un mensaje de texto SMS no deseado. Por esta razón la gran parte de los ataques que resultan exitosos por esta vía se atribuye completamente a la desinformación de los usuarios.

Ejemplos de mensajes fraudulentos:

- Banco Popular Dominicano. Llámenos inmediatamente al 1-809-xxx-xxxx en relación a una reciente restricción en su cuenta. Gracias.

- ¡¡Alerta!! Honolulu City & County Employees ha restringido las verificaciones pendientes de su cuenta. Comuníquese con nosotros AHORA al 213-xxx-xxxx.

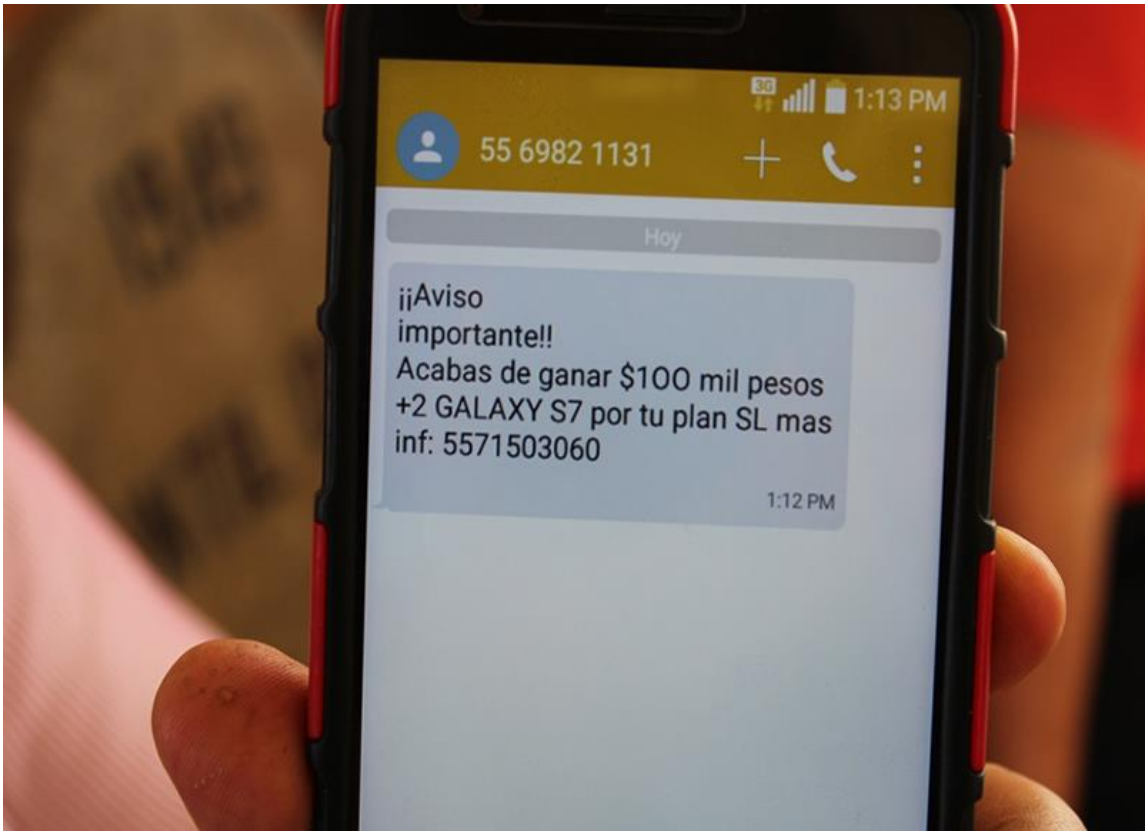


Figura 3.4: Mensaje sospechoso

Fuente: (Movistar)

3.2.4 Redes sociales

Desde un simple “Like” que se encuentren dentro de los primeros vectores de ataques a tomar en cuenta por los agentes maliciosos.

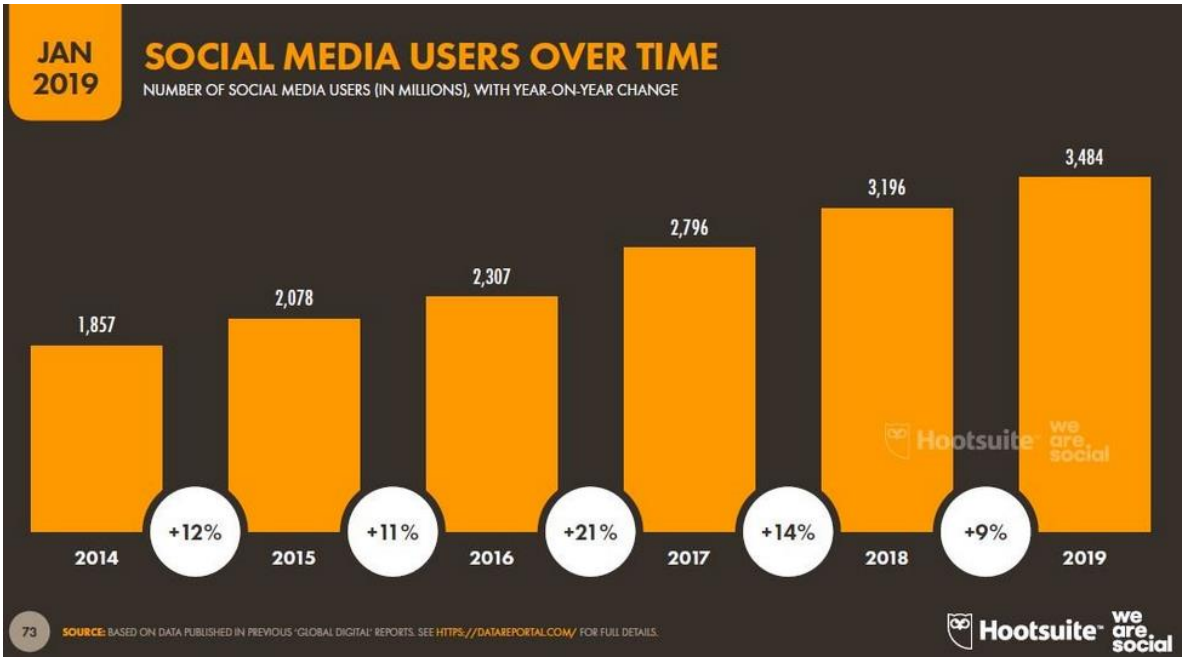


Figura 3.5: Social Media Users Over Time

Fuente: (Hootsuite)

Según la compañía de seguridad informática ESET en su “guía de seguridad en las redes sociales”, las redes sociales son parte de los hábitos cotidianos de muchas personas. Tanto adultos como menores, cualquier internauta usa al menos una red social y la gran mayoría de ellos participan activamente en más de una. Estas plataformas son servicios de INTERNET que permiten a los usuarios generar un

perfil público, en el que pueden plasmar datos personales e información de distinta índole. Tal es el impacto que generaron, que para muchas personas las redes sociales son los motivos principales para conectarse a INTERNET.

Sin embargo, a partir de su uso constante, los usuarios se ven expuestos a un conjunto de amenazas informáticas que pueden atentar contra su información, privacidad, dinero o incluso su propia integridad. Es necesario destacar los ataques o agresiones que podemos encontrar dentro de ellas:

- **Infecciones con malware:** Son archivos con fines dañinos que, al infectar una computadora o dispositivo móvil, tienden a realizar diversas acciones perjudiciales y no autorizadas. Dentro de las cuales destacan: El robo o secuestro de información, el control del sistema, la captura de contraseñas o sesiones activas e inclusive deteriorar el rendimiento del dispositivo infectado. Gusanos, troyanos y ransomware, son las más conocidas variantes en este campo.

- **Estafas digitales:** Al igual que determinados códigos maliciosos, las estafas digitales también se propagan a través de redes sociales. Sin embargo, es llamativo la imponencia que tiene la técnica de phishing dentro de las mismas.

- **Robo de información:** En el uso diario de las redes sociales, los usuarios comparten diversos datos de índole personal que pueden ser de utilidad para los agentes maliciosos. Desde la ubicación de sus lugares favoritos hasta el

nacimiento de su nuevo bebé. El robo de información en redes sociales se relaciona directamente con el robo de identidad, uno de los delitos informáticos que más ha crecido en los últimos años.

- **Grooming:** Consiste en acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad y abusar sexualmente de él (sin duda alguna una de las acciones más aberrantes que podemos encontrar). Las redes sociales son un espacio en donde este tipo de riesgos está muy latente, puesto que los groomers pueden aprovecharse del anonimato para hacerse pasar por niños y, así, llegar a sus víctimas. A continuación, gráfico de porcentaje de usuarios en distintas redes sociales:

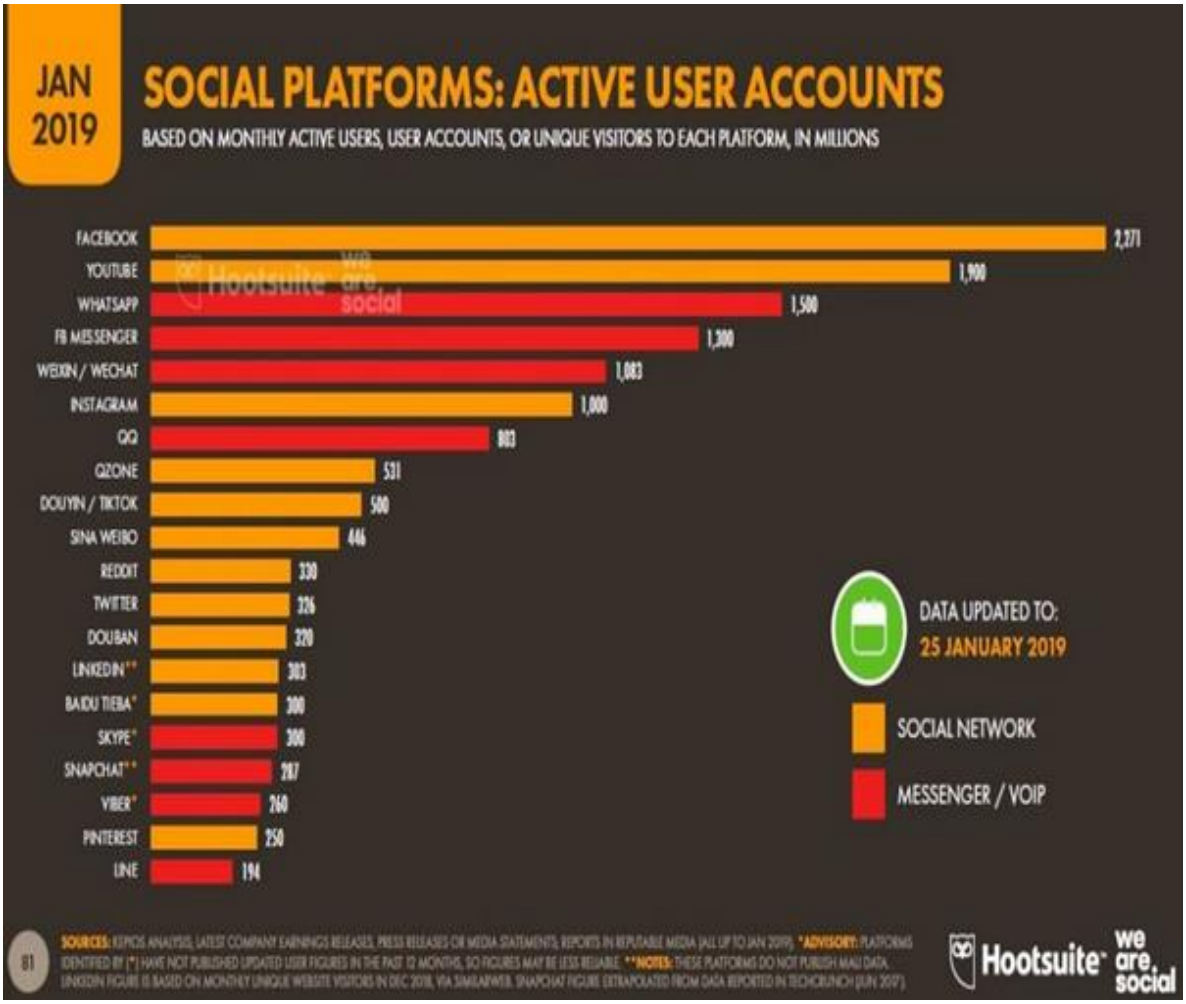
- 

Figura 3.6: Social Platforms, Active Users Accounts

Fuente (Hootsuite)

3.2.5 Confianza

La RAE (Real Academia Española) la define como esperanza firme que se tiene de alguien o algo. En definición llana tenemos que, es la seguridad o esperanza firme

que alguien tiene de otro individuo o de algo. También se trata de la presunción de uno mismo y del ánimo o vigor para obrar.

Por esta razón, la consideramos mucho más que un vector de ataque si no, como la base fundamental de cualquier tipo de arremetida en cuanto a la seguridad de la información se trata. Ya sea un ataque de ingeniería social de manera directa y personal o utilizando la técnica de phishing y esperar que la víctima muerda el anzuelo, la misma debe de estar presente para que los resultados salgan según lo planeado.

3.3 La Ingeniería Social

3.3.1 ¿Qué se conoce como ingeniería social?

Según la ingeniería social consiste en obtener información confidencial a través de la manipulación de usuarios legítimos, los cuales son el eslabón más débil en cualquier sistema de seguridad. Los criminales informáticos utilizan esta técnica para engañar a los usuarios a revelar información o a violar políticas de seguridad, sin que estos se den cuenta.

Ingeniería Social es el término utilizado para describir un grupo de prácticas que tienen como finalidad explotar la ingenuidad de un individuo. En el caso de las

organizaciones, su propósito es engañar al empleado. A razón de que las empresas suelen invertir grandes sumas de dinero en prevención contra ataques, pero solo de manera tecnológica, es común que agentes maliciosos utilicen esta práctica tan eficaz, ya que no necesitan atacar directamente la parte tecnológica de las organizaciones.

Aunque la ingeniería social se ha puesto muy de modo en estos días, no es término nuevo y novedoso. Todos somos víctimas potenciales, en el momento en que tomamos la decisión de publicar detalles personales en redes sociales o cuando hablamos con extraños sobre pormenores de nuestro trabajo somos totalmente vulnerables a ataques de ingeniería social.

Según Kevin Mitnick, quien hizo popular el término, “Ingeniería Social” se basa en 4 principios del comportamiento de las personas:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir No.
- A todos nos gusta que nos alaben.

si se pregunta ¿Qué tan efectiva es? Es tan efectiva y peligrosa que el año pasado fue la técnica más utilizada en el mundo del hacking.

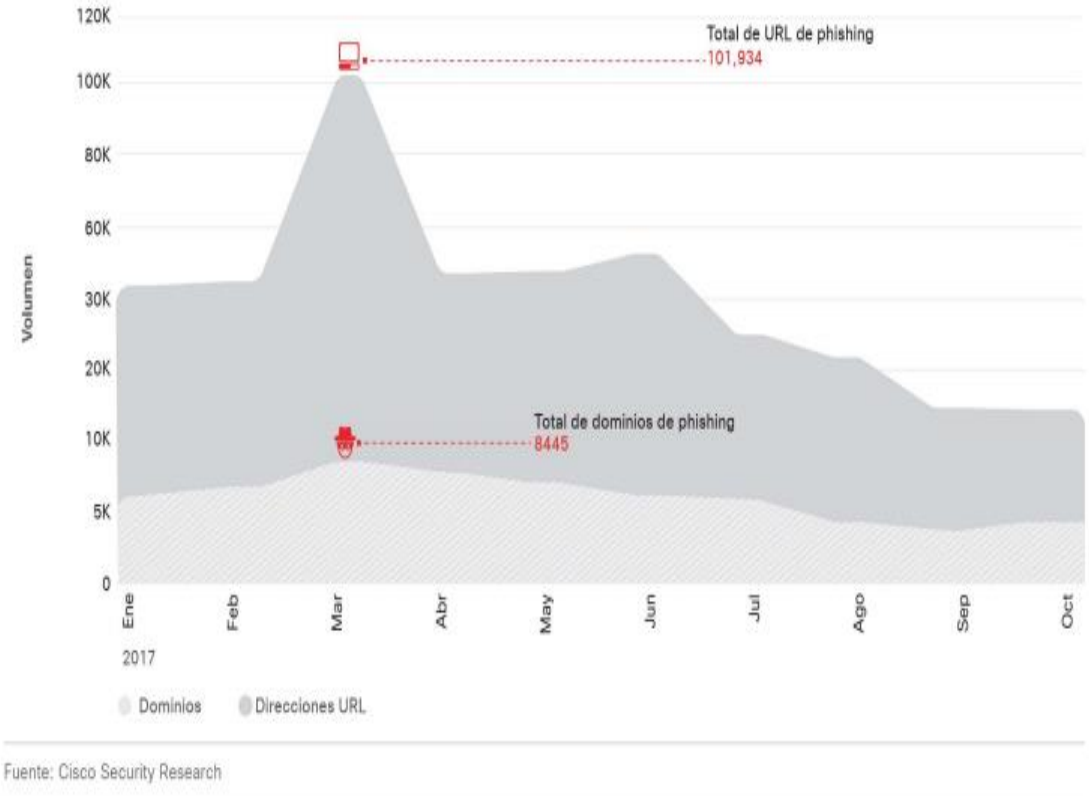


Figura 3.7: Ataques de Phishing.

Fuente (Cisco Security)

3.3.2 Objetivos de la ingeniería social

Recordando que las personas son el eslabón más débil en la cadena por la seguridad de la información y que la ingeniería social está clasificada como el lado oscuro de la psicología, no es para menos que sus objetivos predominantes

intervengan directamente con la mente de la víctima. No solo de manera física sino también de forma virtual, es un peligro y riesgo latente que viven todas las personas y organizaciones a nivel mundial. Con tal de llevar a cabo un ataque exitoso, la ingeniería social cumple con los siguientes objetivos fundamental:

- Engañar la mente de la víctima.
- Evadir todas alertas que puedan despertar en el objetivo.
- Conseguir lo deseado dejando el menor rastro posible.
- Evitar grandes gastos atacando la infraestructura tecnológica de las organizaciones.
- No levantar sospechas.
- Que el objetivo continúe en un estado mental y sentimental neutro.

3.3.3 Metodología de la ingeniería social como vector de ataque

Sea cual sea el ataque para ejecutar se debe seguir una fase previa, la cual al ser llevada a cabo con cautela y atención a los detalles puede marcar la diferencia entre un ataque pésimo y otro totalmente exitoso. Si bien las fases dentro de un ataque de ingeniería social guardan una estrecha relación con la metodología de cualquier ataque informático, es preciso destacar su estructura fundamental:

Attack Formulation (Formular ataque), selección y reconocimiento: Esta primera fase consiste en establecer el objetivo principal en un ataque de ingeniería social, luego se debe de identificar la persona/s o entidad para cumplir con el objetivo principal (el ataque). Es de gran ayuda saber y tener bien claro el escenario que se pretende atacar. Puesto que no es lo mismo obtener una contraseña de un gerente de una empresa, que información sobre empleado de limpieza.

En este apartado se comienza a realizar el perfil en cual encaja la víctima (confiado, con conocimientos informáticos, cauteloso, etc.). También se destacan las siguientes dos preguntas:

- ¿Cuál es el objetivo principal?
- ¿Cuáles o quiénes son el objetivo secundario?

Information Gathering (Recopilar información), Análisis y contacto: Esta fase cuenta con la peculiaridad que se identifican y evalúan las fuentes de información acerca del objetivo previamente establecido. Esta fase es de vital importancia ya que es donde se realiza el contacto con la víctima mediante cualquiera de los vectores antes vistos. Del mismo modo, se construye la relación de confianza y se va ganando terreno en la relación que llevará a la víctima revelar la información deseada por el agente malicioso.

Este paso se puede clasificar en ocasiones como un círculo continuo hasta obtener lo deseado, es decir, se repite hasta que el ingeniero social esté convencido de que

se ha obtenido suficiente información para que pueda comenzar su preparación para el ataque. Dentro de este proceso podemos identificar los siguientes pasos:

- **Identificar las fuentes potenciales.**
- **Recopilar información de las fuentes.**
- **Fuentes Públicas:** Sitios Web, Redes Sociales, Blogs, Foros
- **Fuentes Privadas:** Dumpster diving
- **Evaluar la información recopilada:** Relevante y no relevante

Preparation (Preparación): Luego de haber descartado la información no relevante y analizar en qué renglón se ubica el objetivo, el ingeniero social se asegura de que todo esté según lo planeado antes de empezar el ataque. Es por ello que en esta fase se analiza la información y se desarrolla un plan de acción para comenzar a abordar el objetivo.

