LA FALTA DE CONCIENCIA, UNA VULNERABILIDAD LATENTE PARA LA SEGURIDAD DE LA INFORMACIÓN

Dayhan Geraldynn Zambrano Granada

Identificación: 1118297496

ESPECIALIZACIÓN EN ADMINISTRACION DE LA SEGURIDAD

UNIVERSIDAD MILITAR NUEVA GRANADA

CALI

2019

Introducción

En la actualidad, es imposible controlar los sistemas de información e informática de manera perfecta, debido a los constantes avances tecnológicos y la falta de conocimiento sobre los riesgos y las vulnerabilidades de cada organización y sus procesos. Asumir los riesgos y saber cómo gestionarlos contribuye con la minimización y control de su aparición; así como su materialización. Sin embargo, en mayor proporción los ciber ataques se presentan por falta de conciencia en las personas; estos delincuentes se aprovechan de sus víctimas para sacar provecho y lograr acceder a la información financiera, privada y lograr extorsionar a los dueños de estas; con lo que el foco principal de todas las organizaciones debería ser la formación y monitoreo de la toma de conciencia de las Personas. Por esta razón en este ensayo nos centraremos en los comportamientos de cada individuo dentro de su entorno laboral, más específicamente en el Sector de la Vigilancia y Seguridad Privada y la importancia de su rol como administradores de los activos de información dentro de sus organizaciones.

PALABRAS CLAVES: Seguridad de la Información, Toma de Consciencia, Personas, Vulnerabilidad, Riesgo, Activos de Información.

Abstract

At present, it is impossible to control the information and computer systems perfectly, due to the constant technological advances and lack of knowledge about the risks and vulnerabilities of each organization and its processes. Taking risks and knowing how to manage them contributes to the minimization and control of their appearance; as well as its materialization. However, to a greater extent cyber-attacks occur due to lack of awareness in people; these criminals take advantage of their victims to take advantage and gain access to financial, private information and extort money from their owners; with which the focus of all organizations should be the training and monitoring of awareness of people. For this reason, in this essay we will focus on the behaviors of everyone within their work environment, more specifically in the Private Security and Surveillance Sector and the importance of their role as administrators of information assets within their organizations.

KEYWORDS: Information Security, Awareness, People, Vulnerability, Risk, Information Assets.

Con el paso de los años el crecimiento de la tecnología y los avances en la comunicación han ocasionado que se originen una serie de sucesos inesperados llamados ataques cibernéticos, los cuales hacen parte de una cadena delictiva que ha generado un vuelco en los controles de la información y la conectividad a nivel mundial, la facilidad con la que se puede acceder a los sistemas en la actualidad hace vulnerable a todo el que tenga acceso a la web, equipos, y/o herramientas tecnológicas. Por esta razón, la información representa un capital muy importante y una parte vital del rendimiento y rentabilidad de las compañías. De tal modo, es imprescindible crear sistemas que puedan gestionarla y protegerla.

Una forma de garantizar la seguridad de la información es conocer las normativas que engloban los Sistemas de Gestión de Seguridad de la Información: **ISO 27001**. Las empresas deben estar al tanto de estas normas y formar al personal en ellas, desde el director a los operarios que manejarán el sistema. Así mismo, es importante contar con asesores que estén permanentemente actualizados para descubrir cualquier grieta dentro del sistema.

Lo más importante es trabajar en el punto más vulnerable de la red: los usuarios. La clave en todo sistema de seguridad informático es la educación de las personas, ya que los hackers emplean lo que se conoce como 'ingeniería social' para llevar a un individuo a dar información de manera natural. Mediante la manipulación engañosa, los hackers pueden obtener datos valiosos que resulten perjudiciales para una compañía.

La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada.

Ante esta situación, los Sistemas de Gestión de la Seguridad de la Información deben contener un inciso para educar a los usuarios y evitar que sean víctimas de la ingeniería social. También deben contar con todas las herramientas disponibles para detectar y eliminar las amenazas externas, así como un manual de acciones ante los riesgos.

La OCDE4 desarrolló por primera vez en 1992 una serie de Directrices para la Seguridad de los Sistemas de Información, las cuales tratan de promover el uso y desarrollo de una cultura de la Seguridad, no solo en el desarrollo de Sistemas y Redes de comunicación, sino mediante la adopción de "nuevas formas de pensamiento y comportamiento en el uso de la interconexión de esos sistemas".

Las Directrices presentadas son: Concientización, Responsabilidad, Respuesta Adecuada, Ética, Democracia, Evaluación del Riesgo, Diseño y Realización de la Seguridad, Gestión de Seguridad, Reevaluación.

Con la evolución de los sistemas de información y de la forma de hacer negocios, la información se ha convertido en uno de los activos de mayor valor para las personas y especialmente para las organizaciones. "Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada más dependientes de estos. Sólo un enfoque que tenga en

cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines, puede proporcionar una seguridad efectiva."

Los objetivos que se buscan con la Gestión de la Seguridad de la Información son la protección de la confidencialidad, integridad y disponibilidad de la información y de los bienes que la contienen o procesan. De esta manera, las organizaciones y personas se pueden proteger de:

- Divulgación indebida de información sensible o confidencial, de forma accidental o bien, sin autorización.
- Modificación sin autorización o bien, de forma accidental, de información crítica, sin conocimiento de los propietarios.
- Pérdida de información importante sin posibilidad de recuperarla.
- No tener acceso o disponibilidad de la información cuando sea necesaria

La información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que enfrente. La información valiosa se puede encontrar en diferentes formas: Impresa, almacenada electrónicamente, transmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas, etc.

En términos generales para entender la importancia de la información y lo que la compone siendo conscientes del valor de esta, y teniendo en cuenta que estamos frente a un mundo interconectado, en donde los sistemas, las redes y el personal involucrado en la operación se relacionan entre sí; es importante resaltar que las organizaciones deben ser responsables del manejo y protección de

sus activos; los cuales son objeto de amenazas deliberada y/o accidentales colocando en dificultades la seguridad de la información.

Estas deben definir los lineamientos generales para la implementación, mantenimiento, análisis, evaluación y mejora de un conjunto adecuado de controles, incluido políticas, procesos, procedimientos y estructura organizacional para todas las partes interesadas que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la organización y todo aquel que tenga interacción con esta información y la manipulación física o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo. Esto también incluye la información que pueda ser adquirida o suministrada a la organización de sus partes interesadas o fuentes externas de información que sean contratadas o que tengan alguna relación con la misma y establecer su compromiso con el cumplimiento de las obligaciones legales, regulatorias contractuales y de otra índole, la protección de la información creada, procesada, transmitida o resguardada por cada uno de sus procesos, la infraestructura tecnológica y activos de información, del riesgo que se genera con los accesos otorgados a terceros o como resultado de servicios subcontratados externamente. Lo anterior con el fin de minimizar los impactos que puedan originarse debido al uso incorrecto de ésta.

Tener una visión integral de la aplicación de sistemas de gestión de seguridad de la información y seguridad informática y su importancia es fundamental para cualquier profesional del área administrativa y gerencial. Emplear un SGSI brinda a las organizaciones a administrar la seguridad de los activos, tales como información financiera, propiedad intelectual, detalles de los empleados o información que hubiese sido confiada por terceros.

En el contexto de la seguridad informática se maneja mucho el término de “amenaza”. El diccionario de la lengua española, la define como el “anuncio de un mal o peligro”. En términos generales, existen dos tipos de amenazas, las que provienen de sucesos naturales, como, por ejemplo; terremotos, incendios forestales, huracanes, inundaciones, sequías, plagas, tsunamis y tornados y las amenazas provocadas por la actividad humana, como las explosiones, los incendios, los derrames de sustancias tóxicas, las guerras, el terrorismo, entre otros.

