



SEGURIDAD INFORMÁTICA, LA MEJOR OPCIÓN PARA PROTEGER LOS DATOS

COMPUTER SECURITY, THE BEST OPTION TO PROTECT DATA

- **Luis Eduardo Bohorquez Mesa,**
Corporación Tecnología Industrial Colombiana, Ingeniería de sistemas, 95070304962@teinco.edu.co
- **Daniel Gustavo Arango Pinzón,**
Corporación Tecnología Industrial Colombiana, Ingeniería de sistemas, 80124804@teinco.edu.co
- **Diego Esteban López Franco,**
Corporación Tecnología Industrial Colombiana, Ingeniería de sistemas, diego@neogek.com

RESUMEN

En esta década que empieza se debe estar más atentos a la protección de la información, puesto que hoy en día el activo más valioso son los datos, en donde en cualquier momento, desde cierto lugar y desde algún dispositivo electrónico, se puede ser vulnerados en todo sentido, con lo cual atrae la importancia de la seguridad de los datos, tanto de las grandes y pequeñas compañías que requieren de este sistema, es el deber de los ingenieros y personal enfocados en el campo de los sistemas de seguridad salvaguardar todo tipos de datos.

El objetivo de este artículo es visibilizar la importancia de la seguridad informática en diferentes niveles, desde el personal al empresarial, destacando la relevancia de la implementación del software de seguridad, el cual debe ser adaptado a las necesidades del usuario. Cabe destacar que este documento es un artículo de revisión en el que se abordaron 50 fuentes, las cuáles fueron analizadas a través de las siguientes categorías: Sector del riesgo donde aplica la seguridad informática y sus herramientas, Diferentes procesos de ataques maliciosos en la seguridad informática y su prevención o precaución, Afectaciones de software.

Se utilizó la metodología de revisión de diferentes tipos de artículos relacionados con la seguridad informática con sus pro y contras de área de los sistemas para conseguir un punto el desarrollo de este artículo desde un punto de vista más actualizado y concreto.

PALABRAS CLAVE

Seguridad, informática, sector, software, vulnerabilidad.

ABSTRACT

In this decade that is beginning, it is necessary to be more attentive to the protection of information, since today the most valuable asset is data, where at any time, from a certain place and from an electronic device, it can be violated in every sense, which attracts the importance of data security, both large and small companies that require this system, it is the duty of engineers and personnel focused on the field of security systems to safeguard all types of data.

The objective of this article is to make visible the importance of computer security at different levels, from personal to business, highlighting the relevance of the implementation of security software, which must be adapted to the needs of the user. It should be noted that this document is a review article in which 50 sources were addressed, which were analyzed through the following categories: Risk sector where computer security and its tools apply, Different processes of malicious attacks in computer security and its prevention or precaution, Software Impacts.

The review methodology of different types of articles related to computer security with their pros and cons in the systems area was used to achieve a point in developing this article from a more up-to-date and concrete point of view.

KEYWORDS

Security, information technology, sector, software, vulnerability.

INTRODUCCIÓN

La ingeniería de sistemas, se divide y se compone de diferentes ramas, de las cuales, el enfoque de seguridad informática. Hoy en día se debe tener cuidado con las amenazas informáticas, que se implementa las técnicas necesarias para velar por cualquier tipo de información, a todas las amenazas que están creadas por que sea convertido en herramientas de delincuencia a través de la Web (Zambrano, 2015), basándose en la actualidad los datos personales son el punto máximo de las compañías, organizaciones o personas que dañen la integridad de los datos por medio de la web o el espionaje y desde cualquier dispositivo violando la intimidad y la privacidad de la víctima donde se toma las técnicas de protección para la información (Barrera, 2013; Zambrano, 2015).