Así como las demás fases, la preparación posee pasos a seguir dentro de la misma. El primer paso de esta fase es combinar toda la información recopilada para obtener una imagen más amplia del ataque planificado. Por lo tanto, el victimario puede obtener vista combinada de los escenarios que se pueden utilizar.

Según Tahiri Dicovec, esta vista combinada del escenario se puede utilizar para realizar el pretexting dónde se diseña un escenario para atraer al objetivo a una acción requerida. Un pretexting efectivo debe ser creíble y resistir el escrutinio del

objetivo, a menudo se basa en la calidad de la información recopilada sobre la personalidad del objetivo.

Posterior a todo esto se desarrolla un vector de ataque, el cual a juicio del atacante es el adecuado para la víctima y las situaciones presentadas. Este paso presenta el siguiente esquema:

Combinación y análisis de la información recopilada:

- Imagen amplia del ataque planificado.
- Se puede construir el pretexting.

Desarrollo de un vector de ataque:

- Meta
- Objetivo
- Ingeniero social
- Medio
- Principios de Cumplimiento
- Técnicas

Develop Relationship (Desarrollar relación): En esta fase se establece una línea de comunicación y se comienza a construir una relación. Como ya sabemos el

desarrollo de una relación fructífera con el objetivo es una parte fundamental del ataque de ingeniería social. Recordando que, si no es posible establecer la confianza, es muy poco probable que la información requerida se obtenga del objetivo.

El primer paso para desarrollar una buena relación con el objetivo es tener una buena base en cuanto a pretexting (pretextos) se trata, pues los mismos son los que nos mantendrán enlazados con la víctima. Segundo tenemos el desarrollo verdadero de la relación con el objetivo fuera de los pretextos, llevándonos así a una construcción real de la relación. A continuación, su esquema:

Establecer la comunicación:

- A través de algún medio.

Construcción de relaciones:

- Construir una relación armoniosa.

Exploit Relationship (Explotar relación): El vínculo de confianza se ha creado, el objetivo no sospecha en lo más mínimo lo que se aproxima, es hora de sacarle el mayor provecho a esa confianza creada, tiempo de empezar el ataque. Es claro destacar que en esta fase se utilizan diferentes métodos de manipulación para provocar el tipo de emociones deseadas en la víctima, una vez el objetivo se encuentra en el estado emocionales y mental deseado se puede empezar con el ataque.

Debrief (Debrief): Si pensaban que los ingenieros sociales no tenían nada de clase están totalmente equivocados, ¿Les causa risa no? pero estamos en lo cierto. En esta fase, el agente malicioso vuelve a tratar con objetivo y mantiene su estado emocional de acorde a como lo necesita. En ese momento lo esencial es que el objetivo no se sienta extraño en la relación, de esta manera no podrá notar que ha estado bajo ataque. Es necesario sacar a relucir que el objetivo no debe sentir que fue atacado, por lo cual existe una etapa de ¨mantenimiento¨.

Podemos resumir esta fase en el siguiente esquema:

Mantenimiento:

- Restablecer el estado emocional del objetivo.

Transición:

- Objetivo Satisfecho.
- Se necesita más información.

3.3.4 Aspecto psicológico de la ingeniería social contra el ser humano

Como es de esperarse son varios los perfiles que encuadran bien con el de una víctima de ingeniería social, pero para no extendernos nos referiremos al más común: Aquel que tiene el complejo de superhéroe ¿Quién al ver que alguien pide ayuda no ha estado tentado a ayudar? Estadísticamente sería 70% de la población

mundial, porque el ser humano originariamente nace bueno, el 30% restante son los sociópatas o psicopáticos. (EE. UU.-DSM4 Manual diagnóstico y estadísticas de trastornos mentales).

Algo que todos debemos admitir es que al menos una vez en nuestras vidas hemos sentido el interés de ayudar y ser reconocidos y ratificados por la acción que se ha realizado. Debido a esto, es importante resaltar como el aspecto psicológico más importante de la ingeniería social. El victimario sabe que, si pide ayuda y hay tres personas, al menos una se ofrecerán y habrá otra que le seguirá los pasos.

Por consiguiente, dicho victimario sí es un sociópata. Sus características son parecer inofensivo, indefenso, preocupado o deprimido. En realidad, es frío, calculador, mitómano y siempre sabe lo que hace: sabe diferenciar el bien del mal, pero no le importa (España-CTIO, Clasificación estadística internacional de enfermedades y problemas de salud).

A fin de prevenir estos ataques, es de suma importancia que los gerentes y administradores de TI enfaticen a la hora de enseñar y educar a los empleados sobre estas técnicas. En ese caso, priorizando que la ayuda es bien vista pero siempre y cuando no incluya una situación donde haya que mostrar documentación o información sensible personal o de la propia organización.

3.3.5 Características de la víctima

Dejando claro que no todos los objetivos son iguales, que cada persona o entidad posee sus propias cualidades que, aunque se puedan compartir son ciertamente únicas en cada caso. Aquí podemos apreciar algunas de las características que pueden llegar a compartir las víctimas de un ataque de ingeniería social.

- Actitud de servicio y proactividad.
- Reconocimiento por su ayuda y trabajo.
- Experiencia en su área o trabajo.
- Necesidad de demostrar sus conocimientos y dominio de la información.
- “Alma de la fiesta” o amiguero.
- Resentimiento hacia una persona o la institución en general.
- Insatisfacción con el cargo o puesto en la institución.
- Resistencia al cambio.
- Niveles de tolerancia bajos, no apto para la presión personal influenciada por el medio.
- Facilidad para inducir una conducta o acción.
- Falta de capacitación o entrenamiento, entrenamiento insuficiente e inconsistente.

- Descuido.
- Relaciones personales.
- Presentación física.
- Codicia.

Al leer estas cualidades podemos darnos cuenta de que somos más vulnerables de lo que alguna vez llegamos a pensar, pues ¿Quién no posee o se identifica levemente con algunas de las características anteriores?

3.3.6 Cualidades del atacante

Aunque los ataques de ingeniería social pueden ser llevados a cabo a través de sus diferentes vectores, sale a relucir ciertas cualidades que destacan sobre los agentes maliciosos. Además de poseer la destreza de llevar a la víctima hasta la zona de confort deseada, es importante dominar o poseer basto conocimiento sobre las siguientes características:

- **Conceptualización y definición de objetivos:** Conocer el perfil de la víctima facilita el trabajo.
- **Facilidad de palabra y persuasión:** Recordando que la ingeniería social pare totalmente de la psicología humana, es importante destacar en la versatilidad a la hora de interactuar y persuadir al objetivo.

- **Infundir confianza:** Si señor, la misma que sube en escalera y baja en ascensor, si no se logra transmitir la misma al objetivo, el ataque de seguro será un fracaso total.

- **Improvisación:** Sabiendo que no siempre sale como lo deseado, un buen ingeniero social debe ser creativo y eficaz a la hora de crear soluciones en problemas de última hora. ¿Se imaginan echar abajo un plan de 6 meses solo por no idear las palabras correctas en un momento de apuros?

- **Planeación y precaución (no dejar rastros):** Como vimos en las fases de un ataque informático, es importante que se cubran todas las bases. no serviría de nada lograr el ataque con perfección si el agente malicioso será arrestado al siguiente día.

- **Paciencia:** Un don que no todos poseen, teniendo claro que la ejecución no siempre va a la par con la planeación se tendrá un gran panorama de las situaciones que puedan surgir, de esta manera manteniendo el control con mayor facilidad.

- **Sobrellevar el tema y autocontrol:** A sabiendas que el objetivo puede estar claramente a la defensiva, se debe tener en cuenta el autocontrol ante toda situación que se presente.

- **Saber cómo y dónde buscar la información:** Horas y horas de búsqueda de información sobre el objetivo no servirán de nada si el agente malicioso

no tiene claro dónde buscar y dentro de su investigación que es importante y que no. asociada perfectamente con la fase del escaneo.

3.3.7 La ingeniería social inversa, técnica de migas de pan

Según un artículo anónimo publicado en el blog Jummp, a diferencia de la ingeniería social donde el individuo se muestra más activo, poniéndose en contacto con las personas que pueden suministrarle la información necesaria para atacar o introducirse en un sistema, la ingeniería social inversa es pasiva, ya que en ella se pone la trampa y se espera cautelosamente a que alguien caiga en ella (la trampa puede estar dirigida a un colectivo concreto o bien a una generalidad de usuarios).

Partiendo de esta breve definición podemos enlazar la ingeniería inversa directamente con el tipo de ataque phishing, pues dentro del mismo se coloca o envía una carnada con la intención de que sea mordida. Tomando en cuenta que es una técnica más calmada, es bastante común pues el atacante no necesita de un sobreesfuerzo dentro del proceso de ataque. Esta técnica requiere de paciencia y más que nada infundir confianza a través de la carnada utilizada.

En este caso el usuario (objetivo) es quién se pone en contacto (utilizando cualquiera de los medios que se suelen utilizar en la ingeniería social: de persona a persona, teléfono, sitio web, correo electrónico, red social, etc.), sin tener idea alguna con la persona que desea obtener información del mismo y una vez

establecido el contacto, el agente malicioso obtiene la información necesaria para realizar el ataque o la intrusión.

También llamada técnica de las migas de pan, pues consiste en ponerle al usuario las migas de pan para llegar a él, así como si se tratara de un ave siguiendo un camino de alimento. Destacando que esta variante no tiene por qué actuar siempre una persona para obtener información, ya que este tipo de prácticas puede ser llevado a cabo con el acceso a un sitio web y descarga de un determinado software que se encuentra infectado por un virus (en todas sus formas). A continuación, un ejemplo sencillo:

Se descubre un sitio web en el que dicen que son expertos en arreglar determinados problemas relacionados con el ordenador. Una vez que la persona se pone en contacto con ellos a través de uno de los medios indicados anteriormente, obtienen la información que necesitan para un futuro ataque.

3.4 Ingenieros Sociales más reconocidos

3.4.1 Kevin Mitnick

El 15 de febrero de 1995 el FBI lograba dar caza a Kevin Mitnick, el considerado por el New York Times como "el hacker más buscado de todo el ciberespacio". Mitnick acabaría pasando cinco años en prisión por diversos delitos, incluidos ocho meses en una celda de aislamiento.

¿Por qué tanto tiempo en aislamiento? Pues porque alguien convenció al juez de que era capaz de "iniciar una guerra nuclear silbando en un teléfono público". Aquella decisión aumentó el mito de un hacker que logró mucho más por su habilidad con la ingeniería social que por su capacidad técnica.

Mitnick descubrió muy pronto a aprovechar las debilidades de los sistemas que usaba en su día a día. Todo empezó con los billetes de autobús que usaba para desplazarse en Los Ángeles, y que contaban con una forma particular de estar agujereados según el día, la hora o la ruta de cada autobús.

El joven Mitnick logró descubrir dónde comprar la máquina con la que se agujereaban esas tarjetas, consiguió un montón de tarjetas preparadas para ser perforadas en una terminal en el que los conductores dejaban sus libros de tarjetas sin vigilancia, y así fue como acabó viajando de un lado a otro de la ciudad sin pagar.

Puede que aquella primera aventura con premio (y sin castigo) acabara definiendo su actividad posterior, que pronto acabaría centrándose en la ingeniería social, una práctica con la que lograba obtener información de todo tipo de sistemas manipulando a usuarios legítimos de esos sistemas.

La técnica básica era (y es) tan eficiente como simple, y Mitnick la repetía constantemente. En uno de sus primeros ataques de ingeniería social explicaba cómo necesitaba un número de solicitante para "pinchar" el Departamento de Vehículos de Motor (DMV). Para lograrlo llamó a una comisaría y se hizo pasar por alguien del DMV. Allí le preguntó al interlocutor: "¿Su código de solicitante es el 36472?", a lo cual el agente contestó: "No, es el 62883". ¿Qué sencillo no?

Ese principio básico de la ingeniería social se unía a otro esencial: la gente suele ser el eslabón más débil de una cadena de seguridad, porque "la gente siempre esa intención de ayudar".

Uno de los primeros ejemplos lo tenemos en su intrusión en un sistema llamado 'The Ark' que la empresa Digital Equipment Corporation (DEC) usaba para desarrollar su sistema operativo RSTS/E.

Mitnick contaba con el número de teléfono que daba acceso al sistema, pero no tenía usuario y contraseña, así que se hizo pasar por uno de los desarrolladores de RSTS/E para pedirle a un administrador que le reseteara la contraseña con la excusa de que no podía autenticarse en la que usaba siempre.

En cinco minutos había logrado acceso al sistema aprovechando esas técnicas, y más tarde haría uso de procesos similares para luego dejar pequeños troyanos con los que recolectaba contraseñas de otros usuarios o dejaba puertas traseras con las que poder acceder a estos sistemas posteriormente sin ser descubierto.

Durante buena parte del tiempo que pasó en prisión los responsables y seguidores de la famosa revista '2600: The Hacker Quaterly' organizaron una campaña llamada 'FREE KEVIN' en la que trataban de que la justicia de Estados Unidos liberara a Mitnick. Aquella campaña supuso el contrapunto a la imagen de villano que John Markoff, periodista de The New York Times, había dado de Mitnick en un **célebre artículo** del 4 de julio de 1994.

En aquel artículo Markoff calificaba a Kevin Mitnick como "el más buscado del ciberespacio" y le atribuía delitos como los de haber accedido al NORAD (North American Air Defense Command), algo que el hacker afirmaba que era imposible si tenemos en cuenta que sus sistemas estaban aislados de INTERNET.

Tras su salida de la cárcel en enero de 2000, a Mitnick se le prohibió un ordenador o incluso un teléfono móvil durante los tres años siguientes. Apeló aquella decisión y logró una sentencia a su favor para poder usar esos dispositivos, pero tuvo que acceder a no obtener beneficios económicos de películas o libros basados en su actividad durante 7 años. Tras su salida de la cárcel en enero de 2000, a Mitnick se le prohibió un ordenador o incluso un teléfono móvil durante los tres años siguientes. Apeló aquella decisión y logró una sentencia a su favor para poder usar esos

dispositivos, pero tuvo que acceder a no obtener beneficios económicos de películas o libros basados en su actividad durante 7 años.

En diciembre de 2002 a Mitnick se le consideró "suficientemente rehabilitado" y se le concedió una licencia de radioaficionado, y posteriormente acabaría fundando **Mitcnick Security Consulting LLC**, una empresa de seguridad informática en la que se dedica básicamente a lo mismo que hacía antes de ser arrestado, pero con el permiso expreso de las empresas que le contratan para que analice su seguridad (Hacking ético).

Mitnick da conferencias por todo el mundo y se ha convertido en una figura pública también en redes sociales **como Twitter**.

3.4.2 Mathew Weigman

Sus inicios un niño de 15 años llamado **Matthew Weigman**. Un chico ciego, solitario y obeso que vivía con su madre en un barrio de clase trabajadora en Boston. El joven era un adolescente tímido de cabeza rapada que solía pasar los días escondido en su habitación. Allí gastaba la mayoría de las horas del día hablando a través de las líneas de chat de teléfono gratuitas.

Por teléfono Weigman no era Weigman, era Lil ´Hacker, el miembro más experto de una pequeña banda que se dedicaba a realizar bromas telefónicas, la mayoría de ellos phreakers (apasionados del sistema telefónico). Weigman tenía ciertos

paralelismos con los villanos de los cómics. El joven se había transformado por un trágico accidente. Descubrió cuando desde muy pequeño que su agudo oído le permitía hacer cualquier cosa tras el teléfono. Por ejemplo, era capaz hacerse pasar por cualquier voz, también podía memorizar un número de teléfono por el sonido y el timbre de los botones al marcarlo o de descifrar el funcionamiento interno de un sistema telefónico por las frecuencias de una llamada, lo que Weigman denominaba como “canciones”.

A los 10 años había encontrado el lugar perfecto para huir del mundo real. Se trataba de una línea telefónica, una party-line. Probablemente se sintió fascinado por un sistema que le permitía hablar bajo el manto del anonimato. Podía socializar sin miedo a que se burlaran de él por su dolencia. un día comienza a presionar números aleatorios en su teléfono, sólo para ver qué pasaría. Y de repente y tras presionar el botón de la estrella, una voz computarizada le dice, “moderador on”. No tenía ni idea de lo que significaba, pero cuando posteriormente golpeó sobre la tecla del asterisco, la voz comenzó a marcar el número de teléfono privado de cada persona en la sala de chat en la que se encontraba. Matt había descubierto una herramienta secreta a través de la cual un administrador de party-line podía monitorear el sistema. Dicho de otra forma, cada vez que alguien se metiera con él, podría acceder a su número de teléfono.

The silence:

Con 14 años Weigman ya era capaz de engañar al personal de AT&T y Verizon para que divulgaran información privilegiada (por ejemplo, con números de supervisores o contraseñas) que le dieran plenos poderes del sistema. Si oía la voz de un supervisor una sola vez ya podía **imitarla** con gran precisión al llamar a uno de los subordinados del hombre. Si escuchaba a alguien marcar un número, el joven podía memorizar los dígitos sólo con el tono. Su truco favorito era conseguir que un técnico telefónico acudiera a su casa para luego hacerse pasar por dicho técnico en el teléfono y extraer códigos y datos de compañeros de trabajo desprevenidos.

El chico fue escalando posiciones entre los diferentes grupos de phreakers, y lo hacía sin miedo a nada ni a nadie, atacando sin piedad a cualquiera que se le pusiera por delante: acosándolos, desconectándoles las líneas, desenterrando sus datos personales para usarlos como amenaza o venganza. Si ser un phreaker era entrar de lleno en el juego de la información, Matt era el maestro indiscutible.

Sin embargo, este giro que había tomado su vida comenzó a tornarse en algo cada vez más peligroso. El chico empezó a utilizar sus nuevas habilidades para facturar compras a tarjetas de crédito falsas. Weigman se había convertido en un maestro de lo que los phreakers llaman ingeniería social, es decir, había aprendido la jerga de la industria telefónica, lo que le permitió manipular a los trabajadores de las grandes compañías. El 26 de junio del 2009 Matthew Weigman **fue sentenciado** a 11 años y tres meses de cárcel por conspiración y asaltos telefónicos (swatting).

3.5 Casos reportados más recientes implementando ingeniería social como vector de ataque

3.5.1 Ubiquiti Networks

Ubiquiti Networks es un proveedor de origen estadounidense de servicios de redes de alto rendimiento para organizaciones. En 2015 sufrió un ataque que le hizo perder aproximadamente 39.1 millones de dólares. Con tal de conseguir su objetivo, los cibercriminales escribieron algunos correos haciéndose pasar por miembros ejecutivos de la empresa, y solicitaron a algunos empleados del área financiera que realizarán transferencias de grandes cantidades de dinero a una cuenta bancaria en particular. Como era de esperarse, esta era propiedad de los agentes maliciosos.

Esta técnica de ingeniería social se aprovecha de ciertas debilidades del ser humano, como ya hemos visto el hecho de ser servicial es el más común, ya que eso podría incidir en el reconocimiento por parte de los superiores. También se beneficia en que hay muchas personas que son incapaces de negarse a hacer algo que, pensado fríamente, podría resultar perjudicial.

Como era de esperarse absolutamente nadie se metió dentro de los sistemas informáticos (mayor gasto de recursos) de Ubiquiti Networks, tampoco sustrajeron los datos de la compañía. En este caso, la brecha de seguridad estaba en los

propios empleados, que carecían de la formación, y desconocían los procedimientos necesarios para protegerse ante este tipo de estafas (usuarios no entrenados).

CAPÍTULO IV:

ADMINISTRADORA DE RIESGO LABORALES (ARL)

4.1. ¿Cómo surge la ARL?

4.1.1. Historia de la ARL

A principio de los años 1945-1946 el trabajador dominicano vivía en las peores condiciones infrahumanas que ha existido en toda la historia dominicana. Trabajaban más de 12 horas al día por salarios de verdadera miseria. Es en enero de 1946 el detonante de la clase obrera. Los obreros azucareros de La Romana y de San Pedro de Macorís, organizados y dirigidos principalmente por los señores Báez y Núñez, se declaran en huelga por una serie de reivindicaciones, entre ellas y la más importante, un justo aumento salarial. A partir de la huelga general de enero, los trabajadores azucareros y no azucareros organizados en gremios comienzan a hacer protestas y algunas que otras importantes huelgas, conllevando a la formación del Congreso Obrero Nacional del 24 de septiembre de 1946, organizado por la Confederación Dominicana del Trabajo (CDT).