Dentro de las amenazas provocadas por la actividad humana, en este caso relacionadas con la seguridad informática, se encuentran daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.

Las amenazas en términos generales siempre están aprovechando las vulnerabilidades detectadas, generando con esto la materialización de riesgos tales como; interrupción de un servicio o procesamiento de un sistema, modificación o eliminación de la información, daños físicos, robo del equipo y medios de almacenamiento de la información, entre otros; esto nos permite identificar que las amenazas a la seguridad informática se clasifican actualmente en amenazas humanas, lógicas y físicas.

Normalmente y de acuerdo a las diferentes investigaciones de los diferentes casos, estos ataques provienen de individuos que de manera intencionada o no, causan enormes pérdidas aprovechando las vulnerabilidades que los sistemas de información puedan presentar, como también el

aprovechamiento por la falta de prevención por parte de cada uno de los propietarios de los activos de información.

Estos individuos reciben el nombre hoy en día; derivado claro está del perfil que presentan:

- **Hacker:** Persona que vive para aprender y todo para él es un reto, es curioso y paciente, no se mete en el sistema para borrarlo o para vender lo que consiga, quiere aprender y satisfacer su curiosidad. Crea más no destruye.
- **Cracker:** Es un hacker cuyas intenciones van más allá de la investigación, es una persona que tiene fines maliciosos, demuestran sus habilidades de forma equivocada o simplemente hacen daño sólo por diversión.
- **Phreakers:** Personas con un amplio conocimiento en telefonía, aprovechan los errores de seguridad de las compañías telefónicas para realizar llamadas gratuitas.

Adicionalmente es importante mencionar que no se necesita ser un hacker para realizar alguna acción maliciosa a los sistemas de información; muchas veces un individuo puede realizar una acción indebida por diversión, por desconocimiento, entre otros. De igual manera, se debe recordar que el talón de Aquiles y uno de los más importantes de las empresas es su propio personal, este factor de amenaza, por mucho tiempo ha sido uno de los más reconocidos dentro los términos de Gestión de Riesgos, siempre se han caracterizado por generar altos niveles de probabilidad para la materialización de los riesgos y en este aspecto de la Seguridad de la Información no ha sido indiferente, definitivamente es tema de concientización, este es uno de los puntos más neurálgicos en la consecución de los buenos resultados que cualquier plan de seguridad de la información debe tener; esto en relación a que cada persona, es casi siempre el

punto más débil, por la naturaleza misma del ser humano. Una de las principales vulnerabilidades actuales, se relaciona con la ingeniería social, proceso el cual consiste, en convencer a las personas para que divulguen información confidencial. Generalmente se basa en engaños o suplantación de identidad, así como en aparentar tener una autoridad que no es real, de manera que la víctima quede en una situación desprotegida, de la cual no es consciente, y se convierte en ayuda para el atacante; es un proceso muy efectivo, que solo puede ser reducido con entrenamiento y concientización adecuados; es por ello que han surgido nuevos sistemas de ataque, en la mayoría de las veces generado por las personas, a continuación se describen algunos de ellos:

- **Ingeniería social:** Un atacante utiliza la interacción humana o habilidad social para obtener información comprometedora acerca de una organización, de una persona o de un sistema de cómputo. El atacante hace todo lo posible para hacerse pasar por una persona modesta y respetable, por ejemplo, pretende ser un nuevo empleado, un técnico de reparación, un investigador, etc.
- **Ingeniería social inversa:** El atacante demuestra de alguna manera que es capaz de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto, aprovechando la oportunidad para pedir la información necesaria y así solucionar el problema tanto del usuario como el propio.
- **Trashing (cartoneo):** Generalmente, un usuario anota su login y pasword en un papelito y luego, cuando lo recuerda, lo arroja a la basura. El trashing puede ser físico (como el que se

describió) o lógico, como analizar buffers de impresora y memoria bloques de discos, entre otros.

- **Terroristas:** No se debe de entender a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.
- **Robo:** La información contenida en los equipos de cómputo puede copiarse fácilmente, al igual que los discos magnéticos y el software.
- **Intrusos remunerados:** Es el grupo de atacantes de un sistema más peligroso, aunque es el menos habitual en las redes normales ya que suele afectar más a las grandes empresas u organismos de defensa. Se trata de personas con gran experiencia en problemas de seguridad y con un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos o simplemente dañar la imagen de la entidad afectada.
- **Personal interno:** Son las amenazas al sistema, provenientes del personal del propio sistema informático, rara vez es tomado en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Este tipo de ataque puede ser causado de manera intencional o sin dolo.
- **Ex–Empleados:** Se trata de personas descontentas con la organización que aprovechan las debilidades de un sistema que conocen perfectamente, para dañarlo como venganza por algún hecho que consideran injusto.
- **Curiosos:** Personas con un alto interés en las nuevas tecnologías, pero no cuentan con la suficiente experiencia para ser considerados como hackers o crackers.
- **Personal interno:** Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta, porque se supone un ámbito de

confianza muchas veces inexistente. Estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también son de tipo intencional. Por ejemplo: un electricista puede ser más dañino que el más peligroso de los delincuentes informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema.

Dentro de este tipo de ataque, existen otro tipo de ataques los cuales tienen que ver con los sistemas y se han clasificado de la siguiente manera:

- **Ataques de Autenticación:** Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y Pasword. Algunos de estos ataques son: Spoofing-Looping (los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing), IP Splicing-Hijacking, Spoofing (Existen los IP Spoofing, DNS spoofing y Web Spoofing), Net Flooding.
- **Ataques de Monitorización:** Se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro. Se presentan como: Shoulder Surfing, Decoy (Señuelos), Scanning (búsqueda), Snooping-Downloading, TCP Connect Scanning, TCP SYN Scanning.
- **Uso de Diccionarios:** Son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmo utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente

obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada.

- **Denial of Service (DoS):** Los ataques de denegación de servicio tienen como objetivo saturar los recursos de la víctima, de forma tal que se inhabilitan los servicios brindados por la misma. Ejemplos: Jamming o Flooding, Syn Flood, Connection Flood, Net Flood, Land Attack, Smurf o Broadcast storm, Supernuke o Winnuke, Teardrop I y II, Newtear-Bonk-Boink, E-mail bombing-Spamming.