La mayor parte de la información esta sistematizada, pero surge la pregunta ¿qué tan segura esta?, sin embargo, en el área donde genera más impacto en las empresas u organizaciones en donde los directivos no saben cómo protegerse de la ciberdelincuencia donde entre un 70 y 80% de los directores dan por hecho la creación del crimen organizado dentro de la compañía puesto que la mayoría de ataques son realizados por empleados corruptos, visualizando las vulnerabilidades cibernéticas y el impacto en las organizaciones, con esto se genera interrupción de operaciones, demandas, pérdidas de activos y negocios y multas llevando a la quiebra de la compañía, (Gemma, 2016; Ballesteros, 2018).

Una de las herramientas más vulneradas en la actualidad son los sistemas operativos móviles en todo el mundo, dado que la mayoría de las aplicaciones necesitan permisos y accesos a datos privados del usuario, donde se genera afectación o usurpación de la información, existen medidas de seguridad básicas para la operatividad de android tales como, código de seguridad, bloqueo de pantalla, activar las encriptaciones e instalar un antivirus, (Invitado, 2019), básicamente se implementa varios tipos de defensa contra todos los ataques maliciosos para evitar robos de activos.

Sin embargo, está defensa no es suficiente, uno de los ataques maliciosos llamado malware que es utilizado para el espionaje de información en el mundo, que vulnera los datos por medio de software y hardware, ejemplo la webcam del portátil donde se accede de forma remota, graba lo que hace la víctima sin ser detectado por el usuario poniendo en riesgo la privacidad y seguridad del que se encuentre cerca del portátil como menciona (Andres, 2018). Así como hay personas u organización que causan daños a terceros por los datos, también existen reglas judiciales para hacer responder por las afectaciones realizadas.

Los delitos informáticos son un importante precedente que ajusticia a organizaciones o personas que comentan alguna falta o daño sistemático a terceros como delictivos, modernos, tecnológicos y nuevos penalizados por la ley N°19.366 publicada en el diario oficial el 7 de junio de 1993 en el artículo cuarto castiga a conductas que implementa tecnologías de la información como un medio de comisión se efectúa por hechos punibles esto refiere (Contreras, 2003). De acuerdo a los hechos y actos que realiza las entidades o victimarios se ejecuta su penalización o condena, como medida para evitar los ataques cada

organización o empresa debe crear reglas o parámetros para cada caso que se presente.

Los protocolos de seguridad informática son los parámetros esenciales para cuidar la información satisfactoriamente en cada caso presentado, estas regulaciones son privadas, siendo importante que estén actualizadas cuando se requiera por cada empresa u organización en todo el mundo. El nuevo reglamento general de la protección de datos (GDRP) abarca todas las reglas de privacidad en la plataforma de internet siendo impulsado por Europa menciona, (Patiño, 2018), estipulando la relación entre usuarios y datos aceptando nuevas condiciones para el manejo de las políticas, previamente teniendo una entidad que vele por que se cumplan estos requerimientos.

Existen entidades encargadas de la auditoria de la seguridad de la información sentenciadas en las reglas de privacidad de la compañía como así lo afirma, “realizar Auditorías de Seguridad de la Información, se debe contar con el apoyo y conciencia de parte del plantel directivo, administrativo y ejecutivo de la empresa, con una visión estratégica de negocio de corto, mediano y largo plazo” (Dávalos, AUDITORIA DE SEGURIDAD DE INFORMACIÓN, 2013) que cubra la aplicación de los modelos de seguridad empresarial, gobierno de TI y los ciclos de seguridad, determinando la importancia de la salvaguarda la información.

El objetivo de este artículo es visibilizar la importancia de la seguridad informática en diferentes niveles, desde el personal al empresarial, destacando la relevancia de la implementación del software de seguridad, el cual debe ser adaptado a las necesidades del usuario. Cabe destacar que este documento es un artículo de revisión en el que se abordaron 50 fuentes, las cuáles fueron analizadas a través de las siguientes categorías: Sector del riesgo donde aplica la seguridad informática y sus herramientas, Diferentes procesos de ataques maliciosos en la seguridad informática y su prevención o precaución, Afectaciones de software.