Este movimiento sindical logró reducir a 8 horas la jornada de trabajo. Además, con las duras críticas de los exiliados por el régimen y de los organismos internacionales como la Central de Trabajadores de América Latina (CETAL) y la Organización Internacional del Trabajo (OIT) y con el propósito de evitar acontecimientos como los de enero de 1946, sumado al falso carácter paternalista del régimen y en su afán de presentar a la República Dominicana como un país totalmente democrático.

Rafael Leonidas Trujillo crea en el supuesto beneficio de los trabajadores, las leyes No. 1376 del 17 de marzo de 1947 y la No. 2920 del 11 de junio de 1951, que dan lugar a la creación de la Caja Dominicana de Seguros Sociales y al Código Trujillo del Trabajo, respectivamente.

La Caja Dominicana de Seguros Sociales fue concebida bajo los principios bismarckianos del sistema alemán, con el propósito de cubrir los riesgos de enfermedad, maternidad, invalidez, vejez y muerte del trabajador dominicano. El sistema de seguros sociales es puesto en vigencia mediante la Ley no. 1896 del 30 de diciembre de 1948 (Gaceta Oficial No. 6883 del 14 de enero de 1949), la misma Ley que ha sido modificada en diversas ocasiones.

A partir del 11 de diciembre de 1962, la Caja Dominicana de Seguros Sociales pasa a llamarse Instituto Dominicano de Seguros Sociales (IDSS) mediante la Ley No. 8952 del Consejo de Estado, precedido por Rafael F. Bonnelly. Igualmente, la Ley establece la autonomía de la institución mediante la Dirección Administrativa, Técnica y Financiera de un Consejo Directivo de composición tripartita, donde están representados los Empleados, Trabajadores y el Estado.

4.1.2. Ley 87-01

De acuerdo a la Ley 87-01 destinado para prevenir y cubrir los daños ocasionados por accidentes de trabajo y/o enfermedades profesionales. Comprende toda lesión

corporal y todo estado mórbido que el trabajador sufra con ocasión o por consecuencia del trabajo que presta por cuenta ajena. Incluye los tratamientos por accidentes de tránsito en horas laborables y/o en la ruta hacia o desde el centro de trabajo.

Se rige por las normativas:

- La Ley 87-01, que crea el Sistema Dominicano de Seguridad Social (SDSS).
- El Reglamento del Seguro de Riesgos Laborales.
- Las Resoluciones del Consejo Nacional de Seguridad Social (CNSS) y de la Superintendencia de Salud y Riesgos Laborales (SISALRIL) que así lo establezcan.

Los empleadores y trabajadores bajo dependencia deben estar afiliados al Seguro de Riesgos Laborales (SRL).

Se afilia al usuario automáticamente, cuando el empleador registrar su empresa e inscribe sus trabajadores en la Tesorería de la Seguridad Social (TSS).

Las prestaciones son:

- Prestaciones en especie.
- Atención médica y asistencia odontológica;
- Prótesis, anteojos y aparatos ortopédicos, y su reparación;

Prestaciones en dinero:

- Subsidio por discapacidad temporal
- Indemnización por discapacidad
- Pensión por discapacidad
- Pensión de sobrevivencia.

Las prestaciones en especie se otorgan a través de la red de Prestadores de Servicios de Salud (PSS) contratadas por la Administradora de Riesgos Laborales Salud Segura (ARLSS) a nivel nacional. Las prestaciones en dinero se otorgan en las oficinas de la ARLSS.

El porcentaje para cotizar contiene dos componentes:

- Una cuota básica fija del uno por ciento (1%) para todos los empleadores.
- Una cuota adicional variable desde cero puntos uno (0.1%) hasta cero puntos tres por ciento (0.3%), establecida en función de la rama de actividad y del riesgo de cada empresa, dichos porcentajes se aplican sobre el monto del salario cotizable de cada trabajador.

4.2. Enfoque de la ARL

4.2.1 Misión, visión, valores y principios

Misión

"Garantizamos a los beneficiarios del Seguro de Riesgos Laborales un sistema de prevención, prestaciones económicas y de salud basados en la calidad" (ARLSS,2019).

Visión

"Ser reconocidos en el entorno nacional e internacional por la excelencia en la gestión del Seguro de Riesgos Laborales y la promoción de espacios de trabajo saludables permanentes" (ARLSS,2019).

Valores

- Transparencia
- Solidaridad
- Compromiso
- Equidad
- Calidez

Principio Corporativos

- Excelencia.
- Transparencia.
- Equidad.
- Innovación.

4.2.2 Organigrama

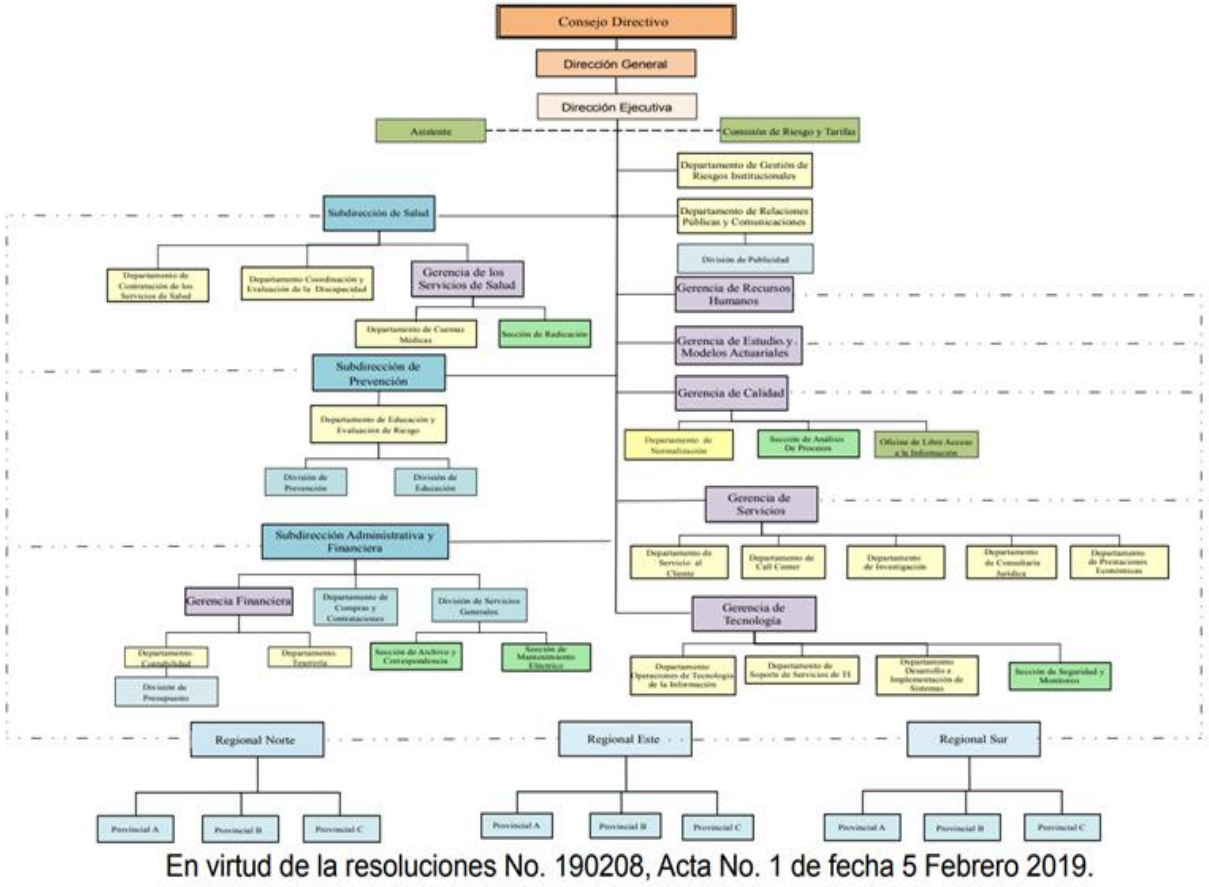


Figura 4.1: Organigrama de la ARLSS

Fuente (ARLSS, 2019)

4.3. Entrevistas o Cuestionarios

En nuestra labor por recopilar opiniones e ideas de primera mano, tomamos la decisión de realizar tres preguntas básicas a algunos encargados y gerentes dentro

de la institución que a nuestro parecer son fundamentales a la hora de trazar las metas de la Administradora de Riesgos Laborales (ARL). Las preguntas fueron las siguientes:

1. Desde su punto de vista debido a su función desempeñada en la Administradora de Riesgos Laborales (ARL), ¿Cuál es el objetivo general de la institución y cuáles son sus objetivos específicos?
2. ¿Qué impacto posee la Administradora de Riesgos Laborales en la sociedad dominicana?
3. ¿Cómo se proyecta o perfila la institución en un plazo de 10 años?

Por acuerdo previo de anonimato y privacidad los nombres de los participantes, así como sus cargos ocupados dentro de la institución no serán difundidos en esta investigación. A continuación, las respuestas de los encargados y gerentes participantes:

Encargado	**Desde su punto de vista debido a su función desempeñada en la Administradora de Riesgos Laborales (ARL), ¿Cuál es el objetivo general de la institución y cuáles son sus objetivos específicos?**	**¿Qué impacto posee la Administradora de Riesgos Laborales en la sociedad dominicana?**	**¿Cómo se proyecta o perfila la institución en un plazo de 10 años?**

Primer encargado/a respondió	Objetivo general: Velar por el cumplimiento de la ley 87-01 y sus normas complementarias para garantizar una cobertura a nuestros afiliados y beneficiarios con eficacia y calidad. Objetivos específicos: • Cubrir los daños ocupacionales a los trabajadores por consecuencia de un accidente de trabajo o una enfermedad profesional. • Garantizar prestaciones en servicios de la salud.	La misma posee un impacto muy importante en nuestra sociedad, debido a la protección que otorga tanto al afiliado como a su núcleo, en casa de fallecimiento del trabajador o del pensionado acorde a lo establecido en art. 187 de la ley 87-01.	Como un instituto transparente, el cual presente un funcionamiento apegado a las leyes vigentes, brindando la cobertura y protección para la cual ha sido creado; en beneficio de la población según corresponda.

	• Prevención y protección de los trabajadores.		

Tabla 4.1 Repuesta de los encuestados sobre la ARL (1)

Fuente (Propia)

Encargado	**Desde su punto de vista debido a su función desempeñada en la Administradora de Riesgos Laborales (ARL), ¿Cuál es el objetivo general de la institución y cuáles son sus objetivos específicos?**	**¿Qué impacto posee la Administradora de Riesgos Laborales en la sociedad dominicana?**	**¿Cómo se proyecta o perfila la institución en un plazo de 10 años?**
Segundo encargado/a respondió	Objetivo general: Es una institución cuyo objetivo principal es cubrir las contingencias de origen laboral (accidentes de trabajo y enfermedad	Ha impactado de manera positiva a la población dominicana, específicamente al trabajador activo que en su mayoría es quien suple económicamente a su núcleo cercano y con el nacimiento	Se proyecta íntegro para seguir siendo la institución líder en la protección de los riesgos laborales y la prevención de imprevistos

	profesional), tanto en el aspecto económico (subsidios, discapacidad temporal y pensiones). También indemnizaciones por discapacidad permanente, como cobertura de la especie: gastos médicos en general. Objetivos específicos: • Tiene a su cargo la administración del seguro de riesgos laborales, el cual es un componente de la seguridad social. • Protección a los empleados afiliados al sistema dominicano	del seguro que administra los riesgos, está protegido ante un accidente o enfermedad profesional.	en el ambiente laboral, así como también ser una institución de referencia internacional.

	de seguridad social.		

Tabla 4.2 Repuesta de los encuestados sobre la ARL (2)

Fuente (Propia)

Encargado	**Desde su punto de vista debido a su función desempeñada en la Administradora de Riesgos Laborales (ARL), ¿Cuál es el objetivo general de la institución y cuáles son sus objetivos específicos?**	**¿Qué impacto posee la Administradora de Riesgos Laborales en la sociedad dominicana?**	**¿Cómo se proyecta o perfila la institución en un plazo de 10 años?**
Tercer encargado/a respondió	Objetivo general: Promover un sistema de prevención y control de los riesgos laborales, así como la administración y pago de las prestaciones del seguro de riesgos laborales.	Su impacto está completamente dirigido a el manejo eficiente y oportuno del pago de las prestaciones en especie y económicas.	Con vistas al futuro teniendo en su poder la exclusividad de una nueva ley la cual crea una institución única de la rama del SNSS con una respuesta satisfactoria a los afiliados del

	Objetivos específicos: • Promoción del estudio, conocimiento y atención integral de la salud de los trabajadores. • La contratación de servicios de salud para la atención de los afiliados por enfermedad profesional, producto del trabajo y accidentes laborales. • Garantizar el pago oportuno de las prestaciones en especie y económicas.		seguro de riesgos laborales.

Tabla 4.3 Repuesta de los encuestados sobre la ARL

Fuente (Propia)

4.4. Encuesta y Análisis

Con la finalidad de adquirir respuestas concisas y de primera mano con relación a qué tanto saben los empleados de la Administradora de Riesgos Laborales acerca de la seguridad de la información, objetivos y ataques dentro de la misma; aplicamos una encuesta de manera anónima la cual arrojó los siguientes resultados:

4.4.1 Genero

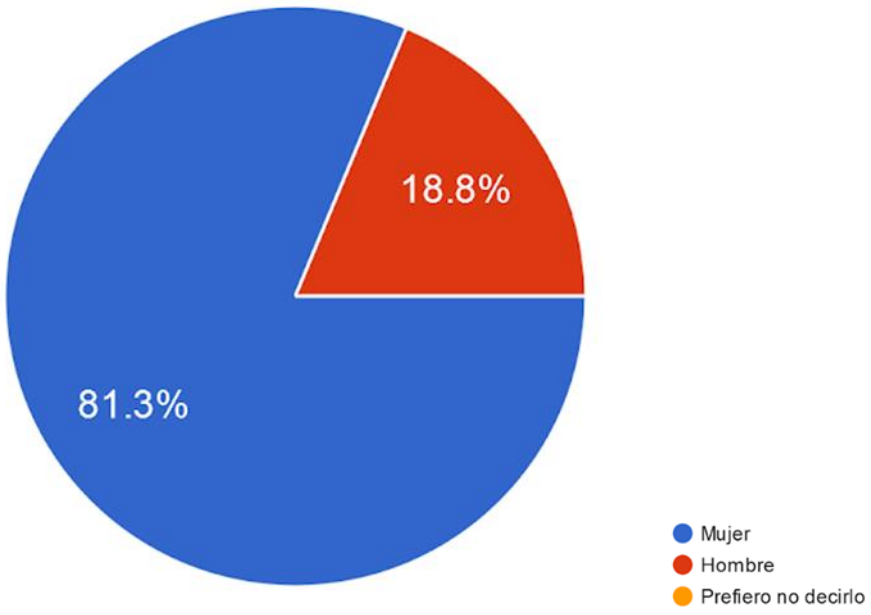


Figura 4.2. Genero de los encuestados

Fuente (Propia)

El género dominante en la institución es el femenino, el cual se encuentra altamente distribuido en las distintas plazas de trabajo que posee la institución.

4.4.2 ¿Qué edad tiene?

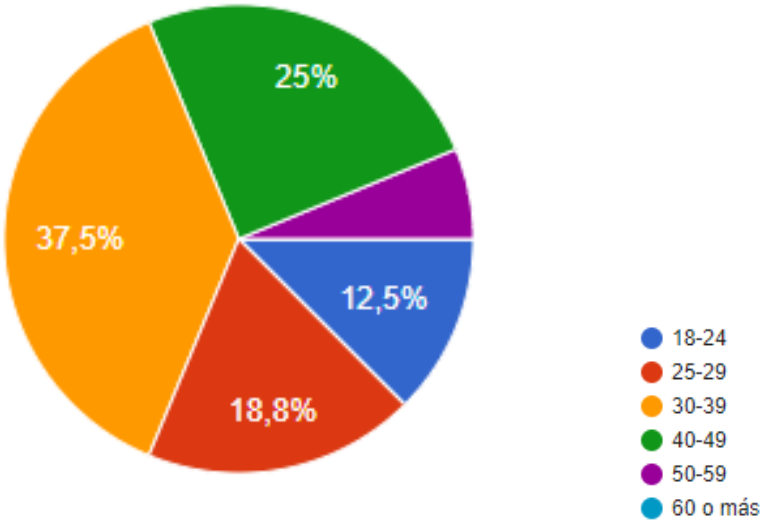


Figura 4.3 Edad de los encuestados

Fuente (Propia)

Un dato interesante es que solo el 12.5 % de los encuetados cumplía con la característica de poseer entre 18 y 24 años, en otro orden es claro que las edades dominantes van de 30 a 39 años, ¿tendrá esto que ver con la confianza que quieren depositar en sus afiliados?

4.**4.3 ¿A qué departamento usted pertenece?**

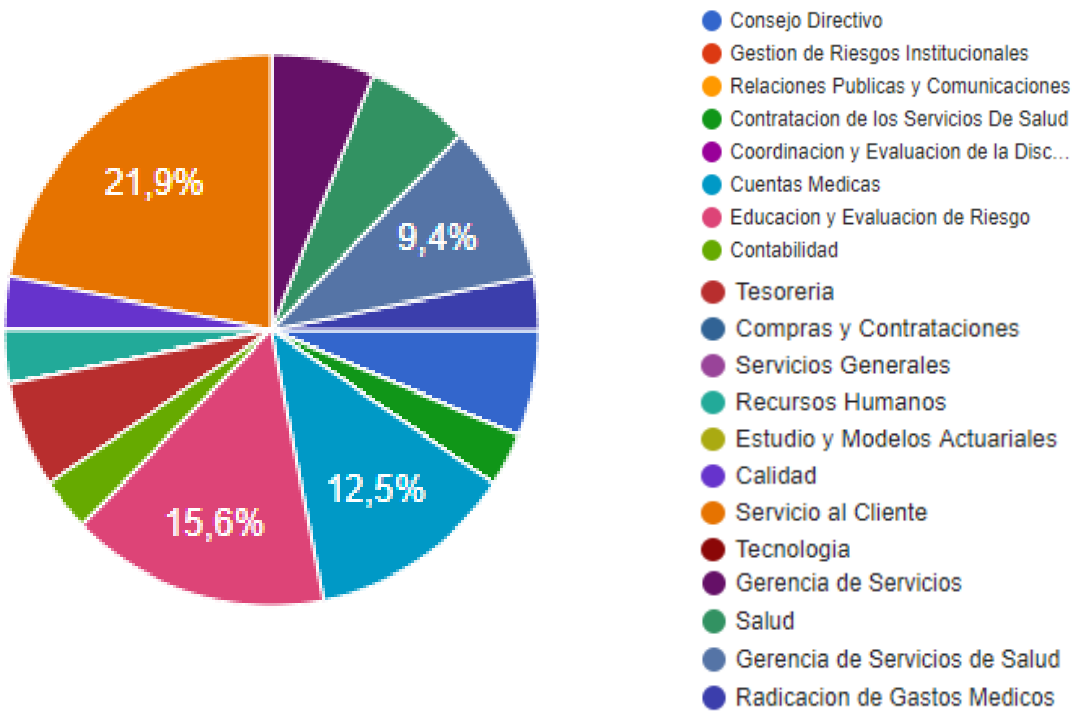


Figura 4.4 Departamentos que pertenecen los encuestados

Fuente (Propia)

Como se aprecia claramente en las imágenes anteriores, el 21.9 % de los empleados encuestados pertenecen al departamento de servicio al cliente, esto así porque son los que sustentan la línea directa de interacción con los afiliados. Los mismos brindan informaciones vía telefónica y de manera personal cuando es requerido, por lo que entendemos que son altamente potenciales a sufrir un ataque de ingeniería social en sus diferentes vertientes.

4.4.4 ¿Usted, posee algún conocimiento relacionado a la informática fuera de sus requerimientos laborales?