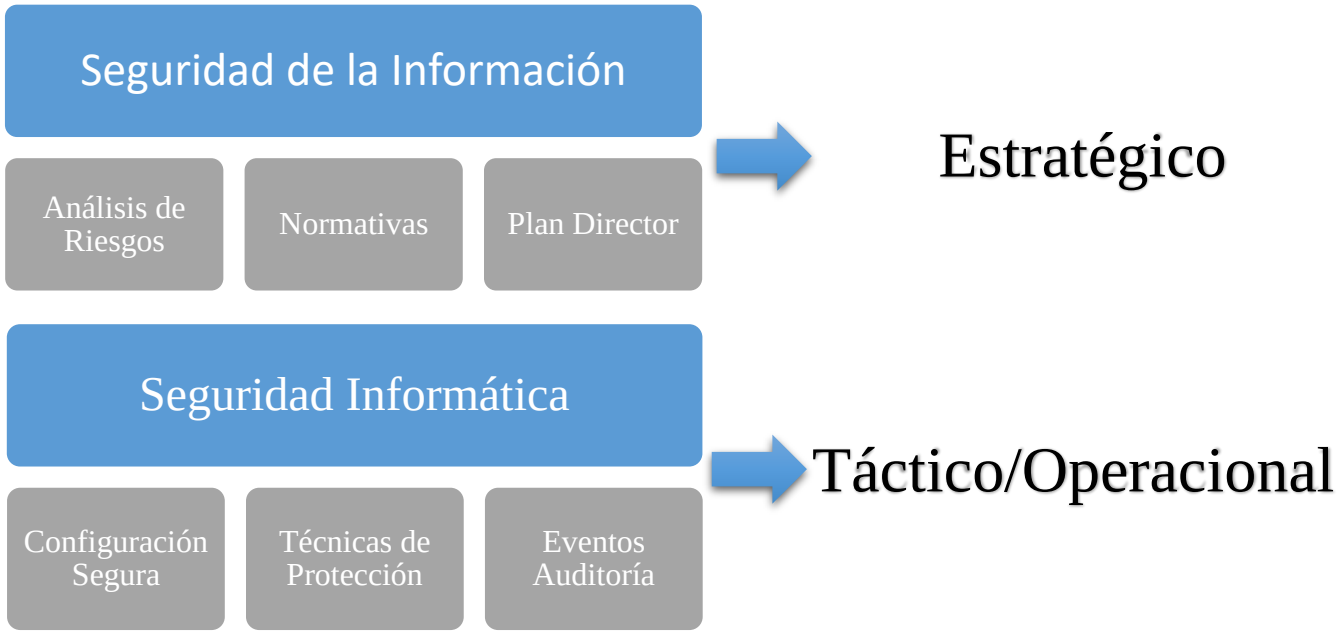
Adicional a lo anterior, es importante tener claridad sobre los conceptos relacionados con la Seguridad de la Información y Seguridad Informática, esto con el fin, que, al avanzar en el desarrollo del ensayo, exista claridad en que nivel se ubicara la falta de conciencia en la seguridad de la información.

Los conceptos de Seguridad de la Información y la Seguridad Informática, pueden parecer lo mismo; sobre todo, si se tiene en cuenta que el desarrollo y la evolución de la tecnología tiende hacia el modelo de digitalizar y manejar cualquier tipo de información mediante un sistema informático. Sin embargo, es importante tener en cuenta que cada una de las áreas de seguridad (información e informática) tiene objetivos y actividades diferentes.

La seguridad de la información es la línea estratégica de la seguridad, de igual manera se define como la disciplina que se encarga de la implementación técnica de la protección de la información y la seguridad informática se describe como la distinción táctica y operacional de la seguridad.

De igual manera es importante tener en cuenta, que la seguridad de la información también se define como la disciplina que nos habla de los riesgos, las amenazas, los análisis de escenarios, las buenas prácticas y los esquemas normativos, los cuales exigen niveles de aseguramiento en los procesos y la tecnología, eso con el fin de elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información.

Por otra parte, es importante brindar claridad en que la Seguridad de la Información también se conoce como la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, traza el plan de acción y se adecua para minimizar los riesgos con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos.



La seguridad de la información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para conseguir el objetivo se apoya a la seguridad informática, es decir, a pesar de ser disciplinas diferentes, la una no puede ir sin la otra. De forma que la seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información, las medidas técnicas serán llevadas a cabo por el equipo de seguridad informática

La seguridad de la información normalmente se apoya en la política de seguridad, que se desarrolla mediante la elaboración de un plan estratégico de seguridad, la dirección será la encargada de marcar todas las líneas de actuación en materia de seguridad y determinar las medidas tanto técnicas como procedimentales que garantice los objetivos marcados por la política de seguridad.

Las medidas técnicas se llevarán a cabo por el equipo de seguridad informática, quienes son los administradores de sistemas y seguridad.

Con el fin de tener mejor contexto a continuación se describen más características de ambos conceptos, por una parte, la seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene, es decir, que se trata de implementar medidas técnicas que preservaran las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa.

La seguridad de la información va mucho más allá, puesto que intenta proveer de medidas de seguridad a otros medios donde se localiza la información, adicional mejora los procesos de negocio, de igual manera añadir a las medidas técnicas, otras organizativas o legales que permitan a la organización asegurarse una mayor solidez de la confidencialidad, integridad y disponibilidad de los sistemas de información.

La seguridad de la información integra toda la información independientemente del medio en el que esté. La seguridad informática atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales.

Con base en todo lo anterior, es recomendable que las empresas realicen análisis de riesgos detallado de las vulnerabilidades a las que están expuestos, como las físicas, de software, humanas, entre otros, para evitar en la medida de lo posible ser puntos blancos de ataque. Es muy importante ser consciente de que por más que las empresas sean las más seguras desde el punto de vista de ataques externos, Hackers, virus, entre otros, la seguridad de esta sería nula si no se ha previsto como combatir un incendio. Por ello se hace mucho hincapié sobre la importancia de la seguridad informática, ya que se está invirtiendo para proteger el objeto más valioso de cualquier empresa, que es la información.

Planteamiento del Problema

La ausencia de una cultura de seguridad de la información en las organizaciones o inclusive a nivel personal, permite a los ciberdelincuentes explotar esta vulnerabilidad mediante técnicas que buscan confundir y crear confianza en la victima para lograr el objetivo buscado por el ciberdelincuente.

Objetivo General

Establecer Planes y mecanismos para la Toma de conciencia que contribuyan con la Formación y el Desarrollo del Personal del Sector de la Seguridad Privada en Temas relacionados con la Seguridad de la Información y Seguridad Informática

Objetivo Específicos:

1. Identificar las principales amenazas que se presentan en la Seguridad de la Información, en la que se involucran personas y el efecto en las mismas.
2. Identificar patrones de comportamiento, en los que las personas son fácilmente manipuladas y se vuelven vulnerables frente a las amenazas de delitos cibernéticos.
3. Identificar desde la Ingeniería social, técnicas de persuasión inversa, es decir que contribuyan en la toma de conciencia del personal frente a la Seguridad de la Información en las Organizaciones.

Seguridad Privada

La seguridad es un estado que toda persona busca en su convivencia con el entorno y sociedad que le rodea. El ciudadano busca poder vivir y convivir con tranquilidad y con garantías de que su entorno más cercano (familia) y su propiedad no sea atacada o violentada. Una gran parte de esta seguridad nos la da la administración a través de los cuerpos y fuerzas de seguridad del Estado.

Pero la seguridad total sabemos que es imposible que la podamos tener, una sociedad con inseguridad "cero", por desgracia, es imposible que exista. Como se suele decir, no podemos tener un policía en cada esquina y por lo tanto siempre existe la probabilidad de que podamos ser víctimas de algún tipo de delito. Es aquí donde entra en escena la seguridad privada.

La Seguridad Privada hace referencia a los servicios que prestan las empresas de seguridad, con objeto de proteger el conjunto de bienes y derechos para los que han sido contratadas. Estos intereses protegidos suelen ser de naturaleza privada: edificios, almacenes, hogares, terrenos, etc, e igualmente de naturaleza pública o mixta.

Dentro de los servicios que se contratan con la seguridad privada se encuentran entre otros: la protección de mercancías e inmuebles, así como de sus ocupantes y el control de acceso a los mismos, son ejecutados por los guardas de seguridad; investigaciones administrativas relacionadas con intereses privados en ocasiones incluyen personas y/o empresas, estas actividades son ejecutadas por personal experto; otro de los servicios son la protección de personas y/o carga critica, normalmente estas actividades son ejecutadas por personal

debidamente entrenado y certificado en el cargo de escoltas por último encontramos la instalación y explotación de sistemas que protejan dichos intereses como alarmas de seguridad o sistemas de vigilancia.

Para la prestación de estos servicios es necesario que el ente regulador de este sector de Vigilancia y Seguridad Privada en Colombia, La Superintendencia de Vigilancia y Seguridad Privada, otorgue la licencia correspondiente para prestar los servicios mencionados anteriormente, adicional a esto, los trabajadores y/o terceros que ejecuten labores en nombre de la empresa deben contar con las certificaciones exigidas en cuanto a formación.