METODOLOGÍA

Se realizaron consultas en diferentes fuentes que proporciona el servicio de internet, como son Scielo-artículos de revistas nacionales e internacionales y periódicos; definidos los criterios y material definidos para el tema principal seguridad informática, recopilando la información, analizando la calidad de los artículos de revisión definidos, y así controlando la variabilidad, fiabilidad y validez de los artículos apuntando a la organización y estructura de los datos como.

- Autores categorizados que declaran conceptos claros con temas relevantes.
- Ubicación geográfica donde se desarrolla el tema analizado, adaptaciones o afectaciones a la ubicación geográfica.
- Identificación y registro de idea principal referida por cada artículo seleccionado.

Concentrados en los 50 artículos fuentes de apoyo y revisión se determinó una identificación por categorías para el parafraseo de los conceptos desde experiencias y conocimientos propios.

Sector del riesgo donde se aplica la seguridad informática, definición y conceptos de los diversos procesos de ataques maliciosos de la seguridad informática y afectaciones de software. Definiendo conclusiones acertadas globalizando los temas abordados durante el desarrollo del documento.

SECTOR DEL RIESGO DONDE APLICA LA SEGURIDAD INFORMÁTICA Y SUS HERRAMIENTAS

Los riesgos de la seguridad informática están aplicados en diferentes sectores del mundo, los cuales son identificados por subsectores de aplicación como en el caso de hogares y empresas que resalta el trato de los datos personales en las compañías que se utiliza para favorecer intereses propios como refiere (Barrera, 2013), la importancia de cada activo personal o industrial se aclara las herramientas o técnicas que detectan amenazas informáticas en la web (Zambrano, 2015).

Las afectaciones que se imparten en los sistemas informáticos son principalmente por diferentes vulnerabilidades que se presenta en el software, por medio de sistemas operativos como macOS colocando en riesgo los datos (TECNÓSFERA, 2018), también incluye el hardware como el espionaje por parte de la webcam implementando técnicas, grabando todo y perjudicando a terceros (Rubén, 2018). Según el programa demandado del gobierno israelí negando cualquier tipo de vínculo con la violación de seguridad de WhatsApp para espiar entidades periodísticas informa (Tecnosfera, 2019).

Actualmente el mundo está pasando por un periodo de crisis por la pandemia del coronavirus, pero los cibercriminales por medio de diferentes ciber amenazas, han aprovechado la situación que se vive ejecutando ataques empresariales y corporativos implementando sistemas de información como redes sociales, digitales y logran el cometido por medio de los dispositivos tecnológicos (Navarro, 2020; Galilea, 2020).

Así como el sector de riesgo afectado sufre ataques y amenazas, también hay medidas de protección a cualquier afectación tanto internamente como externamente (Internet), adicionando sistemas de ciberseguridad como elemento clave para las amenazas informáticas (Álvarez, 2017; Saez, 2019), para prevenir esto necesariamente se actualiza las políticas de privacidad, mitigando los posibles nuevos ataques, estas reglas son actualizadas según los casos de afectaciones a otras empresas, en España el caso de protección de la red en donde detecta e identifica amenazas con un análisis profundo de información que neutraliza los ataques dirigidos al sector empresarial de acuerdo a (Saez, 2019; Palazón, 2016).

El sector de riesgo industrial se ve afectado por la ciberdelincuencia puesto que en la mayor parte de los ataques son internos de la compañía, en un 70 % aproximadamente según los directivos de las compañías, atacan la ciberseguridad, como ejemplo los 33.000

incidentes registrados en el 2018 en España y Portugal, los actos cometidos por medio de las vulnerabilidades presentadas en el medio comercial, las deficiencias se presenta en aplicativos, bases de datos, auto matizadores, servidores, equipos de cómputo entre otros, por lo cual existe el llamado cibercrimen, que utiliza diferentes técnicas de ataque según el estudio realizado por (Cyxtera technologies) da a conocer el listado pronosticado de amenazas en el 2019 (Saez J. M., 2019; Juanes, 2016; Ballesteros, 2018; Digital, 2018), existen técnicas de ciberseguridad para que contrarresta los ataques informáticos.