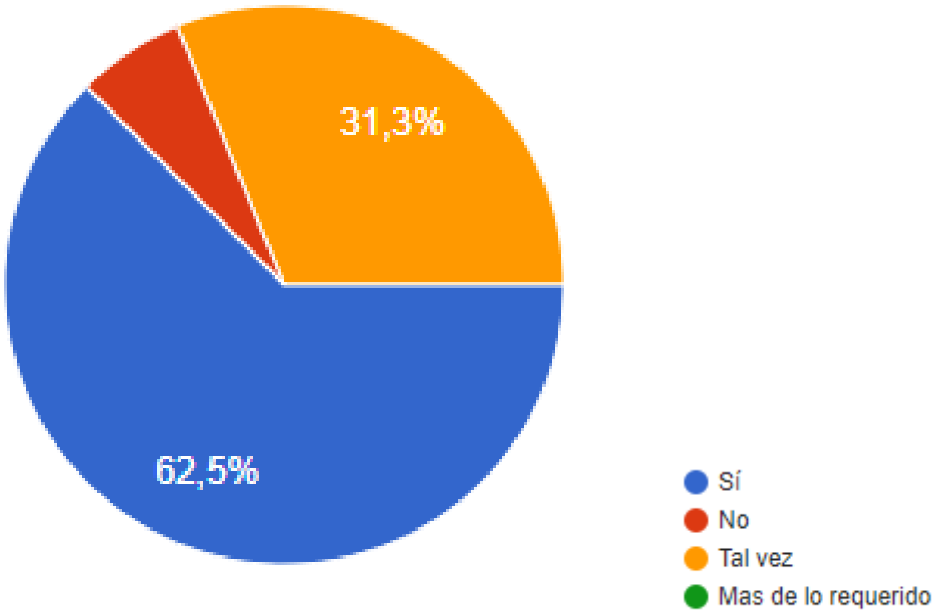


Figura 4.5 Conocimientos de informática de los encuestados

Fuente (Propia)

La anterior fue una de las preguntas más básicas que podemos encontrar dentro de la encuesta, nos referimos abiertamente a cualquier conocimiento fuera de su plaza de trabajo. Aunque el 62.5 % de los empleados encuestados respondió de manera afirmativa, es propicio destacar que un 31.3 % selecciono la respuesta “tal vez” denotando así falta de seguridad en sí mismos con relación a si poseen un conocimiento informático añadido.

4.4.5 ¿Conoce, sabe o ha escuchado mencionar el termino ¨seguridad de la información¨?

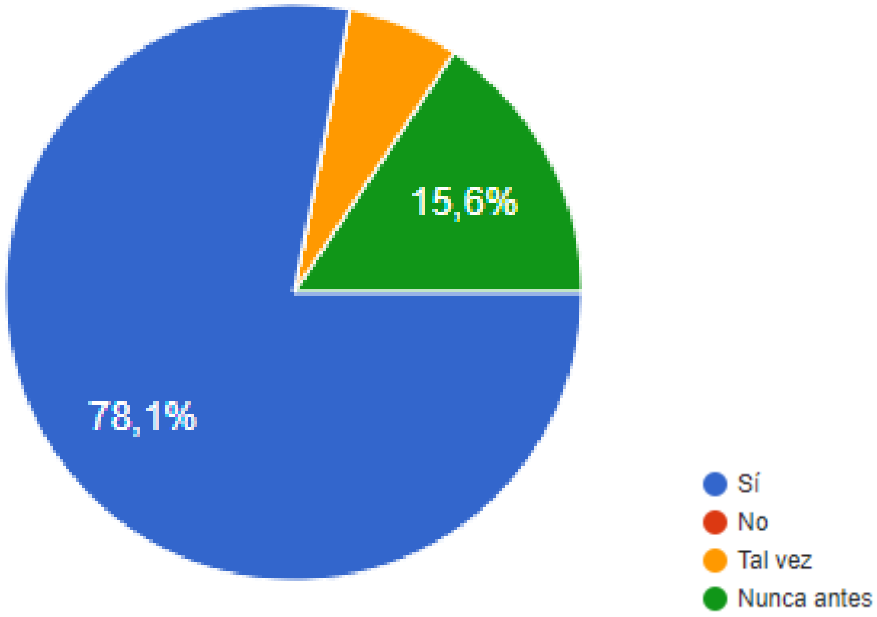


Figura 4.6 Departamentos que pertenecen los encuestados

Fuente (Propia)

En esta pregunta ciertamente teníamos nuestras dudas, pero de manera sorprendente un 78.1 % de los empleados encuestados afirmó al menos haber escuchado una vez el término “seguridad de la información”. De manera no tan positiva nos encontramos que un 15.6 % de los mismos ni siquiera había escuchado mencionar esta frase en el paso.

4.4.6 Sabe usted ¿Cuáles pueden ser los objetivos de la seguridad de la información?

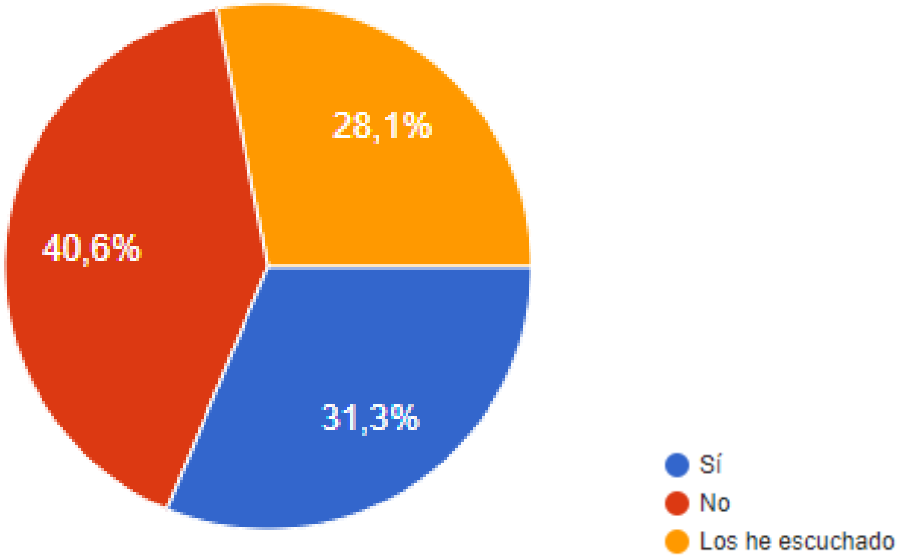


Figura 4.7 Respuestas de los objetivos de la Seguridad de la Información de los encuestados

Fuente (Propia)

Como podemos apreciar, aunque el 78.1 % de los encuestados ha escuchado mencionar este término tan solo el 31.3 % se atrevió a responder que sí conocía sus objetivos, el 28.1 % aseguro al menos haberlos escuchado alguna vez, pero sin duda alguna genera cierto grado de consistencia en sus respuestas.

4.4.7 ¿Conoce, sabe o ha escuchado mencionar lo que es un ataque informático?

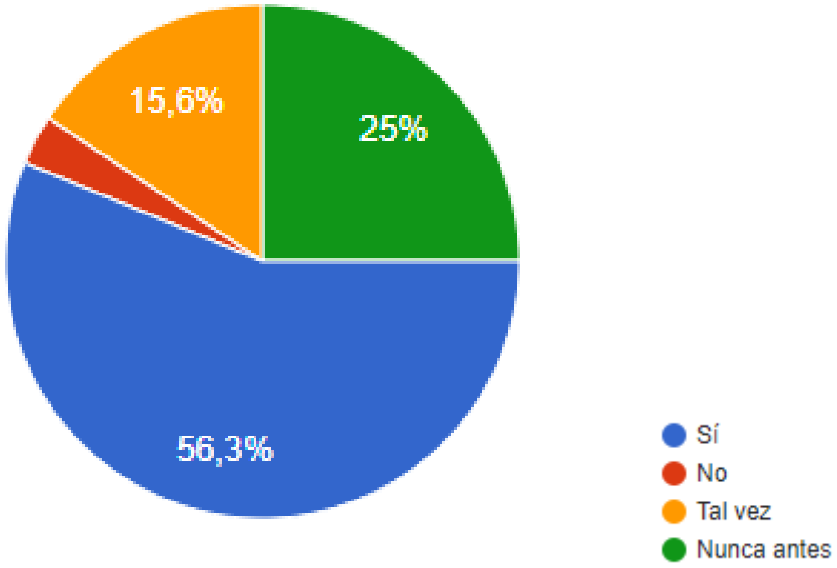


Figura 4.8 Respuesta sobre ataque informático de los encuestados

Fuente (Propia)

Si bien el 56.3 % de los empleados encuestados respondió de manera positiva, un 25 % respondió fuertemente que nunca ha visto o al menos escuchado este término. Si lo sumamos con el otro 15.6 % de un indeciso “tal vez” más el 4.1 % que aseguró no haber tenido ninguna relación con esta frase, obtenemos un 43.7 % de empleados encuestados que no poseen un manejo adecuado de este tema.

4.4.8 ¿Tiene conocimiento o idea de cuáles pueden ser los objetivos de un ataque informático?

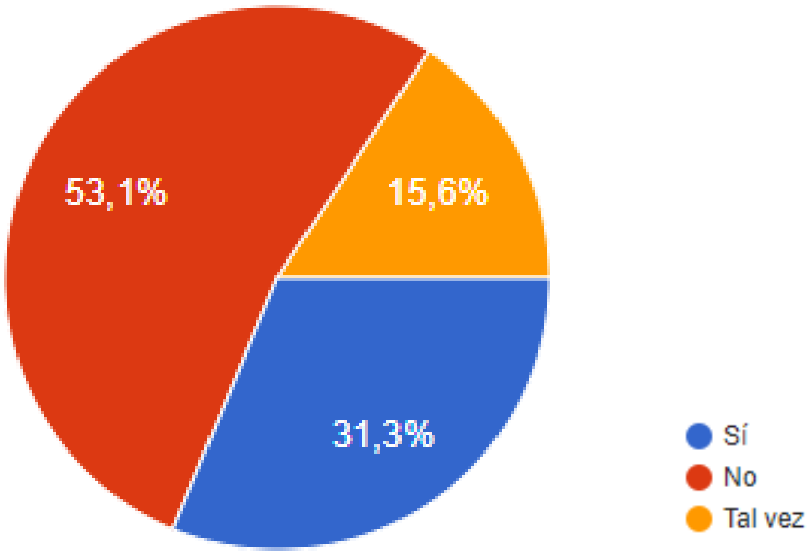


Figura 4.9 Conocimiento de los encuestados con los objetivos de un ataque informático

Fuente (Propia)

Se dice que una imagen vale más que mil palabras pues aquí tenemos esta, la cual refleja que un abrumador 53.1 % de los empleados encuestados no tiene la menor idea de cuáles pueden ser lo objetivos de un ataque informático. A continuación, lo que respondió el otro 46.9 % restante:

4.4.9 Si su respuesta a la pregunta anterior fue ¨si¨ o ¨tal vez¨, por favor indique ¿Cuáles pueden ser los objetivos?

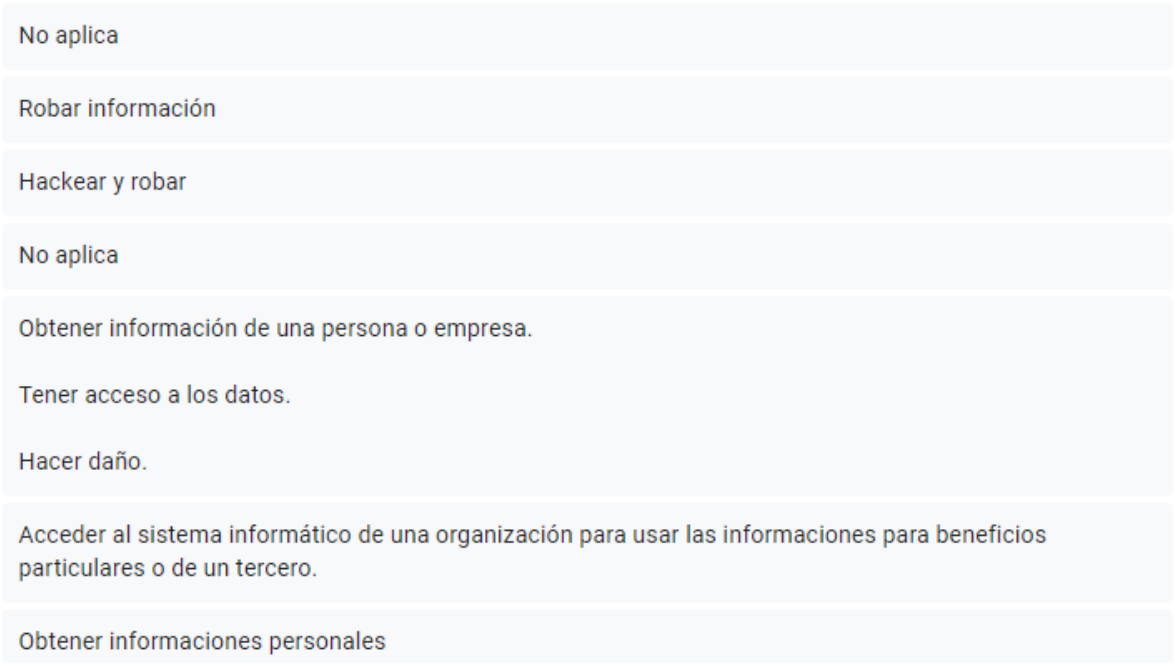


Figura 4.10 Respuesta abierta de los objetivos de un ataque informático de los encuestados

Fuente (Propia)

Antes que nada, aclarando que las respuestas visibles como “no aplica” pertenecen encuestados que luego de decir que “si” o “tal vez” no tenían ni la menor idea de cuáles pueden ser los objetivos de un ataque informático, así que ese 46.9 % anterior sin duda alguna aumenta. Las otras respuestas fueron directas y sencillas sin la implementación de palabras muy técnicas.

4.4.10 ¿Con cuáles de las siguientes palabras relaciona usted el termino ¨ataque informático¨?

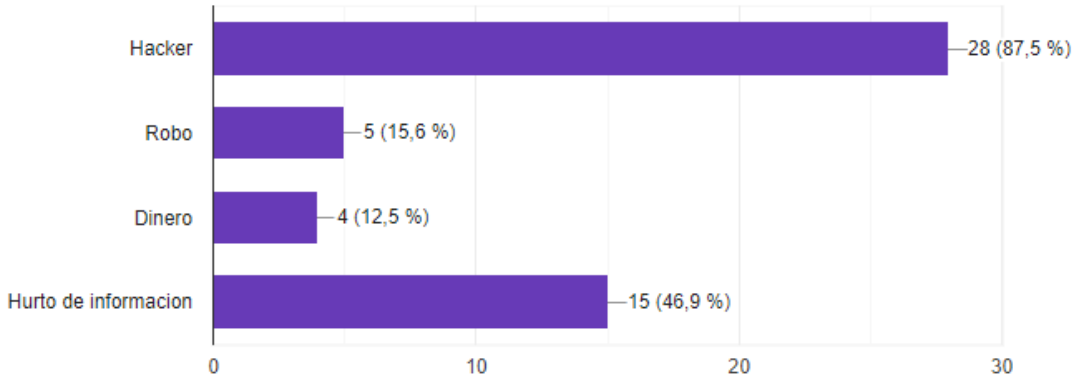


Figura 4.11 Respuesta de los encuestados sobre el término "Ataque Informático"

Fuente (Propia)

Si bien sabemos que el término "hacker" es bastante común y muchas veces mal utilizado, no es sorpresa que el 87.5 % de los empleados encuestados seleccionara esta palabra como la que más se relaciona a un ataque informático. De este mismo modo tenemos "hurto de información" seleccionado por el 46.9 % de los encuestados.

4.4.11 Además de los virus informáticos, ¿Conoce usted otro método de ataque informático?

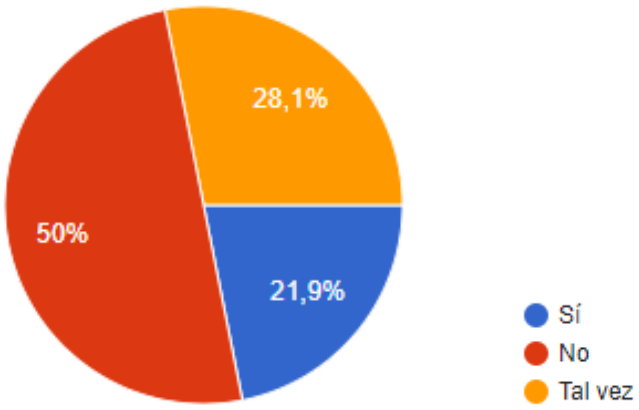


Figura 4.12 Respuesta de los encuestados sobre otro método de ataque informático

Fuente (Propia)

Está verdaderamente no nos tomó por sorpresa, desde pequeños es la única palabra que se repite en cuanto a problemas de un ordenador se refiere, un 50 % de los empleados encuestados desconoce completamente que otros vectores de ataques pueden ser utilizados además de los “virus informáticos”. El otro 50 % restante aseguro o al menos dijo tener un leve conocimiento de otro tipo de ataque informático.

4.4.12 Si su respuesta a la pregunta anterior fue ¨si¨ o ¨tal vez¨, por favor indique ¿Cuáles más conoce?

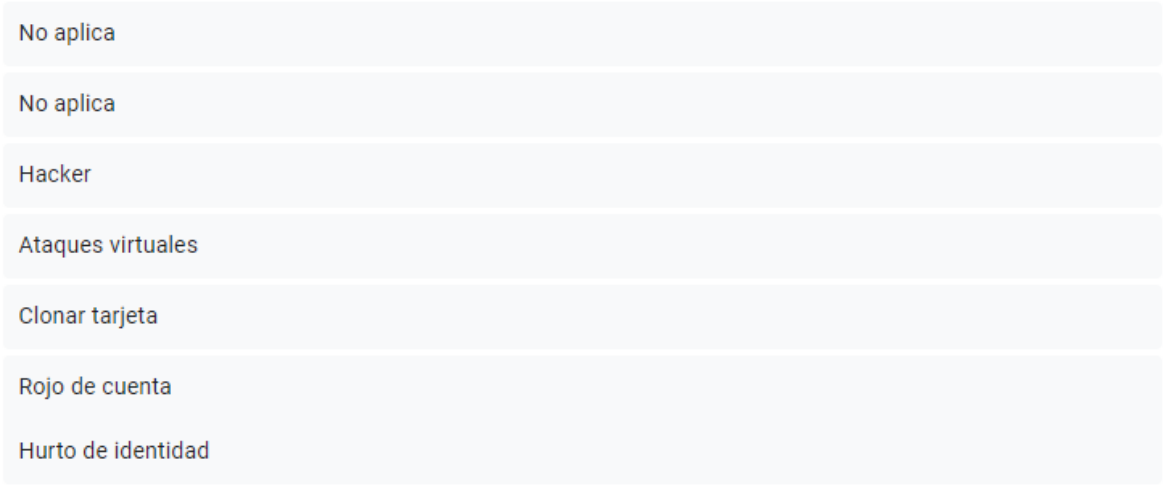


Figura 4.13 Respuesta de los encuestados sobre el término "Ataque Informático"

Fuente (Propia)

Aclarando nuevamente que las respuestas visibles como "no aplica" pertenecen encuestados que luego de decir que "si" o "tal vez" no tenían ni la menor idea de cuales otros métodos de ataque informático conocían. Fuera de esto fueron respuestas un tanto vagas y comunes.

4.4.13 ¿Conoce lo que es la ingeniería social?

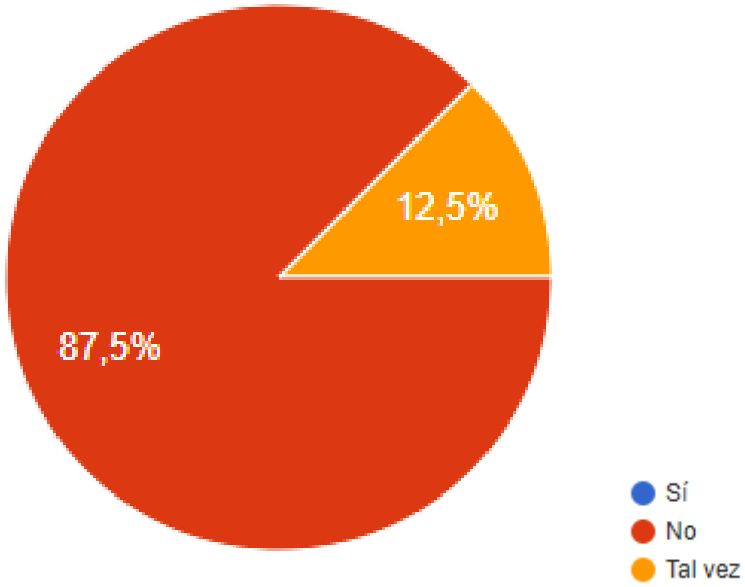


Figura 4.14 Respuesta conocimiento de ingeniería social de los encuestados

Fuente (Propia)

Absolutamente nadie se atrevió a responder de manera afirmativa a sí conocía lo que es la “ingeniería social”. lo que representa una vulnerabilidad bastante marcada y puntual en cuanto a este vector de ataque nos referimos.