Puede existir la idea equivocada que la contratación de la seguridad privada solo es un servicio privilegiado para aquellos que tienen una mejor posición económica, pero es un concepto equivocado. Si es verdad que hay personas que por su posición social y/o económica contratan un servicio de seguridad privada más personalizado y más completo; pero hay que recordar que este servicio está contratado, no va en detrimento de la seguridad del resto de la sociedad. Pero no sólo este perfil de personas son los usuarios de la seguridad privada, si hacemos un listado rápido de los servicios que realizan vemos que la seguridad privada está más cerca de nuestra realidad de lo que pensamos:

- Alarmas y/o cámaras en casas y viviendas particulares;
- Alarmas y/o cámaras en pequeños comercios;
- Alarmas, cámaras y guardas de seguridad en grandes superficies comerciales;
- Cámaras y guardas de seguridad en equipamientos y eventos deportivos;

- Guardas de seguridad en todo tipo de celebración: conciertos, fiestas populares, actos públicos, etc.

- Cámaras y guardas de seguridad en muchos edificios públicos de todas las administraciones;

- Alarmas, cámaras y guardas de seguridad en muchos edificios y zonas privadas, ya sean de empresas, sectores industriales, oficinas de negocios o bloques o urbanizaciones de viviendas particulares, puertos y aeropuertos.

- Cámaras y guardas de seguridad en instalaciones de transporte público como en el metro o en las instalaciones del tren.

- En situaciones de alto riesgo, pueden ser un complemento de las fuerzas y cuerpos de seguridad. Por ejemplo, en una final de un campeonato de fútbol, mientras la policía vela para que el dispositivo de seguridad de buen resultado, por la seguridad del entorno y vigila la zona; los vigilantes de seguridad pueden hacer el control de accesos al recinto deportivo;

- Transporte seguro de dinero y artículos de gran valor; entre otros.

La seguridad privada es un sector necesario y con mucho futuro precisamente por los retos que el futuro visualiza y que nuestra sociedad tiene que afrontar, la delincuencia cada vez está más organizada, está más globalizada y actúa de forma más sofisticada.

Podemos afirmar que todos los cuerpos seguridad públicos y privados, colaboran para proteger y garantizar nuestros derechos y libertades como ciudadanos, así como la protección de bienes y personas, no obstante la capacidad instalada de las fuerzas en Colombia nunca será suficiente, es por eso que se deberá continuar con las diferentes alianzas de seguridad entre sector de la Seguridad Privada y la Fuerza Pública con el fin de garantizar la Seguridad de los Ciudadanos Colombianos y por ende demostrar a nivel internacional, que pese a las dificultades que actualmente se viven en el país, continuaremos esforzándonos para seguir construyendo un país seguro.

Como referente se citan algunas cifras para tener en cuenta con relación a la Seguridad Privada en Colombia; estamos hablando que, en la actualidad, este sector factura anualmente alrededor 8,6 billones de pesos, hay alrededor de 1.000 empresas constituidas en Colombia, alrededor de 235.000 hombres, se manejan aproximadamente 90.000 armas; esto nos permite ser un referente de seguridad a nivel de Latinoamericano.

Toma de Conciencia:

El concepto de Conciencia visto desde la psicología, es la cualidad o el estado de conocimiento de objetos externos o de algo interno a uno mismo. En un sentido más básico, es la experimentación bruta de cualquier sensación, incluso en ausencia de significado o conceptualización sobre la relación entre el sujeto y las cosas. Puede ser definida como: subjetividad, punto de vista en primera persona, capacidad para sentir, cómo se siente ser algo o lo que produce significado. Se ha dicho que la consciencia es

constitutiva de todo estado mental (conjunto de capacidades cognitivas (mentales) que engloban procesos como la percepción, el pensamiento, la conciencia, la memoria, imaginación, etc., algunas de las cuales son características del humano y otras son compartidas con otras formas de vida), a diferencia de la intencionalidad.

A pesar de la dificultad al definirla y estudiarla, algunos filósofos consideran que hay una intuición generalizada sobre lo que es, y que une a todas las definiciones anteriores. Esta intuición se puede compartir con gran eficacia apelando a la diferencia entre dormir (sin sueños) y el estado de vigilia: cuando la conciencia se desvanece es como si toda posible realidad se esfumara, desde el punto de vista del sujeto.

La conciencia no debe ser confundida con la vida, el razonamiento, la inteligencia o la memoria. Para muchos de sus estudiosos tampoco es equivalente a la atención12 ni a la percepción; aunque están íntimamente relacionadas.

Estados de Conciencia:

Conciencia individual: se refiere a la conciencia de uno mismo y de cómo el entorno lo puede perjudicar o favorecer. Se establece lo que es bueno y malo para uno mismo. El ejercicio acertado de esta función mental se llama instinto de supervivencia. En el hombre, el resultado de su racionalización le dota de mayor capacidad de autodominarse.

Conciencia social: se refiere a la conciencia del estado de los demás miembros de su comunidad y de cómo el entorno los puede perjudicar o favorecer. Se establece lo que es bueno y malo para una comunidad. El ejercicio acertado de esta función mental se

llama instinto de protección. En el hombre, el resultado de su racionalización le dota de capacidad cooperacional, y de esto nace la Inteligencia social.

Conciencia temporal o competente: se refiere a la conciencia del medio que le rodea y de cómo afecta a uno mismo y a los demás en la línea del tiempo. Se establece lo que es bueno y malo para el futuro de la comunidad. El ejercicio acertado de esta función mental se llama inteligencia racional.

Conciencia emocional o empatía: Se establece lo que es bueno y malo en función de datos emocionales, y de cómo el entorno y la forma de actuar de uno mismo, afecta al estado emocional de su comunidad. El ejercicio acertado de esta función mental se llama inteligencia emocional.

La conciencia puede funcionar en 'piloto automático', es decir, sin necesidad de ejercitar inteligencia alguna, únicamente basándose en los instintos. El individuo es consciente de lo que está haciendo, pero no se plantea si es bueno o malo.

Las tres primeras no son exclusivas del hombre, sólo la última. Como especie animal no nos cuesta concienciarnos de las dos primeras, pues no depende de la educación o datos externos, va con la propia naturaleza de la conservación de la especie. El ejercicio más o menos acertado de la tercera dependerá de la educación recibida (los hay autodidactas), también es innata a la supervivencia y la cuarta no todo humano logra concienciarse en su mayor exponente (o sea, equipararla al uso que le damos a las otras tres), sino que son

dependientes de la educación, costumbres y moral local. No suele manifestarse de forma consciente, sino como una imagen de lo que podríamos estar sintiendo nosotros en piel ajena. Ello motiva a actuar pensando que eso es lo bueno y lo malo, sin cuestionarlo ni racionalizarlo; las personas que lo han intentado han acabado convirtiéndose en líderes.

¿Qué es tomar conciencia?:

Con el tiempo nos damos cuenta de que repetimos patrones en las relaciones, en el trabajo o en cualquier otro ámbito y no sabemos por qué. Tomar conciencia es comprender los aparentes sinsentidos de la vida.

Más de una vez nos hemos visto atrapados en situaciones que nos parece haber vivido antes. Sin embargo, las repetimos. Es como si hubiera un mecanismo interno que nos lleva a vivir en un bucle, haciendo las mismas cosas, generando los mismos pensamientos. No nos sirve de nada saber que no nos beneficia o, al contrario, tenemos un familiar o un amigo atrapado en una situación en la que le vemos sufrir y le insistimos en que resuelva de alguna manera porque nos cuesta soportar verle en una circunstancia que nos parece perjudicial. En ambos casos, tanto si nos pasa a nosotros como si les pasa a otros, encontramos a algo o a alguien para atribuirle la culpa. Creemos que lo que nos molesta está fuera de nosotros.