El intercambio de información es importante para la ciberseguridad, donde se implementa la transformación digital como medio de protección ante cualquier amenaza informática. El cibercrimen se cataloga en un amplio campo en el sector financiero, denegando el acceso a los servidores de una compañía por amenazas como el malware, phishing financiero es un claro ejemplo de una amenaza que más afecta, mayor mente en España pero a su vez hay contramedidas en Colombia para evitar este tipo de robo de cuentas, el ransomware y virus informáticos desprenden ataques a industrial potenciales a los que ha hecho referencia diferentes autores como (TI, 2020; BILBAO, 2020; Manky, 2018; Empresarial, 2017; Velásquez Durán, 2019). Existen diferentes tendencias de ataques cibernéticos por medio de las vulnerabilidades de ciberseguridad a lo que aplica que sea más efectivo el ingreso de los cibercriminales por las debilidades que presenta el sistema de acuerdo a (Arenas, 2018).

Existen varios ejemplos a nivel mundial de todo tipo de ataques o amenazas en el sector industrial, como el caso de EEUU cuando culpó a Corea del Norte de haber creado el virus global wannacry, con el que se secuestraron los ordenadores de 150 países. Otro ejemplo fueron los ataques DNS, que ocasionaron pérdidas monetarias de 6 millones de euros anuales, por medio de 12 ataques. Por lo anterior, se han desarrollado herramientas que brinden seguridad informática como el CSIRT, que establece controles de seguridad formando un perímetro con finalidad de proteger las páginas web para evitar la extracción de información. (Lázaro, 2017; García, 2020; Miranda, 2016).

En las empresas modernas se implementan nuevas tecnologías para que la información sea inaccesible, protegiéndola de todo riesgo informático, basados en la transformación digital obteniendo beneficios y seguridad a los clientes (Álvarez, 2018); la gestión automatizada mediante sistemas informáticos es controlada por la sección del monitoreo, revisión, operatividad, herramientas de hardware y software que escoge la mejor metodología de manejo (Osmany Valdés Pug, Iván, 2016).

Colombia es un país que prioriza la seguridad informática a lo que exigen metodologías para implementar sistemas de gestión de seguridad, proyectos, investigación, software de la información de forma inteligente y convergente con lo cual se prioriza los datos internos de la industria con normas ISO / IEC 27000 y ISO / IEC 30141 del 2018 aplicados a todos los procesos que requiera salvaguardar las aplicaciones, ejecuciones y posibilidades ágiles según los parámetros de estas normas, como la manera correcta de proceder a la información de acuerdo a (Valencia Duque, 2017; Blanco, 2014; Alarcon,

2019), un país que sufre de estas normas ISO y IEC es el estado de México que no cuenta con las capacidades suficientes en el momento adecuado, para hacer frente a todas las amenazas informáticas pero de igual manera se generan ofensivas con equipos de respuesta incidentes computacionales esto con énfasis (Muñoz, 2015).

En consecuencia los delitos informáticos son más fáciles de cometer si no se utiliza las normas ISO, IEC y con esto genera acciones cometidas por el victimario, las cuales perjudican a la víctima ya sea con daño o destrucción de bienes tecnológicos como ordenadores, servidores, o computadoras, perjudicando los intereses de todos los sectores en general, interna y externamente (Mendoza Huarahuara, 2009).

Por lo anterior, cada sector cuenta con un plan de seguridad informática, en el que se realiza auditorías de efectividad sobre la protección de los activos, calificando si cada ítem como las pérdidas, manipulación, posibles daños y los parámetros jurídicos legales, administrativo, financiero o contable que se cumpla debidamente, si no se genera una penalización por el ente encargado, por no cumplir con las medidas debidas de precaución (DÁVALOS SUÑAGUA, 2013).