4.4.14 ¿Con cuáles de los siguientes términos relaciona la ingeniería social?

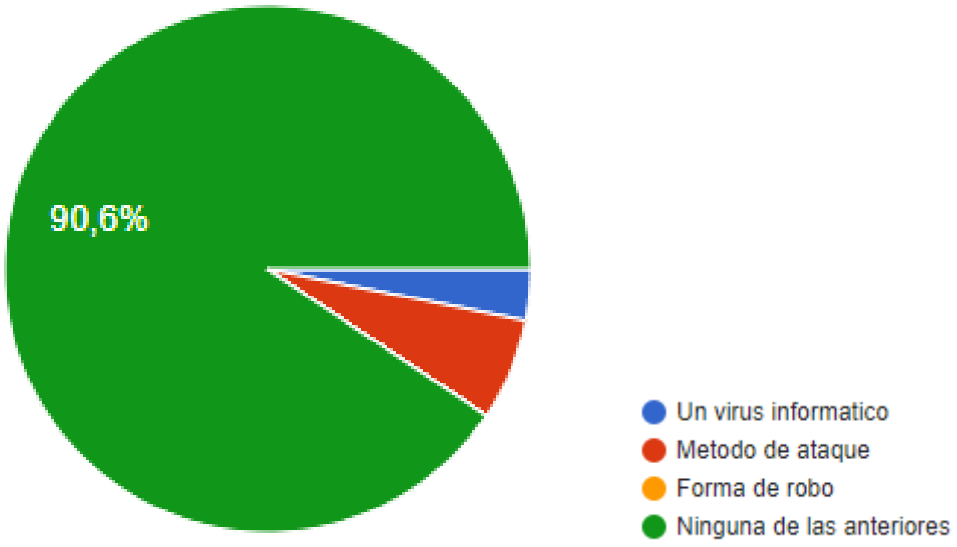


Figura 4.15 Respuesta de los encuestados sobre el término que se relaciona la ingeniería social

Fuente (Propia)

Si un 100 % de los empleados encuestados desconoce lo que es la ingeniería social, no es sorpresa que el 90.6 % de los encuestados no relacione la ingeniería social con ninguno de los términos colocados en las respuestas, el otro 9.4 % fue dividido entre un “virus informático” y un “método de ataque”.

4.4.15 ¿Se considera usted vulnerable a un ataque de ingeniería social?

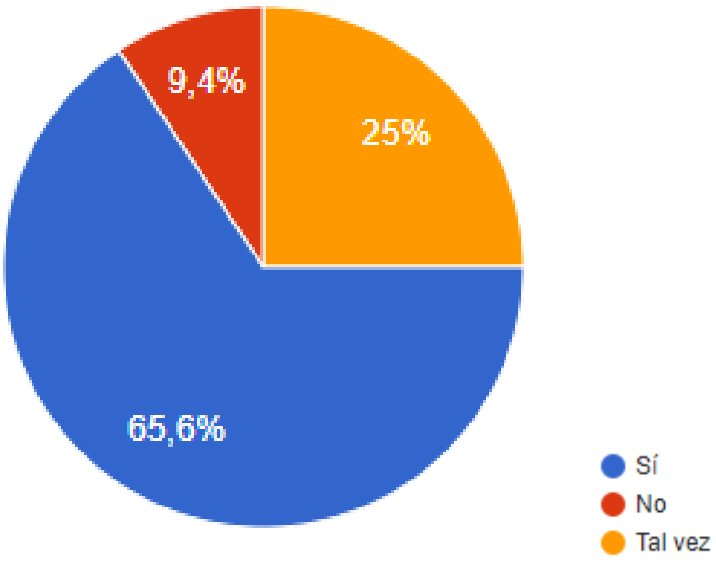


Figura 4.16 Respuesta de los encuestados sobre lo vulnerable de una ingeniería social

Fuente (Propia)

Consideramos que era una pregunta bastante propicia por realizar, debido a la regresión lineal de las preguntas anteriores no fue sorpresa que el 65.6 % de los empleados encuestados se considerara vulnerable a un ataque de ingeniería social. Si bien un 9.4 % de los encuestados respondió que no es vulnerable, es adecuado realizar la siguiente pregunta. ¿Como sabes no eres vulnerables a algo que desconoces por completo?

4.4.16 Si un compañero le pide ayuda la cual involucra sus credenciales de acceso al sistema, ¿Qué hace?

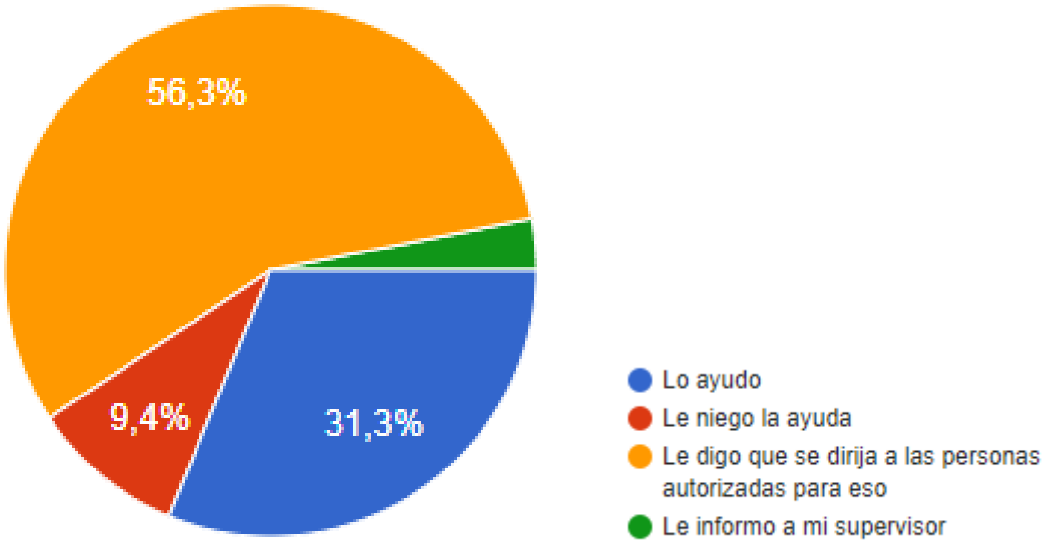


Figura 4.17 Respuesta de los encuestados sobre ayuda con sus credenciales para acceder al sistema

Fuente (Propia)

De forma positiva debemos destacar que el 56.3 % de los empleados encuestados respondió que “enviará a su compañero a las personas autorizadas para ello” en este caso, personal de TI o encargados de departamentos. Por otro lado, no tan positivo tenemos ese latente 31.3 % que sin duda alguna lo ayudará involucrando sus credenciales. En particular creemos que ese 31.3 % es más elevado, pues en

las oficinas de la Administradora de Riesgos Laborales se vive un ambiente bastante familiar y de inspirar confianza.

4.4.17 ¿El departamento de tecnología imparte entrenamientos, informaciones o documentaciones relacionadas a la SEGURIDAD INFORMATICA a los usuarios?

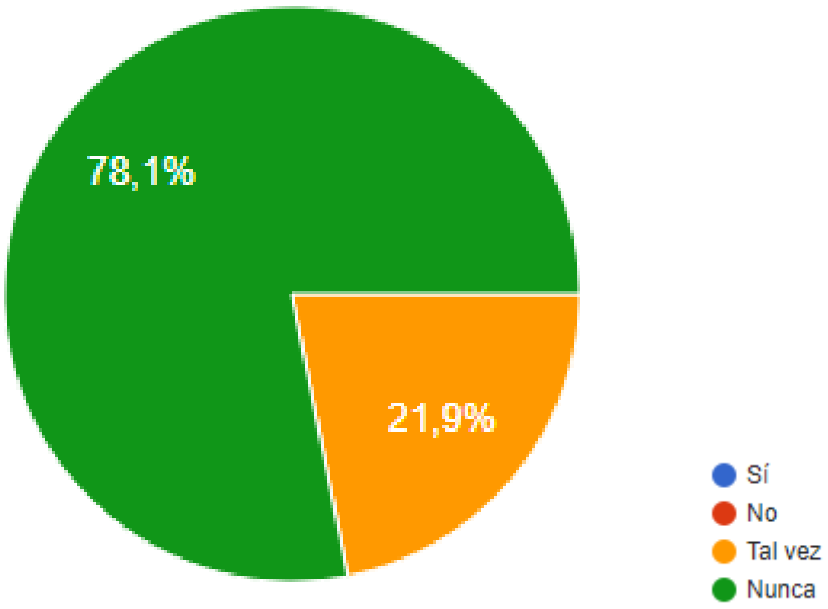


Figura 4.18 Respuesta de los encuestados sobre informaciones o documentación relacionadas a la seguridad Informática

Fuente (Propia)

Podríamos decir que este resultado nos toma de manera sorpresiva, la ARL es una institución que se enfoca mucho en las bases tecnológicas para un mejor servicio,

es por ello que no vemos propició que no se imparten cursos, charlas, informaciones o nada relacionado a la seguridad de la información con sus empleados. Ningún encuestado se atrevió a responder de manera afirmativa, tan solo un 21.9 % dijo “tal vez” y si creen que tal vez se puede interpretar como una posibilidad positiva, pongan énfasis en la siguiente pregunta.

4.4.18 Si su respuesta anterior fue "si" o "tal vez". ¿Con que frecuencia lo hacen?

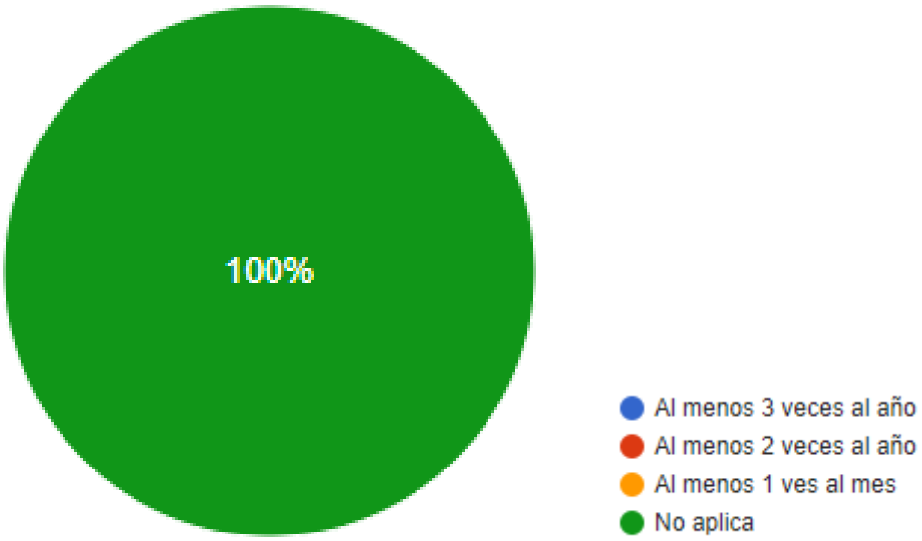


Figura 4.19 Respuesta de los encuestados sobre la frecuencia que imparten informaciones en la organización

Fuente (Propia)

A sabiendas que un “tal vez” puede denotar una respuesta positiva o negativa, le dimos la oportunidad a los empleados encuestados que si respondieron con esta respuesta entonces nos indiquen un punto de partida en la frecuencia con que se imparte el material en relación con la seguridad de la información. el 100 % de las respuestas fueron “no aplica”.

4.4.19 ¿Qué acción realiza cuando entiende que su computador está actuando de manera sospechosa?

Figura 4.20 Respuesta de los encuestados sobre que hacen si su computadora actúa de manera sospechosa

Fuente (Propia)

Esta pregunta se puede clasificar como básica o de rutina, afortunadamente el 59.4 % de los empleados encuestados seleccionó la opción de “realizar una solicitud al departamento de TI”. Otro 31.3 % de los encuestados afirmó que le notifica la situación a su encargado o supervisor, los cuales en este caso proceden a comunicarse directamente con el departamento de TI. De esta manera, se garantiza un seguimiento de los casos reportados para su posterior evaluación y solución.

4.4.20 Usted normalmente conecta su Smartphone a ¿Cuál de las siguientes redes wifi?

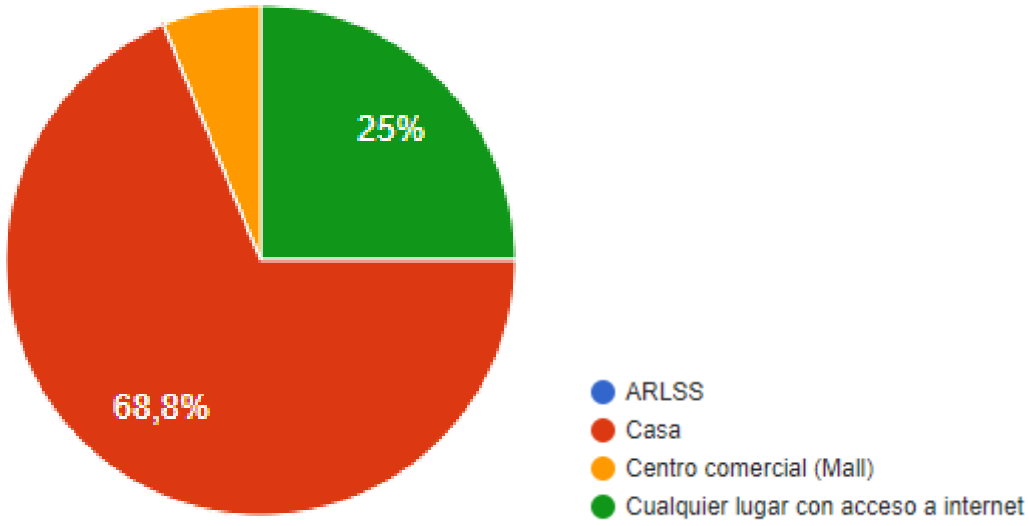


Figura 4.21 Respuesta de los encuestados sobre en qué redes inalámbricas suelen conectar sus teléfonos inteligentes

Fuente (Propia)

Muchos ataques de robo de información privilegiada suceden y son perpetrados cuando agentes maliciosos se aprovechan de usuarios no entrenados y conectados normalmente a redes wifi-públicas. Es por ello, que realizamos esta pregunta, tan solo 31.2 % de los encuestados afirmó que enlaza su dispositivo móvil a cualquier red wifi. De manera positiva debemos destacar el 68.8 % restante que solo conecta su móvil a la red wifi de su hogar.

4.4.21 De los siguientes objetos, ¿Cuáles utiliza que lo identifique como empleado fuera de la institución?

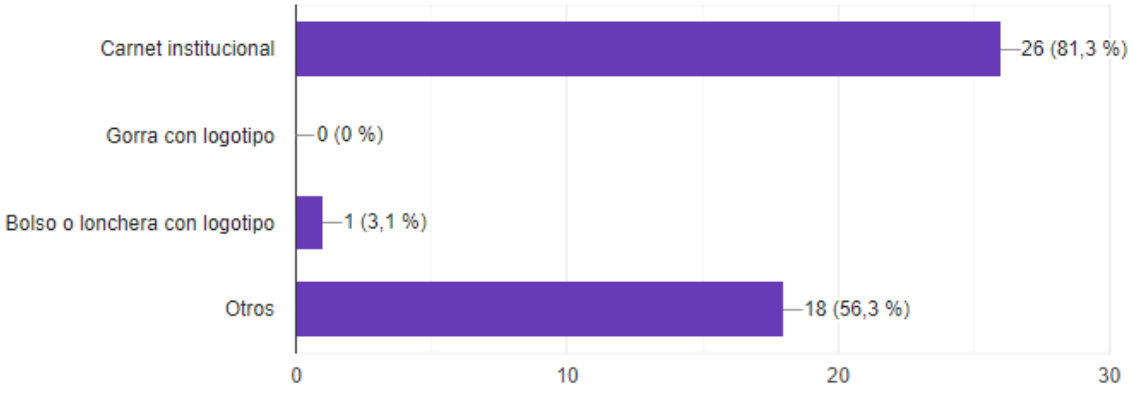


Figura 4.22 Respuesta de los encuestados sobre los objetos que lo identifique como parte de la organización

Fuente (Propia)

Esta pregunta fue realizada con la finalidad de palpar si realmente existía un riesgo latente de identificar un usuario fuera de la institución para un posterior ataque. En la misma, fue altamente reflejado que sí, los encuestados afirmaron utilizar su carné

de identificación de empleado fuera del ambiente laboral, el mismo posee nombre, apellido y cargo ejercido dentro de la ARL. Por otro lado, también son utilizados uniforme institucional o bolsos, pero estos son más comunes y no tan relevantes a la hora de realizar un ataque.

4.5. Prueba de campo

Gracias al equipo de operaciones de la organización, se seleccionaron una población de 10 usuarios de distintas áreas departamentales. Todo con el objetivo de simular un tipo de ataque Phising para captar información de que sistema operativo utilizan, la Ip pública, Hostname al que están conectados, qué navegador y versión de este utilizan.

Figura 4.23 Website GRABIFY

Fuente (GRABIFY, 2019)

La herramienta que se utilizó fue la de “GRABIFY”, esta consta de “IP Logger & Tracker” (registro y rastreador de IP), está diseñada para obtener la información analítica más detallada y avanzada en cada clic. La función de dicha herramienta de registro de IP son algo en lo que crea una URL y se envía a alguien. Si hace clic, solo se registrará la dirección IP de los usuarios en la base de datos. Luego se puede ver las estadísticas a través de la URL del rastreador.

Si se desea que el usuario haga clic, se acorta la URL. Entonces hay más probabilidad de que el usuario haga clic.

Estos son los pasos para utilizar para el registro de IP:

- Cree una URL del registrador ingresando la ID del registrador
- Acorte la URL del registrador y comparta la URL con cualquiera.
- Hay más posibilidades de que el usuario haga clic en el enlace.
- Si la persona hace clic en su dirección IP se registrará
- Puede verificar la dirección IP registrada con la URL del rastreador

La simulación del ataque consistió en que se tomó una noticia relevante y de interés para casi todo el público en general. Se tomó la URL en este caso original.

Figura 4.24: Despedida de Danilo Medina a su difunto padre.

Fuente (Listín Diario, 2019)

Figura 4.25: website que registra los datos del usuario.

Fuente (GRABIFY, 2019)

Luego se procedió agregar la URL original y que el sitio web generará una URL recortada para que se acceda a través de esta. Luego se le adjunta un hipervínculo con la URL recortada a la imagen de la noticia. Después se preparó un correo electrónico dirigido a cada uno de los usuarios seleccionado con el título, autor, correo electrónico y etc. Todo eso con el objetivo de que pareciera una comunicación legítima.

Figura 4.26: Correo electrónico de prueba.

Fuente (Propio)

Al momento del usuario hacer clic lo redirige a la página web que recolecta los datos y la misma lo redirecciona a la supuesta página web con dicha noticia en este caso al Listín Diario.