Nuestras experiencias no son casuales, no estamos mal de la cabeza por hacer cosas ilógicas e irracionales.

Las situaciones que vivimos están directamente relacionadas con situaciones que ya hemos vivido en algún momento anterior de nuestra vida y con situaciones que vivió alguno de nuestros ancestros. Estamos procesando una información que es propia de nuestro clan. Es como si sintiéramos el mismo sufrimiento que nuestros antepasados en algún momento en el que temieron por su supervivencia cuando, en realidad, nosotros no estamos en una situación que ponga en peligro nuestra vida. Vivimos la misma emoción en un escenario distinto.

Tomar conciencia es hacer emerger esa información que está en nuestro interior y comprender que estamos viviendo igual que lo hacían nuestros padres y nuestros abuelos. A pesar de que nuestra circunstancia es diferente resolvemos las situaciones de la misma manera.

Cuando comprendemos dejamos de posicionarnos, perdonamos, nos liberamos del victimismo y alcanzamos una madurez emocional.

Comprender no es lo mismo que entender. Comprender es una sensación que va más allá de lo racional, es dar sentido a algo, aparentemente, ilógico.

Al tomar conciencia comprendemos para qué vivimos lo que vivimos. Lo único que tenemos que hacer es aprender que las situaciones que vivimos en nuestra vida son una oportunidad para crecer en nuestra experiencia de vida. Al tomar conciencia dejamos de

pensar y empezamos a hacer. Comprender lo que no tiene explicación nos da paz y esa paz contribuye de forma muy clara a nuestro bienestar emocional.

"Para ser diferentes de lo que somos, debemos tener cierta conciencia de lo que somos."

Eric Hoffer

Antes de continuar, es muy importante hacer un alto en el camino para reflexionar sobre los conceptos desarrollados (Seguridad Privada en Colombia y Toma de Conciencia) y como estos se articulan, para iniciar con la descripción de las principales amenazas que se presentan en la Seguridad de la Información.

Si bien es cierto y como se mencionó anteriormente, la Seguridad Privada hace referencia a Servicios que se prestan para la protección de personas, bienes e instalaciones apoyado en equipos tecnológicos que un gran porcentaje es administrado de igual manera por personal entrenado y capacitado para tal fin; es entonces a partir de este momento donde adquiere mayor importancia la toma de conciencia por parte de todo el personal que interviene en la planificación e implementación de la operación de seguridad privada, sin perder de vista que el nivel transaccional que se lleva a cabo para la generación y/o administración de la información es no solamente alta sino también critica. Pensemos en el siguiente escenario: Una compañía del Sector Industrial, líder en el mercado de Alimentos y que de acuerdo al resultado en el Análisis de Riesgos, se diseño e implemento un esquema de seguridad integral, compuesto por Personas, Equipos y Procedimientos, todos articulados e inmersos en la Cadena de Valor del Cliente, dicho en otras palabras, cuentan

con Circuito Cerrado de Televisión operado desde una Central de Monitoreo y la cual es administrada por personal de la compañía de seguridad, de igual manera el esquema de seguridad cuenta con guardas de seguridad ubicados en los muelles de exportación, controles de acceso, recibo y despacho de mercancía, entre otros puestos de control. Adicionalmente tiene personal de seguridad, asignado al rol de Auditorias de Seguridad, este escenario nos lleva a pensar al alto volumen de información que se genera producto de la operación y como esta siendo protegida y/o custodiada con el fin de garantizar la integridad, disponibilidad y confidencialidad de la misma. Esto esta soportado claro está por cada una de las Políticas y Directrices emanadas por el área de seguridad del cliente en coordinación con la empresa de vigilancia y seguridad privada que administra el contrato.

A partir de lo anterior, es donde se genera la necesidad sobre la toma de conciencia por el personal tanto operativo como administrativo de la Empresa de Vigilancia y Seguridad Privada para el manejo de la información generada en y por cada uno de los activos de información donde las personas asignadas a ese gran dispositivo de seguridad integral tienen relación bien sea de manera directa o indirecta.

A continuación, se detallan las principales amenazas de Seguridad de la Información, que en la actualidad se están presentando.

Principales amenazas que se presentan en la Seguridad de la Información:

A pesar de las lecciones que ha dejado el mundo corporativo en los últimos años en cuanto a las vulnerabilidades que implica estar conectados, un reporte de la consultora EY que consultó a 1.400 líderes de riesgo y seguridad cibernética de algunas de las organizaciones más grandes del planeta, reflejó que el 80% de las juntas directivas no hacen de la ***Ciberseguridad (práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica)***, un tema estratégico para sus compañías.

El 89% de los ejecutivos consideran que las medidas de Ciberseguridad implantadas en su compañía no son suficientes, esto obedece a varias causas; 59% restricciones de presupuesto, 58% falta de recursos especializados y 29% falta de concienciación y apoyo de la junta directiva; con relación a si se están tomando medida, los resultados que arroja el estudio es: 59% afirma que su presupuesto de ciberprotección ha aumentado en el último año, 56% ha cambiado su estrategia y planificación para evitar ciberataques, sin embargo es muy importante tener en cuenta que aún hay demasiadas cosas por hacer, 57% no cuentan con un programa formal de ciberseguridad, 48% no dispone de un centro de operaciones de seguridad (SOC), 75% afirma que sus sistemas no cuentan con la madurez suficiente y 12% reconoce no haber implantado ningún sistema de detección de amenazas.

Las empresas deben asumir que lo peor también les puede suceder. Los numerosos ejemplos de ciberataques a escala mundial obligan a tomar las medidas necesarias de prevención y de protección.

La ciberseguridad debe ser una prioridad a todos los niveles de las empresas. Más aun teniendo en cuenta que en el actual entorno, complejo y cambiante, las ciberamenazas se mantienen ocultas a nuestros ojos.

La mayoría de las empresas considera que el riesgo de sufrir un ciberataque es hoy mayor, que hace un año, ya que las técnicas de los ciberdelincuentes son más sofisticadas y las empresas están más hiperconectadas que nunca. Las oportunidades que ofrece la digitalización son muy grandes a lo largo de la cadena de valor y con ello el incremento de los riesgos.

No es posible repeler todas las amenazas, pero las empresas resilientes son aquellas que saben protegerse, detectan el problema y reaccionan de forma efectiva. Las estrategias activas de defensa y los mecanismos de inteligencia avanzada proporcionan una base para resistir a los nuevos ciberataques, mientras que conceptos como la seguridad desde el diseño (security by design) dan a las compañías opciones en la batalla por un mundo más seguro.

Para el año 2021 se estima un costo global en ciberseguridad de seis billones de dólares para el doble del registrado en 2015, este costo para las organizaciones es tanto

económico como reputacional, siendo este último uno de los intangibles más valiosos de las Empresas de Hoy.

En la actualidad, prácticamente todas las empresas son digitales por defecto y, según los últimos estudios del Foro Económico Mundial, la brecha de la ciberseguridad supone uno de los cinco mayores riesgos que afronta el mundo.

Nunca ha sido tan difícil para las compañías trazar un mapa del entorno digital en el que operan y sus interacciones con el mismo, producto del desarrollo tecnológico, la proliferación de dispositivos y la aparición del denominado Internet de las Cosas, por lo que tienen que acostumbrarse a desplegar sus tentáculos en todas las direcciones.

Las empresas que comprenden el panorama de ciberamenazas al que se enfrentan y que cuentan con defensas fuertes tendrán más posibilidades de repeler los ataques e identificar a los ciberdelincuentes.

Las empresas deben asumir que lo peor puede suceder, y hay suficientes ejemplos de ciberataques a escala mundial (los virus Petya, Wannacry o Mirai, por ejemplo).