Por otro lado, la aplicabilidad del sector de salud en convenio con la seguridad informática aplica la tendencia en el manejo de la medicina conlleva a que sus procedimientos medicinales, quirúrgicos, medicamentos en general que necesitan herramientas y cursos sistemáticos con base en la enfermería y las experiencias en el cuidado de los procesos, salvaguardando la información estrictamente necesaria como mencionan, (Cuesta García, 2013; Rodríguez González, 2011), un ejemplo del seguimiento de los protocolos de revisión sistemática sobre el tratamiento de adicciones como en México se evidencia que no se cumple con los ensayos clínicos parciales según lo demuestra los resultados a lo que refiere (Rojas, 2011).

Sumado a lo anterior, el sector tecnológico abarca la responsabilidad de generar estrategias en el comercio electrónico, que aprovecha la idea de generar marketing digital, estudiando todo el campo comercial, el cual genera técnicas de desarrollo de negocio que supera obstáculos transaccionales (Llanes, 2018); en este sentido, el ministerio de tecnología colombiano realiza el estudio de revisión de calidad comercial de los procedimientos de todas las áreas de tecnología, con el fin de que cumpla con las restricciones que genera el ámbito internacional (Correa Henao, 2017).

En cuanto a los protocolos de gestión de seguridad informática en el sector público y privado, es de vital importancia la documentación con el enfoque en pro de la sociedad habilitando medios tecnológicos para el conocimiento de la información segura (Zapata, 2010).

Otro sector que aplica la gestión de las TIC es el cultural, donde las bibliotecas universitarias, generan un impacto trascendental en cuanto a la accesibilidad de la información por medios novedosos y sistemáticos, que permite la transmisión general de la información (González Guitián, 2008).

Finalmente, uno de los sectores más importantes sobre

la seguridad informática es la educación, porque genera la mayor parte del conocimiento, con de fin la medida de efectividad del sector surge ideas sobre gestionar el conocimiento a través de medios electrónicos más enfocado hacia la sociedad universitaria que genera un soporte comunicativo por medio de enseñanza virtual y demás áreas tecnológicas implementadas en el área educativa (Hurtado, 2012).

Diferentes procesos de ataques maliciosos en la seguridad informática y su prevención o precaución.

El cibercrimen ha aumentado debido a que tiene financiación por diferentes entes con intenciones maliciosas, por esta razón se debe tener una gran prevención y usar algunas herramientas para evitar estos ataques, algunas podrían ser tener al día los equipos y sistemas con las actualizaciones correctas, tener cuidado con la información que se accede sea conocida o desconocida, no confiarse de todas las páginas que se consultan, también si es necesario tener seguro de riesgos cibernéticos.

Otros procesos de prevención para poder evitar estos ataques es siempre estar activo y pendiente contra cualquier amenaza por más mínima que sea y no confiarse de nada, tampoco esperar que solo una solución o protección trate de gestionar todos los riesgos que existan sino tener varias alternativas contra cualquier ataque según como lo mencionan (Empresarial, 2017; Digital, 2018).

El cibercrimen en la seguridad informática es afectada por el espionaje por medio de la cámara Webcam de los equipos que se utilizan a diario, por medio del uso de virus o fuentes maliciosas en las que activan automáticamente la cámara de los equipos, con el fin de generar extorsiones entre otros procesos con la información recolectada, por ese motivo se deben tomar algunas precauciones y se debe desactivar la cámara siempre que no la estemos utilizando y si es mejor desactivarla del portátil o equipo desde Windows 10 para una mejor seguridad como lo describe Andres (2018).

Entre algunos ejemplos de la vida real está el caso de estados unidos quien sufrió un ataque en el cual usaron un virus llamado wannacry provenientes del grupo pirata informático Lazarus Group los cuales provienen del país Corea del Norte este virus afectó a Sony Pictures Entertainment en el año 2014 y que provocó que varios archivos se perdieran así lo afirmo (Tecnosfera, 2019; Lazaro, 2017).