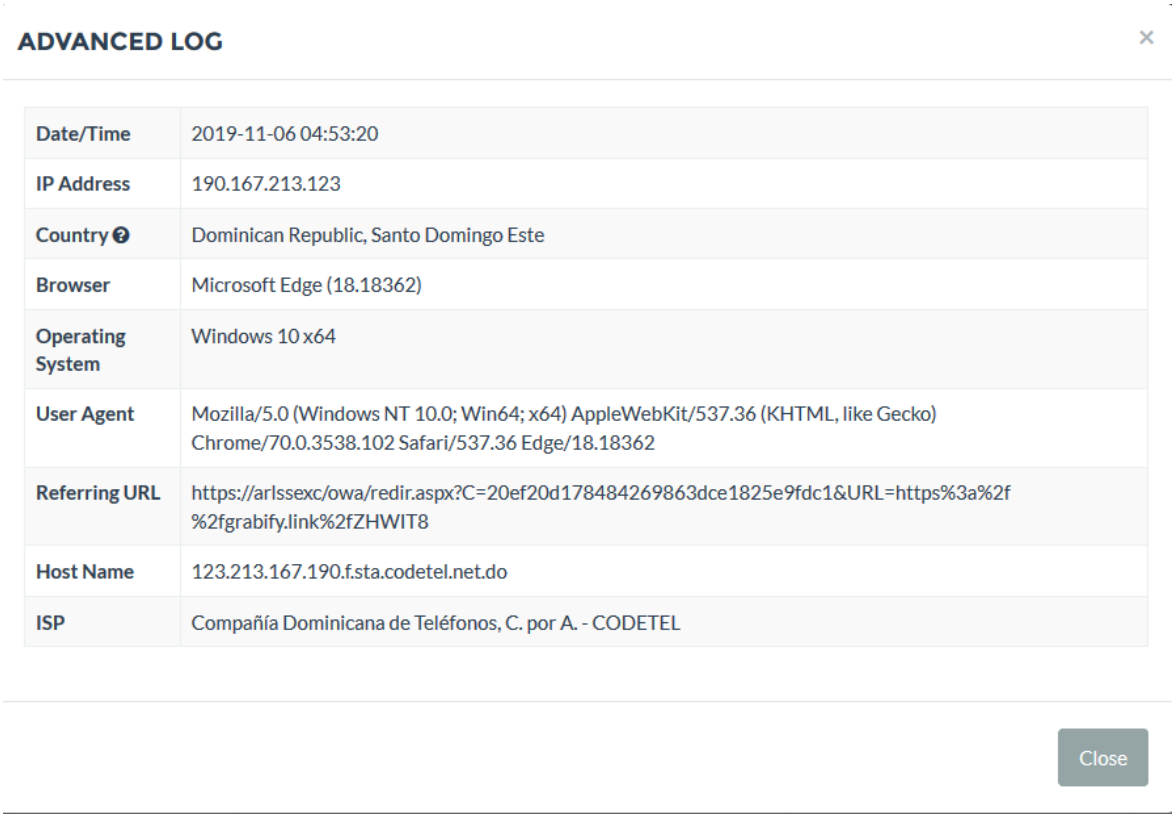


Figura 4.27: Usuario captado por la URL falsa.

Fuente (GRABIFY, 2019)

Se puede observar en la imagen anterior la URL Original donde está alojada la noticia de interés, mientras pasan a través de la URL recortada utilizada para captar la información. Después de varios días el 30% de los usuarios seleccionados hicieron clic a la URL enviada y así los datos de estos quedaron registrados. Dichos usuarios captados respondieron a que la noticia le pareció interesante y por eso accedieron al link presentado, aunque este correo electrónico sea de procedencia dudosa.

Este tipo de experimento demuestra que de simples herramientas gratuitas y con un poco de conocimiento en informática, se puede lograr captar información de sistemas y aplicaciones que en propiedad de personas con conocimiento y mal intencionada pueden explotar algún tipo de vulnerabilidad que estos deseen.

4.6 Descripción técnica

Como bien saben gran parte de las organizaciones e instituciones alrededor del mundo destinan un porcentaje considerable de sus ingresos a la innovación y protección de la información. Ya sea con equipos de última generación o programas basados en inteligencia artificial, sin duda alguna la misión de salvaguardar los datos siempre está en los planes estratégicos fundamentales de cada una. Por consiguiente, podemos decir directamente que las organizaciones poseen manuales o pasos a seguir a la hora de implementar y detectar ataques de seguridad fuera del eslabón humano.

Como se mencionó anteriormente, el fin básico de todas estas implementaciones es el amparo y defensa de la información que sin importar qué valor poseen en el mercado externo siempre será privilegiada para cualquier empresa. De esa manera y en cuanto a la Administradora de Riesgos Laborales nos referimos, tampoco se quedan rezagados, la misma cuenta con un novedoso sistema de firewalls y antivirus capaces de detectar desde una gran amenaza hasta las más

insignificantes encontradas en la red. De ahí, la institución ha detectado y evitado ataques que podrían causar un daño colateral de nivel medio a elevado.

Es por ello, que uno de los objetivos fundamentales perseguidos en este trabajo de grado ha sido demostrar que en la cadena de la seguridad de la información el eslabón más débil siempre será el usuario. Pues no sirve de nada que una organización invierte cuantiosas sumas de dinero en protección, sino trabaja la fuga más significante de todas: completa desinformación en los empleados y usuarios no entrenados.

CAPÍTULO V:

RECOMENDACIONES DIRIGIDAS A LA ADMINISTRADORA DE RIESGOS LABORALES.

5.1 Recomendaciones para la Administradora de Riesgos Laborales

5.1.1 Mitigar la desinformación de los empleados

Según el periódico Listín Diario en su artículo, publicado en fecha 25 de julio del año 2017, “Empleados: un puente para delitos de cibercriminales”, el 46 % de los incidentes relacionados a la seguridad de la información son ocasionados por los propios trabajadores, motivo por el cual esta vulnerabilidad (los empleados) en las empresas debe ser atendida en muchos niveles.

Según el informe factor humano en la seguridad de TI: cómo los empleados hacen que las empresas sean vulnerables desde adentro, los empleados del 40 % de las empresas en todo el mundo ocultan los incidentes de seguridad de TI ya sea por vergüenza o por temor a ser disciplinados.

Según la empresa de seguridad Kaspersky Lab y B2B International, la desinformación o el descuido de los empleados son una de las causas más comunes en un incidente de ciberseguridad, superado sólo por el “malware”. Mientras que el “malware” se vuelve cada vez más sofisticado, la triste realidad es que el factor humano puede representar un peligro aún mayor.

Partiendo de estas investigaciones podemos decir plenamente que la desinformación en los empleados en la Administradora de Riesgos Laborales es un

punto crucial a la hora de efectuar un ataque a la seguridad de la información. Asimismo, como el encubrimiento de sucesos e informaciones pertinentes las cuales pueden jugar un papel de suma importancia a la hora de tomar medidas en cuanto a la seguridad de los datos dentro de la institución se refiere. Con empleados casi nulos en cuanto al tema de la seguridad y vectores de ataques existentes nos referimos, podemos decir que ¿Realmente está protegida la Administradora de Riesgos Laborales?

En vista de lo anterior, consideramos pertinente realizar las siguientes recomendaciones:

- Hacerle entender a los empleados de la Administradora de Riesgos Laborales que la falta de información no es una razón por la cual avergonzarse, sino más bien reconocer la falta para así trabajarla en conjunto.
- Brindar el seguimiento debido a los empleados mediante evaluaciones de conocimientos básicos de seguridad informática periódicamente.
- Proporcionar de manera eficaz información y datos pertinentes a tener en cuenta por parte de los empleados.

5.1.2 Entrenamientos fundamentales

Según Karpersky, ocultar los incidentes en los que se ha involucrado el personal puede traer serias consecuencias, pues aumenta el daño causado de manera general. Incluso, asegura, un evento que no se informa podría indicar que hay una brecha mucho mayor y los equipos de seguridad necesitan identificar rápidamente las amenazas que enfrentan para elegir las tácticas de mitigación adecuadas. Sin embargo, el personal preferiría poner a las organizaciones en riesgo antes que denunciar un problema porque temen el castigo o se avergüenzan de ser responsables de un error.

Según un estudio publicado en el periódico Listín Diario de fuente desconocida asegura que, el 52 % de las empresas admite que el personal es la mayor debilidad de su seguridad informática.

Tomando en cuenta las informaciones presentadas anteriormente podemos llegar a la conclusión de que los entrenamientos dentro del ambiente laboral son de vital importancia para la protección de una organización. Claramente los entrenamientos laborales implican un costo que, dependiendo su concentración y alcance podría ser una inversión significativa de tiempo y dinero. Sin embargo, la palabra de mayor relevancia no es “inversión”, sino recuperación, puesto que los entrenamientos laborales le beneficiarán a corto o largo plazo, dependiendo con qué frecuencia y objetivo se establezcan.

Recomendaciones en cuanto a los entrenamientos laborales:

- Crear un plan de reforzamiento en técnicas y conocimientos básicos de la seguridad de la información tanto para los empleados de nuevo ingreso como los ya previamente establecidos.
- Plantear y seguir fielmente un calendario estratégico de entrenamientos periódicos a lo largo del año.
- Realizar evaluaciones al azar por departamentos, promoviendo el estar preparados ante cualquier eventualidad.

Según Lissette Martínez en su artículo publicado en fecha 3 de agosto del año 2015, la capacitación laboral no solo ayuda a una mejor producción o retención de empleados, también contribuye a la fijación de metas de un individuo y su desarrollo profesional y personal. A medida que los empleados reciben entrenamientos (que no sean únicamente de acuerdo con el tipo de trabajo que desempeñan) van trabajando su autoestima.

5.1.3 Charlas

Si bien en su definición básica las encontramos como una “conferencia o disertación acerca de un tema que se da en un ambiente familiar, distendido y ameno, sin la solemnidad o formalidad habituales”; sin duda alguna tienen un poder mucho más

elevado que solo transmitir un mensaje o información previamente seleccionada. Las mismas cumplen un papel de suma importancia a la hora de impartir documentación pertinente a un mediano o gran grupo de personas.

En efecto, las charlas son una excelente vía de impartir información de manera horizontal (técnica utilizada en la administración y gerencia). Con la intención, de que el personal adopte las medidas que son requeridas por el nivel superior en el manejo de la seguridad de la información, se pueden poner en marcha las siguientes recomendaciones:

- Con la finalidad de mantener a los empleados a la par con los nuevos vectores de ataque que se pueden encontrar, realizar charlas o conferencias cada trimestre. A su vez, reforzando y guiando el conocimiento con pequeñas encuestas o evaluaciones.
- Trazar metas en conjunto y llevarlas a cabo trabajando a la par con los empleados de la institución.
- No todo debe ser visto como una presión ejercida sobre los empleados, cada trimestre a una cantidad limitada que cumpla con el propósito planteado podría ser premiado o compensado con algo de su agrado.

5.1.4 Transmisión de información o documentación

“Invertir en el futuro de un empleado es más importante que la compensación inmediata,” dijo Eric Rolfe Greenberg, director de Estudios de Gestión de la American Management Association en una encuesta sobre recursos humanos publicada por la firma.

Tomamos esta frase de referencia porque a la hora de transmitir las informaciones o documentaciones pertinentes muchas organizaciones solo conocen una manera, vía correo electrónico. Este método de comunicación empresarial no está mal, pero debemos admitir que si se transmite una documentación la cual requiere énfasis en todos los empleados de uno o varios departamentos lo más probable es que solo sea recibida o vista por el encargado o supervisor. Por consiguiente, la idea de que todos conozcan o visualicen la información proporcionada se desborona.

En consecuencia, de lo anterior, recomendamos lo siguiente en cuanto a trasmitir las informaciones y documentaciones de la seguridad de la información de refiere:

- Consejos con relación a la seguridad de la información colocados en el Homepage del Intranet.
- Recordando que la Administradora de Riesgos Laborales es una institución gubernamental puede canalizar formas gratuitas de impartir cursos relacionados a la seguridad de la información, así creando una cultura de aprendizaje dentro de los propios empleados.

- Talleres proporcionados por los propios empleados de TI que estén capacitados en el área.

Según el sitio web oficial de las Normas ISO, la gestión de riesgos es uno de los elementos clave en la prevención del fraude online, robo de identidad, daños a los sitios Web, la pérdida de los datos personales y muchos otros incidentes de seguridad de la información. Sin un marco de gestión de riesgos sólida, las organizaciones se exponen a muchos tipos de amenazas informáticas. Entonces aquí vemos donde radica la importancia de que todos los empleados posean al menos una base sólida en cuanto a seguridad de la información nos referimos.

Según el sitio web oficial de las Normas ISO, la gestión de riesgos es uno de los elementos clave en la prevención del fraude online, robo de identidad, daños a los sitios Web, la pérdida de los datos personales y muchos otros incidentes de seguridad de la información. Sin un marco de gestión de riesgos sólida, las organizaciones se exponen a muchos tipos de amenazas informáticas. Entonces aquí vemos donde radica la importancia de que todos los empleados posean al menos una base sólida en cuanto a seguridad de la información nos referimos.

5.2 La comunicación laboral y seguimientos dentro de la organización

5.2.1 Proceso de comunicación dentro de la empresa

“Dentro de la empresa debes estar preparado para manejar diversos tipos de comunicación” (BUENOS NEGOCIOS, 2018). Si se sabe utilizar de la manera correcta esta puede ser de mucha utilidad ya que con esta se transmiten mensajes tales como la dirección que toma la empresa, avisos importantes, informaciones relevantes, etc.

La comunicación interna efectiva ayuda a garantizar que todos los miembros de la organización trabajen en colaboración hacia un objetivo común. Desarrolla una cultura coherente y permite a los empleados tomar las decisiones correctas de acuerdo con los objetivos de la organización. Esto a su vez conduce a una mayor eficiencia y productividad y mejora el servicio al cliente. Estos resultados son relevantes para todas las organizaciones, por lo que el tamaño realmente no debería importar a este respecto.

Siendo así la importancia de la comunicación dentro de las organizaciones es de mantener a todos los empleados informados en este caso es de la seguridad de información. Como existen tantas formas de penetración hacia los sistemas, se tiende a no tomar en cuenta a los usuarios de estos como una debilidad del mismo.

Si se mantiene bien informado con las recientes políticas, documentaciones e informes de reconocidas revistas de seguridad informática, el porcentaje de vulnerabilidad podría disminuir considerablemente.

5.3 Contra medida y protección

Los ataques de ingeniería social son una de las amenazas más difíciles de defender porque involucran al elemento humano, que en sí mismo es bastante impredecible. Sin embargo, hay algunas medidas que ciertamente pueden traer el riesgo asociado con la ingeniería social con una cultura de seguridad activa en toda la organización que sigue evolucionando a medida que cambia el panorama de amenazas.

Las amenazas por su parte se pueden presentar en diferentes versiones y con niveles de riesgos variantes entre las mismas. En definitiva, una amenaza puede contener niveles de riesgos variantes dependiendo de ambiente en el que se desarrolle, no poseen las mismas características de importancia para las diferentes organizaciones. Pero, sin lugar a duda se debe tener en cuenta su mitigación en función de la alerta o interés que despierte para una institución.

5.3.1 Política de seguridad documentada

Una política de seguridad bien documentada y accesible, los estándares asociados y las pautas forman la base de una buena estrategia de seguridad. La política debe documentar claramente en términos simples, su alcance y contenido en cada área a la que se aplica. Junto con cada política debe especificarse, los estándares y las pautas a seguir para cumplir con la política. En general, una política debe contener declaraciones de política en los dominios, tales como:

- Política de uso aceptable: Forma de uso comercial aceptable de correo electrónico, sistemas informáticos, teléfono, redes, etc.
- Clasificación y manejo de la información: para identificar activos de información crítica e instrucciones de manejo asociadas.
- Seguridad del personal: Selección de posibles empleados, contratistas para garantizar que no representen una amenaza para la seguridad de la organización, si están empleados.
- Seguridad física: Para proteger la instalación del acceso físico no autorizado con la ayuda de procedimientos de inicio de sesión, dispositivos de seguridad electrónicos y biométricos, etc.

- Control de acceso a la información: Uso de contraseña y pautas para generar contraseña segura, autorización de acceso y procedimientos de responsabilidad, asegurar módems de acceso remoto, etc. El restablecimiento automático de contraseña y las herramientas de sincronización pueden eliminar la responsabilidad de administrar las contraseñas del soporte técnico y la mesa de ayuda, sin colocar una carga de deshacer para los usuarios finales.

- Protección contra virus: Para proteger los sistemas y la información contra virus y amenazas similares.

- Capacitación sobre concientización sobre seguridad de la información: Para garantizar que los empleados estén informados sobre las amenazas y contramedidas y sus responsabilidades en la protección de los activos de la organización.

- Monitoreo de cumplimiento: Para garantizar continuamente que se cumpla la política de seguridad.

5.3.2 Evaluación de riesgos

Como ya se ha mencionado en esta investigación, la evaluación de riesgos es un enfoque sistemático que ayuda a la gerencia a comprender los factores de riesgo

que pueden afectar negativamente las capacidades operativas de la organización. También ayuda a tomar decisiones informadas sobre el alcance de las acciones necesarias para mitigar el riesgo. Implica priorizar los activos de información en función del riesgo asociado a ellos. Esto ayuda a identificar los activos más críticos de la organización y a centrar la energía y el esfuerzo de la organización en protegerlos. Si la evaluación de riesgos se lleva a cabo de manera efectiva en una organización, los controles y los procedimientos de seguridad protegerán el activo más crucial contra los ataques.

		Severidad									
		1	2	3	4	5	6	7	8	9	10
Ocurrencia	1	1	2	3	4	5	6	7	8	9	10
	2	2	4	6	8	10	12	14	16	18	20
	3	3	6	9	12	15	18	21	24	27	30
	4	4	8	12	16	20	24	28	32	36	40
	5	5	10	15	20	25	30	35	40	45	50
	6	6	12	18	24	30	36	42	48	54	60
	7	7	14	21	28	35	42	49	56	63	70
	8	8	16	24	32	40	48	56	64	72	80
	9	9	18	27	36	45	54	63	72	81	90
	10	10	20	30	40	50	60	70	80	90	100

Riesgo Bajo - Condición aceptable.

Riesgo Medio - Se deben considerar acciones en el futuro.

Riesgo Alto - Se requieren acciones inmediatas.

Figura 5.1: Tabla utilizada en la Gestion de Riesgos para su evaluación

Fuente: (SPC Group)

La tabla consiste en multiplicar los números en posición vertical con los colocados en posición horizontal para así obtener el resultado.

5.3.2.1 Recomendación relacionada al Estándar de Seguridad de la Información ISO/IEC 27001

En esta investigación se ha tratado el tema de una buena gestión de riesgo como es el caso del Estándar ISO/IEC 27001. Es el único estándar internacional auditable que define los requisitos de un sistema de gestión de seguridad de la información (SGSI). Hay que recordar que SGSI es un conjunto de políticas, procedimientos, procesos y sistemas que gestionan los riesgos de la información, como los ataques cibernéticos, los piratas informáticos, las fugas de datos o el robo. certificase de ISO/IEC 27001 demuestra que una organización ha definido y establecido los mejores procesos de seguridad de la información. No todas las organizaciones eligen obtener la certificación, pero utilizan ISO/IEC 27001 como marco para las mejores prácticas que podría ser el caso de la ARLSS.

Ahora bien ¿Qué beneficios tiene implementar este estándar?

- **Protege y mejora tu reputación**. Los ataques cibernéticos aumentan en volumen y fuerza a diario, y el daño financiero y de reputación causado por una postura de seguridad de la información ineficaz puede ser desastroso.

- **Cumplir con los requisitos comerciales, legales, contractuales y reglamentarios**. El Estándar está diseñado para garantizar la selección de controles de seguridad adecuados y proporcionados que ayuden a proteger la información de acuerdo con los requisitos reglamentarios cada vez más rígidos, como el Reglamento General de Protección de Datos de la Unión Europea (GDPR).
- **Reduce la necesidad de auditorías frecuentes**. La certificación ISO 27001 proporciona una indicación globalmente aceptada por la efectividad de la seguridad, negando la necesidad de auditorías repetidas de la organización, lo que reduce el número de días de auditoría externa de la misma.
- **Obtenga una opinión independiente sobre su postura de seguridad**. La certificación ISO 27001 implica realizar revisiones periódicas y auditorías internas del SGSI para garantizar su mejora continua. Además, un auditor externo revisará el SGSI a intervalos específicos para establecer si los controles funcionan según lo previsto. Esta evaluación independiente proporciona una opinión experta sobre si el SGSI funciona correctamente y proporciona el nivel de seguridad necesario para proteger la información de la organización.

Teniendo entendido los beneficios de la utilización de este estándar en la reducción de riesgos y mejores prácticas. Hay consideraciones que se debe tener en cuenta para la implementación del SGSI.

Partiendo de que “no existe un procedimiento que describa paso a paso cómo implementar el estándar, existen factores que resultan fundamentales para tener una mejor proyección de los esfuerzos necesarios y para la obtención de resultados aceptables” (Mendoza. M, 2017).

1. **Respaldo y apoyo**

   El primer elemento a tener en cuenta al intentar implementar el estándar es tener el apoyo de la alta gerencia y que los mismo tengan las pautas de todas las actividades que conlleva comenzar a implementar un SGSI. Esto no debe de manejase como un proyecto cualquiera o aislado y que lo administre un personal de bajo nivel, el compromiso de ambas partes tanto de los colaboradores y la alta dirección debe reflejarse en una colaboración y cooperación mutua.