Entre las **vulnerabilidades** de ciberseguridad que más preocupan a los encuestados del estudio, destacan las que involucran a **empleados desprevenidos o descuidados** (60% de la muestra) y las que utilizan **mecanismos obsoletos de control** de seguridad de la información (46%).

Los **ataques tipo** *malware* **y** *phishing* son las dos principales **amenazas** identificadas por los encuestados, ambas seleccionadas por el 64%.

Protección frente a las amenazas:

Ataques Comunes

Realizados por agresores poco sofisticados (empleados descontentos, competidores, hacktivistas, algunos grupos criminales…) que explotan vulnerabilidades conocidas y que se basan en herramientas de hacking habituales.

Defensa: Las empresas deben cerrar la puerta a los tipos de ciberataques más comunes, utilizando las herramientas conocidas (software antivirus, sistemas de detección y prevención de intrusiones, cifrado de datos, etc.) para frenar el porcentaje más alto de los ataques.

Además, los empleados deben tomar conciencia de la importancia de su contribución en avanzar en la ciberseguridad, con actuaciones básicas como la gestión de sus contraseñas.

Ataques Avanzados

Son realizados por hackers sofisticados (grupos criminales organizados, equipos de espionaje industrial, ciberterroristas y hasta naciones) que se dirigen hacia vulnerabilidades complejas y, en ocasiones, desconocidas (“zero day”) con herramientas avanzadas.

Defensa: La implantación de un **Centro de Operaciones de Seguridad** (SOC, por sus siglas en inglés) que centralice todas las medidas de ciberseguridad. A pesar de su importancia, el 48% de los encuestados en el estudio no dispone de un SOC y sólo el 12% de la muestra afirma que es muy probable que su empresa detecte un ciberataque sofisticado.

Ataques Emergentes

Se realizan también por hackers sofisticados (como sucede en el caso de los avanzados) y se dirigen hacia nuevas vulnerabilidades surgidas por la aplicación de las tecnologías emergentes tras un proceso de investigación específico.

Defensa: Las empresas no pueden anticipar todas las ciberamenzas, pero las organizaciones innovadoras deben trabajar en anticipar la naturaleza de las amenazas potenciales futuras y reaccionar rápidamente cuando aparezcan.

Las empresas deben actuar con calma, con un plan de respuesta probando con antelación y en el cual cada uno conoce sus responsabilidades

Claves para una efectiva aplicación de la Ciberseguridad:

Ser Estratégico e Innovador

Enfocarse en los Riesgos

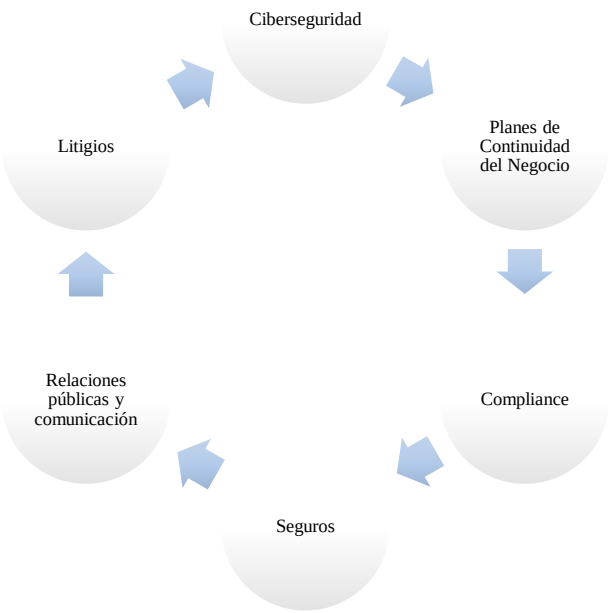
Centrarse en el Talento

Ser resiliente y escalable

Operar de forma inteligente y ágil

Gestión de Crisis: plan de respuesta ante un incidente de seguridad

Las empresas deben contar con un Plan de Respuesta ante Brechas Cibernéticas, que se active de forma automática cuando se detecta un incidente. En la práctica este es un mecanismo que contempla al menos seis aspectos claves:



Tendencias de amenazas de ciberseguridad

1. **Phishing y Fraude del CEO:** El primer hace referencia a un tipo de ingeniería social cuyo objetivo es conseguir información confidencial de manera fraudulenta (como contraseñas o información bancaria). El "Fraude del CEO", técnica que consiste en un email que los atacantes envían a empleados de la compañía suplantando la identidad del director ejecutivo. Estos ataques los sufren especialmente a quienes tienen acceso a recursos financieros y económicos de la empresa. En dicho email se informa al empleado que tiene

que llevar a cabo una transacción financiera. Actualmente es considerada una de las ciberamenazas más difundidas.

2. **Amenazas de Ciberseguridad en entornos Cloud:** Los atacantes se están aprovechando del hecho de que los equipos de seguridad tienen dificultades para defenderse de la evolución y la expansión de entornos cloud. Una razón es la falta de claridad sobre quién es exactamente el responsable de proteger esos entornos. Otros riesgos que entrañan los entornos cloud son el factor humano, es decir, usuarios que no siguen las medidas de seguridad. También son entornos de fácil entrada de terceros no autorizados y sensibles a dar problemas de disponibilidad o pérdida de información. Por ejemplo, no se realizan actualizaciones o copias de seguridad de los archivos que se encuentran en la nube, lo que los convierten en presa fácil para un ataque.
3. **Shadow IT:** TI en las sombras o Shadow IT se refiere al hardware o software dentro de una empresa que no es compatible con el departamento de TI central de la organización.

   El término lleva una connotación negativa porque implica que el departamento de TI no ha aprobado la tecnología o ni siquiera sabe que los empleados la están utilizando. Hoy en día, más del 80 % de los empleados admiten utilizar aplicaciones de TI en la sombra en el trabajo.

   La mayoría de las veces, las motivaciones de los usuarios no son maliciosas o negligentes; solo están tratando de hacer su trabajo más fácil o eficiente. Sin embargo, el uso de TI en la sombra es una seria amenaza para el cumplimiento y la ciberseguridad. Estas aplicaciones pueden tener problemas de seguridad o de cumplimiento que los usuarios desconocen y, dado que los departamentos internos de TI ni siquiera conocen las

aplicaciones, no pueden supervisar los registros de acceso, garantizar que se realicen copias de seguridad regulares o aplicar actualizaciones de software importantes.

4. **Cryptojacking:** es el uso no autorizado de ordenadores y otros dispositivos con el objetivo de **minar criptomonedas** y que en los últimos años ha crecido de manera exponencial, hasta el punto de que se ha convertido en una **amenaza** más común que el ransomware. A pesar de que es una **amenaza** de la ciberseguridad que no compromete a los datos del usuario, afecta a la **capacidad de procesamiento**, produciendo un menor rendimiento del ordenador o **dispositivo afectado**. En el caso de una empresa, esto produciría un **crecimiento** en la **partida de gastos** en asistencia técnica, así como un **daño** a la **imagen pública** de la empresa cuando se conocen los hechos.
5. **Ransomware:** La llegada de los **ransomware worms** basados en la red elimina la necesidad del elemento humano en el lanzamiento de campañas de ransomware. Y para algunos adversarios, el premio no es un **rescate**, sino la **destrucción** de sistemas y datos
6. **Ataques IoT y DDoS:** los **dispositivos IoT** (En español como "internet de las cosas") están **evolucionando** precipitadamente. Por lo que muchas organizaciones están **incorporando** dispositivos IoT a sus entornos de TI, sin prestar la atención necesaria a la seguridad de estos sistemas. Los **ataques a IoT** permiten propagar una amplia gama de ataques. Por ejemplo, solo en julio de 2018 se vieron afectadas un **45 % de las empresas por ataques dirigidos a IoT.** Por otro lado, nos encontramos con los ataques de **denegación de servicio (DDoS)**. Consiste en el intento por parte de atacantes maliciosos de interrumpir el **tráfico** normal de un servidor o red de destino lanzando

múltiples peticiones hacia el mismo recurso. Los recursos atacados pueden incluir ordenadores y otros dispositivos en red como los mencionados IoT.