El ransomware otro de los tantos virus maliciosos, su funcionalidad consiste en secuestrar toda la información que hay en los sistemas y equipos teniendo control sobre esta, para después pedir un determinado precio con el fin de que el usuario pueda recuperar su información, por medio de la extorsión. Para poder protegerse de estos ataques es necesario que los sistemas tengan varias capas de seguridad y sobre todo tener varias copias de seguridad de toda la información que manejan (Galilea, 2020), otro famoso ataque que se está llevando a cabo es el phishing, el cual ha aumentado considerablemente año a año, para prevenir su ataque y protegerse es necesario generar procesos ya sea de compras u otros ámbitos monetarios o personales verificando correctamente las

páginas y que sea la verdadera viendo sus direcciones web, usar seguridad informática antiphishing, no generar las mismas contraseñas para varias páginas web sino diferente si es posible como lo afirma Byte TI (2020).

Como otros consejos y referente al cuidado de la información de los datos personales ya que actualmente es lo que más desean tener las compañías o grandes empresas para tener poder sobre esta misma y no todas las veces con fines buenos, es necesario usar la herramienta puking money la cual lo que hace es evitar que mientras uno navega en la red no lo puedan rastrear es decir ubicarlo en el mapa, también eliminar todo lo que son datos personales que queden grabados en algún sistema, no registrar o entregar mucha información personal en los sitios web no seguros así lo menciona Barrera (2013).

A raíz de todos los inconvenientes que hay sobre la privacidad de los datos personales y su delincuencia lo que es el Reglamento General de Protección de Datos están generando regulaciones y normas en la cual las empresas tienen que tener un buen manejo y ciertas restricciones sobre la información personal que manipulan con la idea de que esto se implemente a nivel mundial o en la mayoría de los países en diferentes plataformas o empresa lo afirma Patiño (2018).

La mayor preocupación a nivel general en las empresas según un estudio realizado en la que se encuestaron a más de 700 altos directivos de 18 sectores y países el 68% tiene que ver con la ciberseguridad, ya que sus propios empleados son los mismo involucrados en estos casos y más que todo los que trabajan en áreas que tienen que ver con el manejo de información, con el fin de mitigar estos procesos algunos consejos es generar constantes monitoreos sobre la seguridad informática y el manejo de los empleados con la información que gestionan, también a partir de análisis que se validen generar políticas de seguridad de acuerdo a los inconvenientes o los problemas que se encontraron, generar evaluaciones y a su vez dar capacitaciones a los empleados sobre los riesgos que existen y cómo actuar en caso de alguno así lo describe Juanes (2016).

Teniendo en cuenta lo mencionado anteriormente, para poder afrontar o castigar todo lo que tiene que ver con delitos informáticos y que no sean impunes, hay leyes y artículos que sancionan estas actividades ilícitas, como lo es la ley número 19.366 del país de Chile la cual contiene cuatro artículos que abordan todo lo que tiene que ver con espionaje informático y sabotaje informático lo describe Clunes (2003).

Como cada vez son mayores las amenazas en el ámbito de los sistemas en la seguridad de la información, ha sido necesario generar más sistemas o programas para combatir o prevenir los ciberataques, uno de estos es el tema de la criptografía, lo que hace que nuestros datos sean más seguros y protegidos como lo enuncia Travieso (2003), también existen otras herramientas o equipos de ayuda en el tema de la protección de información con lo que es el manejo de páginas o plataformas y a su vez la creación o implementación de estas mismas con todo lo que es el cuidado que se debe tener con las tecnologías que se van a utilizar sin haber algún fraude que tenga que ver con robo de información, este proceso se llama CSIRT que sus siglas son Computer Security Incident Response Team así lo explica Miranda (2016).

AFECCIONES DE SOFTWARE

Los sistemas operativos Android en su mayoría instalados a los equipos móviles, están catalogados como vulnerables, por la gran cantidad de ataques realizados a estos sistemas operativos, con el fin de vulnerar datos de los usuarios para los secuestros o robos de información, ataque conocido como Phishing (Invitado, 2019), también el año pasado 2018 se detectó en el sector financiero crecimiento y variedad en la modalidad de spam donde la víctima por desconocimiento queda vulnerable para el atacante (Redhat, 2020).