   Se recomienda crear una estructura para la toma de decisiones en cuanto al sistema de gestión. Se puede crear lo que es un comité de seguridad (o gobierno de Seguridad de Información) que pueda llevar las buenas prácticas, es decir, este tiene la responsabilidades y acciones a ejercer en cuanto a la seguridad.

2. **Estructura para la toma de decisiones**

   El comité creado debe ser un grupo de interdisciplinario que tendrán la tarea de tomar decisiones de acuerdo con la implementación y operación del sistema de gestión y de administrar el marco de trabajo de seguridad.

El objetivo de esto es integrar a los miembros de la alta dirección a proporcionar una visión general de la organización y alinear las necesidades de seguridad con los objetivos de la organización. Luego se puede agrupar las necesidades y punto de vista de los distintos departamentos y que los responsables de las distintas áreas puedan formar parte del comité.

3. **Análisis de brecha**

   Esto es un estudio preliminar que se realiza con el objetivo de conocer la forma que se desempeña la organización en cuanto a la seguridad de la información, para esto se utilizan criterios establecidos en estándares. En este se establece el desempeño actual y el deseado. Se suele utilizar esquemas de certificación nuevos ya que estos generan más dudas, debido a su novedad.

4. **Análisis de impacto al Negocio**

   Este elemento es utilizado para estimar en qué nivel puede afectar a la organización cuando ocurre algún incidente o desastre. Este contiene dos objetivos principales, el primero contempla las bases para identificar los procesos críticos para la operación de la organización. El segundo se refiere a la prioridad del conjunto de procesos, “siguiendo el criterio de cuanto mayor sea el impacto, mayor será la prioridad” (Miguel. M, 2014).

5. **Recursos, tiempo, dinero y personal**

   Según los resultados del análisis de brecha y el impacto al negocio, se puede estimar los elementos necesarios para la implementación de ISO/IEC 27001.

En el primer ciclo conlleva una carga de trabajo menor, permitiendo una planificación adecuada, puede ser necesario contratar personal enfocado para esa tarea. No es recomendable que el tiempo dedicado al sistema de gestión exceda el de un año debido a los cambios continuos en los riesgos, prioridades de la alta gerencia, nuevas amenazas, etc.

6. **Revisión de los estándares de seguridad**

   Otra tarea muy útil previa a la implementación del estándar es la de conocer el contenido y estructura de este y así como la serie 27000 que conforma el mismo. “ISO/IEC 27000 contiene el glosario de todos los términos utilizados en la serie 27000, un resumen general de esta familia de estándares, así como una introducción al SGSI. Este estándar adquiere mayor relevancia, ya que se convierte en la única referencia normativa de la nueva versión de ISO/IEC 27001” (Mendoza. M, 2017).

5.3.3 Conciencia y educación

Crear conciencia entre los usuarios sobre las técnicas comunes empleadas y los comportamientos dirigidos por un ingeniero social es una parte importante de la estrategia de defensa. También es obligatorio educar a los empleados sobre el daño causado por dicho robo. No hay sustituto para una buena campaña de concientización para implementar los elementos de 'ingeniería social' de una política

de seguridad. Los elementos de una campaña de sensibilización dependen de cómo se comunica la información al personal de la organización. Cuanto más se refuerza los mensajes de precaución dentro de las políticas, más exitosa es su implementación. La mejor manera de crear tal conciencia en un profesional general que no es de seguridad es a través de ejemplos de la vida real de compañías que han sido pirateadas debido a información privilegiada, o incluso por negligencia e ignorancia por parte de un empleado.

5.3.4 Auditorías y Cumplimiento

Haber creado la política y educar al usuario no es suficiente, si nadie se ajusta a la política. Por lo tanto, es necesario auditar el uso en toda la organización. Por ejemplo, cuando un proyecto está pasando por el aseguramiento de la calidad, también debe pasar por la verificación del cumplimiento de la política de seguridad. Deben existir procedimientos de auditoría para verificar, por ejemplo, que la persona de la mesa de ayuda no está comunicando contraseñas por teléfono o por correo electrónico no cifrado. Periódicamente, los gerentes deben revisar el acceso de sus empleados. Las auditorías de seguridad deben confirmar que los empleados que ya no necesitan acceso no tienen acceso. Los puntos de acceso, como las puertas de entrada, etc., deben ser monitoreados de manera rutinaria. Esto asegurará que los empleados cumplan con la política con respecto al acceso a ubicaciones seguras.

Los espacios de trabajo de los empleados deben someterse a una inspección aleatoria para garantizar que el material confidencial siempre esté asegurado en armarios cerrados. Las estaciones de trabajo deben estar bloqueadas y los protectores de pantalla protegidos con contraseña deben estar en uso.

5.3.5 Gestión de identidad

Es importante que las organizaciones tengan un identificador único para cada empleado. Esto a menudo se usa como su ID para acceder a todos los sistemas informáticos, y también como el identificador clave para el individuo en la organización. Sin embargo, mantener la base para la identificación del personal distinta de la utilizada para los sistemas informáticos puede mitigar este riesgo. Puede llevar a un trabajo adicional, pero seguramente ayudará a limitar el daño de un ataque.

5.3.6 Procedimientos de operación

Los procedimientos operativos estándar, especialmente aquellos relacionados con la provisión de acceso o autorización de seguridad, deben tener una verificación cruzada o un paso de 'devolución de llamada' antes de que se otorgue la solicitud.

Esto reducirá la cantidad de veces que el hacker puede salirse con la suya tratando de hacerse pasar por un usuario legítimo.

5.3.7 Gestión de incidentes de seguridad

Cuando se produce un ataque de ingeniería social, asegúrese de que el personal de la mesa de servicio sepa cómo gestionar el incidente. Cada incidente proporciona nuevas entradas

para una revisión continua de la seguridad dentro del modelo de respuesta a incidentes. Para gestionar un incidente, el personal de la mesa de servicio debe tener un protocolo sólido de notificación de incidentes que registre la siguiente información:

- Nombre del objetivo
- Departamento objetivo
- Fecha
- Vector de ataque
- Descripción del ataque
- Resultado del ataque
- Efecto de ataque

- Recomendaciones

Al registrar incidentes, es posible identificar patrones y posiblemente evitar ataques adicionales.

5.3.8 Protección del seguro

Finalmente, una organización puede comprar un seguro contra ataques de seguridad. Sin embargo, la mayoría de las aseguradoras buscarán políticas y procedimientos de la compañía que trabajen para reducir la amenaza de ataques. En general, las aseguradoras no se molestan tanto con los productos de seguridad que una organización está utilizando para mitigar los ataques en comparación con el enfoque en la conciencia de los empleados, los controles de acceso lógicos, físicos y administrativos y las políticas de seguridad establecidas

Conclusión

En este proyecto de evaluación de la seguridad de la información en la Administradora de Riesgos Laborales, se ha hecho una extensa introducción y definición de la Ingeniería Social y todas sus técnicas. Asimismo, se han desarrollado extensamente los diferentes vectores de ataques alrededor del mundo y sus contramedidas, tales como, las normas y certificaciones de identificación y mitigación de los riesgos y los métodos de control para prevenir y contener los ataques a la seguridad de los datos. Se han explicado las técnicas que los agentes maliciosos e ingenieros sociales usan hoy en día para lograr que los usuarios revelen información personal y confidencial describiendo cada una de ellas y los métodos de los que son apoyados. En efecto, se ha hecho un pequeño análisis de los conocimientos y capacidades de los empleados dentro de la institución a la hora de identificar posibles ataques a la seguridad de la información.

Recordando que la Ingeniería Social es la técnica más influyente a nivel psicológico de las personas, siendo estas más vulnerables desde un punto de vista humano y social. La Ingeniera Social utilizada como vector de ataque y dependiendo de si el objetivo del atacante es el usuario o la empresa para la que trabaja puede ser de un impacto bastante significativo. Para finalizar, se ha propuesto una serie de recomendaciones que deben ser tomadas en consideración por la Administradora de Riesgos Laborales para la futura preparación de sus empleados. Ante todo, estas medidas son de concienciación dirigida a educar a los empleados de una forma directa acerca de los peligros de la Ingeniería Social y todas sus facetas.

Un tema para destacar dentro y fuera de esta investigación es la falta de campañas de concientización con respecto a la Ingeniería Social y otros vectores de ataques. En cuanto a este caso se refiere, existe bastantes tabúes y exclusión del tema en las empresas. Ya sea por cuestiones de imagen corporativa o simplemente miedo a ser cuestionadas por sus empleados. Personalmente somos participes de trabajar mano a mano con este tema para y de manera directa, para así eludir el miedo y des concertación en los empleados.

La Ingeniería Social muchas veces es olvidada por los “expertos” en ciber seguridad, los cuales se enfocan más en aspectos tecnológicos y no trabajan es eslabón más débil en la cadena de la seguridad de la información, el ser humano.

Glosario de Términos

Ingeniería social: El conjunto de técnicas o estrategias sociales utilizadas de forma predeterminada por un usuario para obtener algún tipo de ventaja respecto a otro u otros. Por lo que de ingeniería tiene más bien poco, es más, de hecho, se acerca más a la psicología social o la sociología de ventas. Ya que, para llevar a cabo ataques de ingeniería social, no tienes por qué tener conocimientos técnicos de ningún tipo.

Usuario no entrenado: Usuario con falta de educación en el tema u herramienta que maneja, en este caso podemos decir llanamente que utiliza equipos tecnológicos para manejar información delicada pero no tiene idea de lo riesgoso que puede ser en manos equivocadas.

Malware: El término malware (también conocido como software malicioso o software malintencionado) hace referencia a todo tipo de programas diseñados específicamente para dañar un ordenador o una red o para obtener algún tipo de beneficio o hacer mal uso del mismo.

Phishing: El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como puede ser una contraseña, información bancaria u otra información personal de la víctima.

Ancho de banda: El ancho de banda en términos informáticos, es básicamente la cantidad de datos que podemos enviar y recibir en el ámbito de una comunicación por unidad de tiempo. Nosotros podemos consumir una serie de recursos o datos expresados 9 en bits y sus distintos múltiplos, entonces podemos entender el ancho de banda como un rango para trasferir datos o la tasa de transferencia de datos.

El software malicioso: O el termino programa maligno es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El termino virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

Datos: Los datos son números, letras o símbolos que describen objetos, condiciones o situaciones. Son el conjunto básico de hechos referentes a una persona, cosa o transacción de interés para distintos objetivos, entre los cuales se encuentra la toma de decisiones. Desde el punto de vista de la computación, los datos se representan como pulsaciones o pulsos electrónicos a través de la combinación de circuitos (denominados señal digital).

Escudriñar: Este concepto permite aludir al desarrollo de un análisis o un examen pormenorizado de algo, tratando de comprender su funcionamiento o sus características.

Integridad de los datos: Asegura que la información y los programas puedan ser cambiados solo por el personal autorizado. En este mismo orden, podemos describir integridad de sistema, la cual asegura que el sistema funciona como se espera, sin necesidad de manipularlo de manera deliberada o sin la debida autorización.

Vector de ataque: El término en sí es un préstamo del argot militar; y en este sentido, un vector de ataque se refiere literalmente a un agujero o falla presente en la defensa establecida.

Homepage: Es una página designada para ser el principal punto de entrada a un sitio web, apareciendo cuando un usuario comienza una sesión. Las páginas de inicio suelen ofrecer una bienvenida al internauta, un texto donde se explica el significado del sitio **web** y un menú con links a otras páginas.

Wifi: Es una *tecnología de comunicación inalámbrica* que permite conectar a Internet equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información. Es originalmente una abreviación de la marca comercial Wireless Fidelity, que en inglés significa 'fidelidad sin cables o inalámbrica'.

Variable: Una variable refiere, en una primera instancia, a cosas que son susceptibles de ser modificadas (de variar), de cambiar en función de algún motivo determinado o indeterminado.

Cisco: Es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.

Intranet: Una Intranet es una plataforma digital cuyo *objetivo asistir a los trabajadores en la generación de valor para la empresa*, poniendo a su disposición

activos como contenidos, archivos, procesos de negocio y herramientas; facilitando la colaboración y comunicación entre las personas y los equipos.

Hacker: Es simplemente un sujeto inteligente, experto en manipular o modificar un sistema o red informática, un hacker malicioso es alguien que utiliza sus conocimientos de informática para obtener acceso no autorizado a datos tales como información de tarjetas de crédito o imágenes personales, ya sea para diversión, beneficio, para causar daño o por otras razones.

Auditoria: La actividad de auditar consiste en realizar un *examen* de los procesos y de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios.

Bibliografía

- *Alicante, U. d. (2018). Seguridad Informática. Obtenido de https://moodle2018-19.ua.es/moodle/pluginfile.php/152856/mod_resource/content/7/seguridad/2confidencialidad.html.*
- *Barzanallana, R. (2017). Introduccion a la Seguridad Informatica. Obtenido de https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf.*
- *BISSON, D. (5 de Noviembre de 2019). 5 Social Engineering Attacks to Watch Out For. Obtenido de https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.*
- *Caballero, J. (16 de Septiembre de 2019). Ingeniería social en la universidad, breve repaso a las principales técnicas. Obtenido de https://www.yolandacorral.com/ingenieria-social-universidad-tecnicas/.*
- *CIsco. (2018). Reporte Anual de Ciberseguridad. Obtenido de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf.*
- *Department, S. R. (17 de Enero de 2019). Número de cuentas de correo electrónico activas en todo el mundo 2014 - 2019. Obtenido de https://es.statista.com/estadisticas/637679/numero-de-cuentas-de-correo-electronico-activas-en-todo-el-mundo--2019/.*
- *Desconocido. (17 de Diciembre de 2012). SEGURIDAD PERSONAL Y PROFESIONAL. Obtenido de https://seguridadpersonalyprofesional.com/2012/12/17/ingenieria-social/.*
- *Desconocido. (2015). ¿Qué es el vishing? Obtenido de https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/.*
- *Desconocido. (7 de Noviembre de 2018). 20 ejemplos de ataques informáticos que puede sufrir una empresa. Obtenido de https://uss.com.ar/corporativo/ejemplos-de-ataques-informaticos-empresa/.*
- *Diario, L. (25 de Julio de 2017). Empleados: un puente para delitos de cibercriminales. Obtenido de https://listindiario.com/tecnologia/2017/07/25/475414/empleados-un-puente-para-delitos-de-cibercriminales.*
- *Dikovec, T. (25 de Marzo de 2019). Ingeniería Social: el arte de la manipulación humana. Obtenido de https://tahiridikovec.com/ingenieria-social-el-arte-de-la-manipulacion-humana/.*
- *ESET. (8 de Enero de 2016). Top 5 de las brechas de datos más devastadoras de 2015. Obtenido de https://www.welivesecurity.com/la-es/2016/01/08/top-5-brechas-de-datos-devastadoras-2015/.*

- *FBI. (2019). Cyber Crime. Obtenido de https://www.fbi.gov/investigate/cyber.*
- *Flatley, B. N. (13 de Mayo de 2018). ROOTKIT DETECTION USING A CROSS-VIEW. Obtenido de https://pdfs.semanticscholar.org/5395/480dc945df9dcf52bb2cc5969e2b593cf5c6.pdf.*
- *Fyodor. (1997). The art of port scanning. Phrack Magazine.*
- *Gopali, G. (2018). https://www.csoonline.com/article/3257429/what-is-sql-injection-how-sqli-attacks-work-and-how-to-prevent-them.html. Obtenido de https://muep.mau.se/bitstream/handle/2043/25890/Gopali.pdf?sequence=1&isAllowed=y.*
- *Guedez, A. (27 de Febrero de 2018). Conoce los riesgos y amenazas de la ingeniería social sobre tus activos y datos sensibles. Obtenido de https://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/.*
- *Herrera, E. (15 de Septiembre de 2014). Principios fundamentales que se busca proteger con la seguridad informática. CIA. Obtenido de https://informaticaseguraupc.wordpress.com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/.*
- *http://www.ecoeediciones.com/wp-content/uploads/2016/08/seguridad-informatica-basico.pdf. (2016). Seguridad Informatica Basico. Obtenido de http://www.ecoeediciones.com/wp-content/uploads/2016/08/seguridad-informatica-basico.pdf.*
- *INCIBE. (5 de Septiembre de 2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.*
- *Jaramillo, V. d., Rivera, S. P., Juárez, J. E., Gutiérrez, H. E., & García, N. F. (2016). http://rikudazr17.weebly.com/uploads/4/9/8/2/49821357/3_casos_de_ingenier%C3%8Da_social_m%C3%81s_famosos_en_los_%C3%9Altimos_3_a%C3%91os.pdf. Obtenido de http://rikudazr17.weebly.com/uploads/4/9/8/2/49821357/3_casos_de_ingenier%C3%8Da_social_m%C3%81s_famosos_en_los_%C3%9Altimos_3_a%C3%91os.pdf.*
- *Jorge, M. (2016). Pioneros de la ingeniería social: el hacker ciego que puso de rodillas al FBI. Obtenido de https://es.gizmodo.com/pioneros-de-la-ingenieria-social-el-hacker-ciego-que-p-1789268307.*
- *Kaspersky. (2 de Noviembre de 2017). LokiBot: robo o extorsión. Obtenido de https://www.kaspersky.es/blog/lokibot-trojan/14718/.*
- *Ledesma, C., Ledesma, A., & Pascale, M. (10 de Octubre de 2014). Ingeniería social – El hackeo al ser humano. Un enfoque holístico. Obtenido de https://www.magazcitum.com.mx/?p=2747#.XciG7DMzY2y.*

- *Mendoza, M. Á. (6 de Noviembre de 2017). 6 consideraciones previas a la implementación del SGSI. Obtenido de https://www.welivesecurity.com/la-es/2017/11/06/consideraciones-implementacion-del-sgsi/.*
- *Moes, T. (2019). ¿Qué es spyware? La definición y los 5 ejemplos principales. Obtenido de https://softwarelab.org/es/que-es-spyware/.*
- *Mundo, B. (2016). "12 ataques por segundo": cuáles son los países de América Latina más amenazados por "malware". Obtenido de https://www.bbc.com/mundo/noticias-37286420.*
- *MuySeguridad. (31 de Diciembre de 2018). Los 12 peores incidentes de ciberseguridad de 2018. Obtenido de https://www.muyseguridad.net/2018/12/31/12-incidentes-de-ciberseguridad-de-2018/.*
- *NIST. (2002). https://informaticaseguraupc.wordpress.com/2014/09/15/principios-fundamentales-de-la-seguridad-de-la-informacion-cia/. Obtenido de https://www.ucop.edu/information-technology-services/initiatives/resources-and-tools/sp800-30.pdf.*
- *Ojeda, C. (2018). Ingeniería social: ¿el lado oscuro de la Psicología? Obtenido de https://psicologiaymente.com/social/ingenieria-social-psicologia.*
- *Pandini, W. (16 de Junio de 2015). 16 Jun Seguridad de la información: qué es y por qué las empresas deben invertir. Obtenido de https://ostec.blog/es/generico/seguridad-de-la-informacion.*
- *PENAGOS, E. B. (2015). INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN LA UNIVERSIDAD COOPERATIVA DE COLOMBIA SEDE NEIVA. Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3629/1/1075210015.pdf.*
- *PETTERS, J. (24 de Abril de 2018). What is a Rootkit? How Can You Detect it? Obtenido de https://www.varonis.com/blog/rootkit/.*
- *Poggl, N. (3 de Diciembre de 2018). 24 Estadísticas de Seguridad Informática que Importan en el 2019. Obtenido de https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/.*
- *Ponce, R. A. (2018). EL VALOR DE LA PRIVACIDAD: DATOS PERSONALES EN TIEMPOS DEL PANÓPTICO. Obtenido de https://revista.seguridad.unam.mx/.*
- *Porup, J. (2 de Octubre de 2018). What is SQL injection? How SQLi attacks work and how to prevent them. Obtenido de https://www.csoonline.com/article/3257429/what-is-sql-injection-how-sqli-attacks-work-and-how-to-prevent-them.html.*
- *Regan, J. (11 de Julio de 2019). What is Malware? How Malware. Obtenido de https://www.avg.com/en/signal/what-is-malware.*
- *Rivero, A. O. (2009). Ciencias Sociales y administrativas. Investigación académica. Bolivia.*

- *Rivero, M. (2008). ¿Que es el Phising? Obtenido de https://www.infospyware.com/articulos/que-es-el-phishing/.*
- *Rouse, M. (2019). Trojan horse (computing). Obtenido de https://searchsecurity.techtarget.com/definition/Trojan-horse.*
- *Seals, T. (2018). Android Banking Trojan Fakebak adds Vishing Dimension. Obtenido de https://www.infosecurity-magazine.com/news/fakebank-android-banking-trojan/.*
- *Security, P. (25 de Marzo de 2019). What is Adware? Tips for Preventing and Removing. Obtenido de https://www.pandasecurity.com/mediacenter/panda-security/what-is-adware/.*
- *Sevilla, M. (2011). Anteproyecto de investigacion. Santo Domingo.*
- *Shcherbakova, T. (29 de Agosto de 2018). Loki Bot: On a hunt for corporate passwords. Obtenido de https://securelist.com/loki-bot-stealing-corporate-passwords/87595/.*
- *Shoniregun, C. A. (2008). CSTST '08 Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology. New York: ACM.*
- *Solano, E. R. (23 de Junio de 2010). La ingeniería social, una de las herramientas más importantes en las pruebas de seguridad. Obtenido de https://www.magazcitum.com.mx/?p=313#.XciF4DMzY2y.*
- *Souza, Á. (17 de Mayo de 2018). 17 May Ingeniería social y los impactos en el medio corporativo. Obtenido de https://ostec.blog/es/generico/ingenieria-social-impactos.*
- *Stuart Staniford, J. A. (2000). Practical automated detection of stealthy portscans. 7th ACM Conference on Computer. Athens, Greece.*
- *Torres, G. (25 de Septiembre de 2018). Man-in-the-Middle Attacks: What They Are and How to Prevent Them. Obtenido de https://www.avg.com/en/signal/man-in-the-middle-attack.*
- *UnderC0de. (2017). ¿Qué es la Ingeniería Social? Obtenido de https://underc0de.org/hacking/ingenieria-social.html.*

Anexo

DECANATO DE INGENIERÍAS E INFORMÁTICA

ESCUELA DE INFORMÁTICA

Anteproyecto del Trabajo Final de Grado para optar por el título de Ingeniería en Sistema de Computación.