7. **Ataques a los sistemas de tecnología operativa (OT):** Las **redes de tecnología operativa** (OT) desempeñan un papel fundamental en la **fabricación**, la defensa, los servicios de emergencia, la alimentación y la agricultura solo por mencionar algunos. Las redes y dispositivos OT incluyen **sistemas de control de supervisión** y adquisición de datos (SCADA) y sistemas de control industrial (ICS). Los ciberataques a la tecnología operativa (OT) **pueden producir paralizaciones en las operaciones comerciales**. Estos ataques presentan amenazas para la salud y la vida de los empleados y del público en general, y su frecuencia va en aumento. Los sistemas de tecnología operativa se enfrentan a **vulnerabilidades** y amenazas a la ciberseguridad de la empresa. Estas amenazas son muy diferentes de las que amenazan a los sistemas de tecnología de la información, por lo que suponen un reto para la ciberseguridad.
8. **Troyanos bancarios en aplicaciones móviles:** Los **troyanos bancarios** son una de las amenazas más peligrosas dentro del *malware*. Los usuarios descargan los troyanos bancarios a través de **aplicaciones móviles.** En la mayoría de los casos, los ciberdelincuentes hacen pasar por aplicaciones móviles legitimas para **engañar** a los usuarios. Este tipo de troyanos son cada vez más frecuente y se estima que siga aumentado para el próximo año.

Patrones de Comportamiento de Personas fácilmente manipulables:

El Factor Humano muchas veces podía llegar a contraseñas y otras piezas de información sensible de su empresa fingiendo ser otra persona y sólo pedirla. Es natural que se anhela una sensación de seguridad absoluta, lo que lleva a muchas personas a resolver por un falso sentido de seguridad. El factor humano es realmente el eslabón más débil de seguridad. La seguridad es a menudo más que una ilusión, una ilusión a veces incluso peores cuando la credulidad, ingenuidad, ignorancia entran en juego. La mayor parte del mundo respetado científico del siglo XX, Albert Einstein, es citado diciendo, "Sólo dos cosas son infinitas, el universo y la estupidez humana, y no estoy seguro sobre el primero. "Al final, los ataques de ingeniería social pueden tener éxito cuando la gente son tontos o, más comúnmente, simplemente ignorantes acerca de buenas prácticas de seguridad.

La seguridad no es un producto, es parte de un proceso, por otra parte, la seguridad no es un problema de la tecnología - es un pueblo y gestión de problemas. Descifrando el firewall humano es a menudo fácil, no requiere ninguna inversión más allá del costo de una llamada telefónica, e implica un riesgo mínimo.

¿Cuál es la mayor amenaza para la seguridad de los activos de su empresa? Eso es fácil: la ingeniería social - un mago sin escrúpulos que tiene que ver con la mano izquierda mientras con la derecha roba sus secretos. Este personaje es a menudo tan amable, locuaz, y obliga a que se siente agradecido por haberlo encontrado.

En la mayoría de los casos, el éxito de los ingenieros sociales tiene fuertes habilidades de la gente. Es encantador, amable y fácil como los rasgos sociales necesarios para el establecimiento de una rápida, relación de confianza. Un ingeniero social experimentado es capaz de acceder a prácticamente cualquier información específica mediante el uso de las estrategias y tácticas de su oficio. Técnicos ingeniosos han desarrollado cuidadosamente seguridad de la información, las soluciones para minimizar los riesgos relacionados con el uso de las computadoras, sin embargo, no se abordan la vulnerabilidad más importante, el factor humano. A pesar de nuestro intelecto, que los seres humanos - usted, yo, y todos los demás - siguen siendo la amenaza más grave a cada otro de seguridad.

La ingeniería social, es el arte del engaño, hace referencia al arte de manipular persona para eludir los sistemas de seguridad, consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Se puede decir casi con total seguridad que el perfil de las víctimas de delitos informáticas es casi la totalidad de la población, que con su conducta favorece en el 99% de los casos que sea víctima.

Al igual que en otros tipos de delito la víctima puede tener una posición neutral, en la que ni favorece ni perjudica la conducta del criminal, en los delitos informáticos es esencial la posición que tiene la víctima y la conducta preventiva o proteccionista que esta tiene para evitar ser atacada y perjudicada por el agresor.

El sujeto pasivo, en el caso de los delitos informáticos pueden ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. Víctima puede ser cualquier persona física o jurídica que haya establecido una conexión a Internet (ya que es la principal ventana de entrada para estas conductas), una conexión entre computadoras, o que en definitiva cuenta con un sistema informático para el tratamiento de sus datos.

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del *modus operandi*, esto es de las maniobras usadas por los delincuentes informáticos.

Las víctimas de delitos informáticos no adoptan precauciones técnicas mínimas para evitar tales agresiones. Además, una vez afectadas, las víctimas no presentan denuncias ni persisten en sus pretensiones durante el procedimiento correspondiente. A veces ni siquiera son conscientes de que son víctimas de un delito informático. Otras no se quiere aceptar el rol de víctima por miedo o vergüenza, por el perjuicio a su imagen pública que ello pueda tener.

Aunque las principales víctimas de este tipo de delitos son empresas y profesionales que trabajan con datos sensibles o información confidencial, las personas particulares también lo son.

Técnicas de Persuasión Inversa que contribuyen en la Toma de Conciencia del personal frente a la seguridad de la información:

La persuasión técnicamente no lava el cerebro, pero es la manipulación de la mente humana por otro individuo, sin que el partido manipulado esté consciente de que causó su cambio de opinión. La base de la persuasión sirve siempre para tener acceso a la mitad derecha de su cerebro.

La mitad izquierda del cerebro es analítica y racional. El lado derecho es creativo e imaginativo, la idea es distraer el cerebro izquierdo y mantenerlo ocupado.

La persuasión consiste en la utilización deliberada de la comunicación para cambiar, formar o reforzar las actitudes de las personas, siendo estas últimas representaciones mentales que resumen lo que opinamos de las cosas, personas, grupos, acciones o ideas: si preferimos una marca a otra, si estamos a favor o en contra del aborto, qué opinamos de determinados partidos políticos, etc.

Debido a que las actitudes juegan un papel importante en la forma de comportarse, un cambio en ellas debería dar lugar a un cambio en nuestro comportamiento, que es lo que, en última instancia, se pretende con la persuasión

Los estudios actuales sobre la persuasión dan una importancia crucial a la fuente de la que parte la acción persuasiva. La fuente debe ser creíble para que el mensaje tenga efecto. Un mensaje es competente si el mensaje es emitido de tal manera que el receptor se ve obligado a procesarlo y tomarlo en cuenta.

Un mensaje es persuasivo si el mensaje moviliza emociones o cogniciones capaces de transformar una actitud. Muchas veces un mensaje es persuasivo, pero poco competente.

Un mensaje es apropiado si por su formato, por quién emite el mensaje, canal escogido y otras características, puede obtener los resultados apetecidos. Este concepto es muy global pues se refiere a sí en la vida real el mensaje ha logrado o no su propósito. La pregunta clave para saber si un mensaje es apropiado sería: ¿Es o fue eficaz para cambiar conductas? Como es lógico, tanto más será un mensaje apropiado cuanto más legítimo, competente y persuasivo. El buen comunicador sabe sacrificarse él mismo como emisor de mensajes cuando detecta que otra persona o grupo de personas pueden ser más persuasivas. ¡Persuadir no debe confundirse con ejercer un liderazgo carismático!