Evaluación de la seguridad de la información utilizando ingeniería social como vector de ataque en la Administradora de Riesgos Laborales. Periodo cuatrimestral Septiembre-Diciembre 2019.

Integrantes:

Luis Rafael Segura 2015-2252

Bryan Isaul Peña 2009-0238

Jueves 18 de Julio del año 2019

Santo Domingo, R.D

DEPARTAMENTO DE SOCIALES
PROYECTO DE TRABAJO DE GRADO
APROBADO
FIRMA
FECHA 22/7/19

Índice.

Índice.

Evaluación de la seguridad de la información utilizando ingeniería social como vector de ataque en la Administradora de Riesgos Laborales. Periodo cuatrimestral Septiembre-Diciembre 2019.

INTRODUCCION.

Refiriéndonos a la ingeniería social como las técnicas y estrategias sociales utilizadas especialmente desde un ámbito psicológico para obtener algún tipo de ventaja sobre un objetivo predeterminado. Entonces dicho esto, podemos afirmar que en las manos equivocadas y con las intenciones no debidas, dicha técnica podría ser mortal para cualquier individuo. Pero, sobre todo a organizaciones e instituciones, las cuales poseen bajo su responsabilidad todo tipo de documentación personal de todos sus clientes, usuarios y personas allegadas a las mismas.

Es por ello, que se hace evidente la clara necesidad de evaluar la seguridad de la información utilizando mencionada técnica como vector de ataque. Asimismo, incentivar a la precia documentación por parte de los empleados dentro de la misma, los cuales son el factor más importante a la hora de llevar acabo el ataque. Sin embargo, no todo el conocimiento debe de provenir de una sola vía, pues la parte directiva de la institución está obligada a estar al tanto de las posibles causas de un ataque mal intencionado.

JUSTIFICACION.

Justificación teórica

Es claro que a instituciones y organizaciones de mediana y gran escala no le convence del todo decir que hasta cierto punto si son vulnerables y poseen mínimas debilidades que corren el riesgo de ser explotadas por una amenaza latente; los agentes maliciosos. Siguiendo lo antes dicho, podemos decir abiertamente que poseemos un enfoque fuera de lo común en cuanto a esto, pues buscamos la aceptación propia para así poder construir una base fructífera en cuanto a protección y prevención de los ataques de ingeniería social se refiere.

Justificamos este estudio por como la información debe ser tratada y a su vez manipula, teniendo como enfoque primario la desinformación por parte de los empleados con relación a estos casos. Entendemos que en ocasiones es de suma importancia dar el primer paso y más aún cuando nos referimos a la seguridad de la información, lo más preciado en nuestra actualidad. Sin duda alguna.

Justificación practica

Esta investigación se realiza porque existe la necesidad de mejorar el nivel de información por parte de los empleados en relación a los ataques de ingeniería social y las consecuencias de los mismos. Asimismo, entendemos que dicho trabajo de investigación llevara a la contribución de medidas que podrían ser aplicadas a partir de nuestros resultados obtenidos.

Justificación metodológica

A sabiendas que la observación es el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en el ambiente y que el método deductivo parte de lo general a lo particular, justificamos la implementación de estos por ser y poseer las características más adecuadas para esta investigación.

DELIMITACION DEL TEMA Y PLANTEAMIENTO DEL (LOS) PROBLEMA (S) DE INVESTIGACION.

La Administradora de Riesgos Laborales (ARL) tiene bajo su tutela un gran manejo de información personal y financiera de sus afiliados en los casos presentados así mismo como todos los datos interinos de la institución, referencia delicada y de sumo interés para atacantes maliciosos. Es por ello, que la institución coloca bastante énfasis en sobre guardar todos estos datos privilegiados. Sin embargo, en los últimos años se ha incrementado considerablemente la penetración, sustracción y des integridad de los datos por parte de dichos agentes mal intencionados.

A razón de esto es importante evaluar las debilidades en la integridad y confiabilidad de los datos en dicha institución, los cuales son manejados día tras día por usuarios que no siempre están a la par de estar conscientes de lo que tienen en sus manos. Manejadores de información con nivel pobre de conocimiento de que tan importante son los que tienen a su disposición y en cuanto a los vectores de ataque existentes para el hurto de información pertinente. La cual mal utilizada y en el momento preciso puede ser mortal para el afectado y de gran ayuda para quien la posea.

Cabe señalar que en la actualidad existen normas y protocolos a seguir, Pero la mayoría de estos son totalmente desconocidos por los empleados. Dichas normas y protocolos no son para erradicar por completo el riesgo latente antes visto, sino que buscan disminuir y colocar más cerca de la marca cero los éxitos en los ataques de ingeniería social y usuarios no entrenados. Hay que destacar que la mayoría de las instituciones y organizaciones no le es atractivo sacar a flote este tipo de problemas, pero, en definitiva, es preciso insistir en el conocimiento y capacitación pertinente sobre dicha situación, no ver el problema como enemigo en todo esto sino, hacer evidente a nivel interino estos… detalles y así atacar directamente; para brindar un seguimiento y soporte de ayuda a situaciones presentadas.

Esta investigación se enfocara en la sede principal de la Administradora de Riesgos Laborales, ubicada en el Distrito Nacional de República Dominicana. Los datos que serán recolectados los cuales sustentan la investigación serán obtenidos de primera mano. Periodo cuatrimestral Septiembre-Diciembre del año 2019.

OBJETIVO GENERAL Y ESPECIFICOS.

Objetivo general

Evaluar la seguridad de la información en la Administradora de Riesgos Laborales.

Objetivos específicos

- Cuantificar las consecuencias ante la inseguridad de los datos.
- Enumerar los pasos existentes en la elaboración de la seguridad de la información.
- Clasificar las vulnerabilidades en la seguridad de los datos.
- Mitigar los posibles daños obtenidos luego de un ataque de ingeniería social.

MARCO REFERENCIAL (FUNDAMENTOS TEORICOS, ANTEDENTES DEL PROBLEMA).

Marco teórico referencial

Pensemos que las contraseñas son la puerta de entrada de un usuario a decenas de servicios online, y solo una parte de las buenas prácticas que se deben seguir para estar seguros en Internet. El robo de credenciales siempre ha estado a la orden del día y es por eso que la importancia de reforzarlas hace rato quedó demostrada. (Pagnotta, 2015)

"En la década de 1960 de acuerdo con Frank Abagnale pudo convencer al personal de Pan Am, junto con muchos otros, de que era un piloto comercial. Después de usar un pretexto en el que asumió la identidad de un periodista de un periódico escolar, pudo recopilar información sobre políticas, procedimientos y la inestimable terminología de la industria. Armado con este conocimiento y un uniforme de piloto de Pan Am, pudo volar de forma gratuita, así como utilizar su conocimiento del proceso bancario de Pan Am para cobrar cheques fraudulentos. Si un ingeniero social ve, actúa y suena la parte, existe una gran probabilidad de que las personas tomen al atacante a su valor nominal y no cuestionen más el pretexto." (Nathaniel S. , 2018)

Según el mismo en 1971, se envió el primer correo electrónico, consolidando un nuevo vector de ataque para que los ingenieros sociales lo usaran en los próximos años una vez que las empresas y los usuarios domésticos obtuvieran acceso a este método de comunicación y comenzaran a usarlo con frecuencia. La disponibilidad del correo electrónico como plataforma de ingeniería social elimina aún más al ingeniero social de los riesgos al utilizar este el anonimato de establecer comunicaciones con el objetivo.

En 2016, según IBM informó que 1 de cada 131 correos electrónicos no fueron solicitados y contenían archivos adjuntos de malware. Según las cifras del mismo año, se enviaron 269 mil millones de correos electrónicos a nivel mundial en un Solo día. Una estimación de los correos electrónicos de phishing / malware distribuidos cada día en base a estos números es la asombrosa cifra de 2,044, 400,000. Esto no quiere decir que cada uno de esos correos electrónicos entregados alcanzó su objetivo, pero en el juego de los números, se garantiza que al menos uno de esos correos electrónicos se habrá entregado y obligado al objetivo a divulgar información o instalar software malicioso. Sin duda, esto aumentará año tras año, ya que los avances tecnológicos permiten un mayor almacenamiento y ancho de banda.

Con más usuarios que cargan datos confidenciales en repositorios en línea, cada vez es más sencillo de obtener acceso y utilizar estos datos a los que no se deberían de tener dominio público. A pesar de los frecuentes artículos de noticias que destacan la importancia de administrar los datos y utilizar contraseñas que sean seguras o no para varias cuentas, las personas tienen y seguirán sin prestar atención al consejo. Para aquellos usuarios que protegen sus datos con contraseñas complejas, todavía están a la orden de los controles de seguridad de los repositorios de datos. "Con la disponibilidad de brechas de datos históricos, así como las brechas que sin duda ocurrirán en el futuro, creo que los atacantes evitarán el uso de campañas de phishing genéricas y utilizarán más campañas de phishing de lanza combinadas con tácticas de chantaje de las brechas de datos. Por ejemplo, una campaña de phishing estándar contra un director financiero de una empresa probablemente se ignoraría y no daría resultados. Un ataque de phishing dirigido contra el director financiero, que utiliza datos de la brecha de datos de Ashley Madison (Red Social de parejas), diseñado para invocar el pánico basándose en datos de la vida real que podrían causar un daño significativo tanto dentro como fuera del lugar de trabajo, es más probable que reciba la atención del objetivo y tendría una mayor posibilidad de obtener los resultados esperado desde la perspectiva de los atacantes" (Nathaniel, 2018).

Es más fácil engañar a alguien para que dé su contraseña de ingreso a un sistema que hacer el esfuerzo para hackearlo. (Mitnick, 2016)

Marco conceptual

Ingeniería social: "El conjunto de técnicas o estrategias sociales utilizadas de forma predeterminada por un usuario para obtener algún tipo de ventaja respecto a otro u otros. Por lo que de ingeniería tiene más bien poco, es más, de hecho, se acerca más a la psicología social o la sociología de ventas. Ya que, para llevar a cabo ataques de ingeniería social, no tienes por qué tener conocimientos técnicos de ningún tipo" (Berenguer, 2018).

Usuario no entrenado: "Usuario con falta de educación en el tema u herramienta que maneja, en este caso podemos decir llanamente que utiliza equipos tecnológicos para manejar información delicada pero no tiene idea de lo riesgoso que puede ser en manos equivocadas" (Alonzo, 2019).

Malware: "El término malware (también conocido como software malicioso o software malintencionado) hace referencia a todo tipo de programas diseñados específicamente para dañar un ordenador o una red o para obtener algún tipo de beneficio o hacer mal uso del mismo" (Universidad de Jaen , 2018).

Phishing: "El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como puede ser una contraseña, información bancaria u otra información personal de la víctima" (AndaluciaCERT, 2017).

Ancho de banda: "El ancho de banda en términos informáticos, es básicamente la cantidad de datos que podemos enviar y recibir en el ámbito de una comunicación por unidad de tiempo. Nosotros podemos consumir una serie de recursos o datos expresados en bits y sus distintos múltiplos, entonces podemos entender el ancho de banda como un rango para trasferir datos o la tasa de transferencia de datos" (Castillo, 2019).

El software malicioso: "El termino malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El termino virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos" (Ezquerra, 2016).

Datos: "Los datos son números, letras o símbolos que describen objetos, condiciones o situaciones. Son el conjunto básico de hechos referentes a una persona, cosa o transacción de interés para distintos objetivos, entre los cuales se encuentra la toma de decisiones. Desde el punto de vista de la computación, los datos se representan como pulsaciones o pulsos electrónicos a través de la combinación de circuitos (denominados señal digital)" (Dip, 2009).

Escudriñar: "Este concepto permite aludir al desarrollo de un análisis o un examen pormenorizado de algo, tratando de comprender su funcionamiento o sus características" (Porto, 2017).

Integridad de los datos: "Asegura que la información y los programas puedan ser cambiados solo por el personal autorizado. En este mismo orden, podemos describir integridad de sistema, la cual asegura que el sistema funciona como se espera, sin necesidad de manipularlo de manera deliberada o sin la debida autorización" (Monrrobert, 2019).

Vector de ataque: "El término en sí es un préstamo del argot militar; y en este sentido, un vector de ataque se refiere literalmente a un agujero o falla presente en la defensa establecida" (Guedez, 2018).

HIPOTESIS PRIMER Y SEGUNDO GRADO E INDENTIFICACION DE LA VARIABLES.

Hipótesis de primer grado

Los ataques de ingeniera social a instituciones y organizaciones son más nocivos si se posee usuarios no entrenados.

Hipótesis de segundo grado

Cuando se ejecutan con éxito ataques de ingeniería social las instituciones y organizaciones pierden dinero y credibilidad.

Identificación de las variables

- Usuarios/Empleados
- Vulnerabilidades
- Motivación
- Institución

DISEÑO METODOLOGICO: METODO Y TECNICAS DE INVESTIGACION CUENTITATIVAS Y/O CUALITATIVAS.

Metodología

La siguiente investigación busca como resultado final, evaluar la seguridad de la información en la Administradora de Riesgos Laborales e identificar y mitigar las razones principales de la plena desinformación por parte de los empleados con relación a los danos que los ataques de ingeniería social pueden provocar. Por tal razón, podemos clasificar la investigación de tipo explicativa, pues su objetivo final es explicar por qué ocurre dicho fenómeno y en qué condiciones se ejecuta el mismo.

Debemos tener claro que en esta investigación ocurrirá un proceso deliberado de observación, el cual ayudara a lograr resultados de los objetivos ya planteados previamente. A su vez, podemos afirmar que iremos de la mano con el método de estudio deductivo, pues partiremos de una vista general para luego identificar las verdades particulares. Sin embargo, también nos apoyaremos en el método analítico, el cual puede establecer la relación causa-efecto.

Teniendo claro que las fuentes de la investigación vendrán por parte de libros, textos y trabajos de estudios previamente realizados, la podemos clasificar como primarias. Al mismo tiempo que, iremos apoyados con técnicas como las encuestas, cuestionarios, observación y sondeos, para llegar de una manera focal a los objetivos.

Tipo de investigación

Explicativa: (Sevilla, 2011) Buscan encontrar las razones o causas que ocasionan ciertos fenómenos, su objetivo último es explicar por qué ocurre un fenómeno y en qué condiciones se da éste.

Investigación de campo: (Rivero, 2009) Es el conjunto de acciones encaminadas a obtener en forma directa datos de las fuentes primarias de información, es decir, de las personas y en el lugar y tiempo en que se suscita el conjunto de hechos o acontecimientos de interés para la investigación.

Método de investigación

Observación: (Sevilla, 2011) Es el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en la realidad por medio de un esquema conceptual previo y con base en ciertos propósitos definidos generalmente por una conjetura que se quiere investigar.

Deductivo: (Sevilla, 2011) Consiste en ir de lo general a lo particular; se inicia con la observación de fenómenos generales con el propósito de señalar las verdades particulares, el proceso deductivo no es suficiente por sí mismo para explicar el conocimiento.

Análisis/analítico: (Sevilla, 2011) Maneja juicios, es un proceso de conocimiento que se inicia por la identificación de cada una de las partes que caracterizan una realidad, podrá establecer la relación causa-efecto entre los elementos que componen el objeto de investigación.

Fuentes documentales de la investigación

Primarias: (Sevilla, 2011) Es un documento original de investigación o escrito en el que se puede hallar la información completa, presentada de manera detallada y utilizando un lenguaje técnico, referente a un informe de investigación o a una teoría, en el proceso de investigación suelen ser fuentes primarias los libros, los textos y las revistas, entre otros.

Técnicas de estudio cualitativas

Encuestas: (Sevilla, 2011) Es una técnica que al igual que la observación está destinada a recopilar información, se realiza mediante el uso de formularios para determinar los problemas a ser investigados.

Cuestionarios: (Sevilla, 2011) Es un conjunto de preguntas, preparado cuidadosamente, sobre los hechos y aspectos que interesan en una investigación, para que sea contestado por la población o su muestra. Se aplica a una población homogénea con niveles similares y problemática semejan

FUENTES DE DOCUMENTACION (FUENTES BIBLIOGRAFICAS).

Bibliografía

AndaluciaCERT. (2017). *Informe de divulgacion de phishing* . Andalucia .

Berenguer, D. (2018). *Estudio de metodologias de ingenieria social.* Catalunya.

Castillo, J. A. (2019). Ancho de banda: Definición, qué es y cómo se calcula. *Profesional review*.

Dip, P. (2009). Datos. *Tecnologia e Informatica*.

Ezquerra, J. (2016). Definicio de software malicioso .

Guedez, A. (2018). ¿A qué se le conoce como vectores de ataque en ciberseguridad y cómo puedes eliminarlos de tus ambientes digitales? *gbadvisors*.

Mitnick, K. (2016).

Monrrobert, E. (2019). *Hacking etico* . Santo Domingo .

Nathaniel. (2018).

Nathaniel, S. (2018). The History and Evolution of Social Engineering Attacks. *comissun*.

Pagnotta, s. (2015). *welivesecurity*.

Porto, J. P. (2017). *Definiciones.DE*.

Real Academia Española . (2019).

Rivero, A. O. (2009). *Ciencias Sociales y administrativas. Investigación académica.* Bolivia.

Sanjuan, L. D. (2011). *textos de apoyo didactico.*

Sevilla, M. (2011). *Anteproyecto de investigacion.* Santo Domingo.

Universidad de Jaen . (2018). Guia de Seguridad UJA.

2.3 Técnicas de la ingeniería social

2.4 Tecnología aplicada en la ingeniería social

ESQUEMA PRELIMINAR DE CONTENIDO DEL "TRABAJO DE GRADO".

Portada

Índice

Dedicatoria y Agradecimientos

Introducción

Metodología

Capítulo 1: ASPECTOS INTRODUCTORIOS DEL PROYECTO

1.1 Selección del tema

1.2 Planteamiento del problema

1.3 Justificación

1.4 Objetivos

1.4.1 General

1.4.2 Específicos

1.5 Alcance

1.6 Metodología de investigación

1.6.1 Métodos

1.6.2 Técnicas

1.7 Población de la muestra

1.7.1 Determinación de la muestra

El Sistema de Gestión de La Seguridad de la Información que propone la Norma ISO 27001

Fuente: (sitio web oficial de las Nomar ISO)

Método de Evaluación y Tratamientos del Riesgo

Fuente: (Sitio web oficial de las Normas ISO)

Parte frontal de la Sede Central de La Administradora de Riesgos Laborales.

Fuente: (Consejo Nacional de Seguridad Social)

Sede Central de Google.

Fuente: (Periódico el Dinero)

The Renaissance Center, Detroit. Sede Central de la cadena de Hoteles Marriott.

Fuente: (Flickr)

Logo de Ubiquiti Networks.

Fuente: (LLoud´S)

L