Otras maneras de incrementar la credibilidad de la fuente serían:

- Aportar estadísticas, datos y testimonios incontestables.
- Invitar a un ponente de prestigio a que refuerce la línea argumental.
- Presentar adecuadamente a quien habla o emite la información. Sobre todo, interesa destacar su imparcialidad o falta de interés para decir lo que dice a favor de una opción determinada.
- La fuente de información más creíble es aquella que habla en contra de sus propios intereses. Por consiguiente, la persona más creíble suele ser aquella que a pesar de tirarse piedras sobre el tejado admite que el mejor camino a emprender es el que expone.

- Se logra mayor persuasión combinando canales. Un mismo mensaje repetido por diferentes canales activa en mayor medida la atención del receptor, sobre todo si tienen continuidad temporal.

Un mensaje será tanto más persuasivo cuanto logre mover a la persona o grupo que lo reciba hacia:

- Sentimientos de inconsistencia con su situación actual, y necesidad de cambiar en la dirección indicada por nosotros.
- Sentimientos de agradecimiento hacia el emisor de los mensajes. Por ejemplo: «Vaya suerte que tengo de haberme enterado de esta información privilegiada».
- Sentimientos de «estar en la tónica de lo que ahora mismo se lleva», y por extensión, promover expectativas de prestigio.
- Sentimientos de oportunidad.

A continuación, se describen algunos métodos de prevención frente a los Delitos Informáticos e igualmente como lograr generar concienciación al personal de las organizaciones para no ser víctimas de los Delitos Informáticos y que permitan contribuir a la Seguridad de la Información y Seguridad Informática de sus Organizaciones.

La manera más efectiva para evitar ser víctima de procedimientos de ingeniería social es no revelando información personal y confidencial:

- ✓ Estar enterados sobre los métodos de estafa más utilizados y los nuevos, esto con el fin de estar a la expectativa sobre las diferentes estrategias que se esten utilizando por parte de criminales. En el caso de las organizaciones, es importante colocar sobre aviso a la autoridad competente ante la identificación de cualquier riesgo que se identifique. Esto pasa también con personas, no solo con empresas, el mal uso de la información personal en las técnicas nuevas y antiguas de ingeniería social concluyen con la ejecución de estafas y delitos de los que cualquiera puede ser víctima.
- ✓ Generar sentido de pertenencia para implementar seguridad de manera más acertada, es una de la mejor forma de contrarrestar la ejecución de delitos informáticos a través de esta metodología de ingeniería social, la concientización de las personas debe ser primordial para el autocuidado de la información y la minimización de los riesgos en materia de seguridad.

- ✓ Capacitarse, informase y utilizar ejemplos de la vida real como método de prevención y preparación para recibir ataques, se debe crear un modo de prevención para las personas, cuando se tienen antecedentes se pueden identificar mucho más fácil si se está siendo sujeto de recibir algún ataque de este tipo.

- ✓ Fomentar la Cultura de la Seguridad de la Información, realizar campañas de protección de datos, con el fin de prevenir ataques y ayuda a las personas a ser más cuidadosa a la hora de revelar información confidencial.

- ✓ Es importante tener conocimiento sobre los temas relacionados con la ingeniería social, sus aplicaciones, sus componentes y sus afectaciones para saber a ciencia cierta al problema que la sociedad se enfrenta.

- ✓ Es importante no brindar información que tenga relación con usuarios y contraseñas de aplicaciones solicitadas a través de algún mail o de una página web. Esta información siempre será personal e intransferible, recordemos que este es el código de acceso a cualquier aplicación informática, el uso indebido de usuarios y/o contraseñas puede generar faltas graves incluso para el usuario que comparte esta información confidencial.

Descripción de un Plan de Sensibilización, Capacitación y Comunicación:

Un programa efectivo debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas de información, las cuales se encuentran plasmadas en las políticas y procedimientos de seguridad de la información que la Organización requiere que sean cumplidos por parte de los dueños de los activos de la información y todos los usuarios de los sistemas de información.

Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción al personal que genero el incumplimiento, siempre y cuando exista el registro de la

capacitación y/o formación en el tema correspondiente, teniendo en cuenta lo anterior, un plan de capacitación, sensibilización y comunicación adecuado, debe llevarse a cabo en las siguientes 4 fases:

Diseño	•Identifica las tareas a ser realizadas para cumplir con las metas de entrenamiento
Desarrollo	•Su enfoque en las fuentes de información disponible, alcance y contenidos del material de entrenaminto
Implementación	•Direcciona efectivamente la manera como deberá comunicarse el material diseñado
Mejoramiento	•Indica como mantener el programa actualizado, monitorizando su efectividad

Es importante tener en cuenta que previamente a las fases mencionadas, se hace necesario ampliar la información de los siguientes conceptos:

Sensibilización	•Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular
Entrenamiento	•Busca enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo. Un programa de entrenamiento no busca certificar (aunque puede llegar a hacerlo), pero puede tener mucha temática relacionada con un curso de certificación.
Educación Formal	•Se define como todos los niveles y habilidades de seguridad envueltos en un único cuerpo de conocimiento
Desarrollo Profesional (Educación No Formal)	•Busca asegurar que los usuarios desde el más principiante hasta el más experimentado, tengan los conocimientos suficientes para desempeñar sus roles.

Conclusión

La información, en los últimos años se ha vuelto uno de los activos más importantes y de mayor valor para las organizaciones, esta se debe proteger a todo momento de posibles ataques o de fugas de información, por tal motivo las compañías de Vigilancia y Seguridad Privada teniendo en cuenta las diferentes interacciones que tienen con el procesamiento, almacenamiento y generación de información a través de los altos volúmenes transaccionales que se generan para garantizar la integridad, confidencialidad y disponibilidad de la información no solamente por parte de la empresa de seguridad sino también en coordinación con la empresa-cliente, y en general todas las partes interesadas.

El usuario final es clave para el desarrollo de un programa de gestión de la seguridad de la información, sin un usuario sensibilizado acerca de las amenazas y vulnerabilidades a los que está expuesto, es más probable que se produzcan incidentes de seguridad que puedan tener impacto considerable dentro de la organización.

La Alta Dirección demuestra un compromiso como parte clave para poder llevar a cabo un buen plan de capacitación. Las métricas son fundamentales para el mejoramiento continuo de cualquier proceso de gestión de seguridad incluyendo el de capacitación y sensibilización.

De igual manera a través de este trabajo se logró evidenciar que existen muchas falencias en la sociedad para tratar los temas de seguridad de la información y de datos confidenciales, adicionalmente el desconocimiento de lo que significa ingeniera social es bastante grande.

Actualmente los delincuentes informáticos usan técnicas cada vez más nuevas, innovadoras y que no alertan fácilmente a sus víctimas, es por eso, que es muy importante lograr llevar a cabo programas de capacitación en cada una de las personas relacionadas con la Seguridad de la Información.

Referencias Bibliográficas

1. https://canaltrece.com.co/programas/mundo-hacker-solombia/ (25/marzo/2018)
2. https://economipedia.com/definiciones/organizacion-la-cooperacion-desarrollo-economico-ocde.html (Junio/2019)
3. https://www.dinero.com/noticias/vigilancia-y-seguridad/1648 (Abril/2019)
4. https://asosec.co/2019/09/el-papel-de-la-seguridad-privada-en-nuestra-sociedad/ (Septiembre/2019)
5. NIST (National Institute Of Standards And Technology) Special Publication 800-50 Building an Information Technology Security Awareness and Training Program.
6. ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident management
7. ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
8. ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
9. BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia. Facultad de educación, 2015. 116 p.