Los accesos remotos son vulnerabilidades del software cuando se acceden remoto, debido a que es necesario interconectar por medio de una web con el servicio de internet, teniendo en cuenta que los niveles o parámetros de seguridad se encuentran a niveles altos siempre existe debido a que el canal de conexión entre el dispositivo y el acceso remoto será a través de internet, señalado por (García Urra, 2013).

Como protección o blindaje a los datos personales y evitar homónimos, se debe solicitar o tramitar a las diferentes entidades la debida actualización de los datos personales, con el fin de evitar clonación de datos que pueden afectar en diversas situaciones, como en las transacciones financieras y afectaciones de software (Patiño, 2018).

Cada actualización del recurso tecnológico software de protección para las vulnerabilidades generadas en las diferentes máquinas y dispositivos con acceso a internet, se convierte en la herramienta indispensable para mitigar riesgos de afectaciones de los diferentes ataques, generando vulnerabilidad de contaminación por virus en el dispositivo para cumplir un objetivo diseñado como lo afirma (Miranda Cairo, 2016), adicionalmente, se deben aplicar las actualizaciones vigentes aprobadas y validadas por el desarrollador de la herramienta, protegiendo las máquinas de las actualizaciones que también realizan los atacantes (Muñoz, 2015).

Así como para la protección de una afectación de software existen actualizaciones, los atacantes crean nuevas maniobras para vulnerar esas actualizaciones, exigiendo que los desarrolladores implementen mayores seguridades en cada actualización a sus herramientas, apuntando principalmente en los sectores financieros (Manky, 2019); las nuevas estrategias de los atacantes crean herramientas de ataque que facilitan los accesos sin límites de tiempos ni espacios (Alvarez, 2018), por ello el sector financiero se convierte en el blanco principal de los atacantes, por medio de las afectaciones de software (García, 2020).

En las investigaciones de una auditoría forense, las huellas y rastros son las evidencias para generar un informe a una auditoría por una afectación de software, ayuda a indicar el proceso realizado para la afectación identificando que los protocolos y actividades realizadas acorde a los lineamientos establecidos, realizando el procedimiento real de una ingeniería forense concluyendo un resultado exitoso, coherente y lograr programar exigir acciones de mejora para las afectaciones generadas (Mejía Apaza, 2009).

Como los procesos de la seguridad de la información se replica la importancia de la formación constante, es

decir capacitación periódica para afrontar y mitigar afectaciones de riesgo de los activos tecnológicos (Hurtado, 2012), así como las preparaciones deben ser constantes la formación académica debe contener los medios para entregar profesionales aptos para la atención especializada en mitigar y proteger de las afectaciones de software (Correa Henado, 2017).

Los sectores públicos son los más vulnerados por los ciberataques, porque estos sectores generalmente por el volumen de tránsito y procesos no se preparan para implementar la ciberseguridad, afirmando que los adversarios ciberataques suelen ser ex empleados o empleados activos contaminados según estudio según menciona (Saenz, 2016) , además se suma el cibercrimen, el cual en la actualidad genera unas estadísticas de dispositivos y sectores afectados proyectando donde se debe aumentar las herramientas de protección informática, de acuerdo a los avances y accesos que brindan plataformas de redes sociales, incrementando el riesgo de vulnerabilidad de las afectaciones a los sistemas de información (Redaccion digital, 2018).

La efectividad de controles se centra directamente a los parámetros, seguimientos, auditorias y monitoreos periódicos con el fin de certificar y avalar la efectividad de herramientas implementadas, para contrarrestar las afectaciones de software que debido a la diversidad de medios y formas son inevitables, también en ocasiones complejas de percibir si no se cuenta con los refuerzos en los escudos (Mejia Miranda, 2016).

La correcta planificación e implementación de un sistema de controles de riesgos hacia las afectaciones de software genera la posible evasión de un ataque, porque entre el atacante y su objetivo la barrera estará tan blindada que el nivel vulnerabilidad será mínimo y las herramientas de ataque aumentaran, esto se cumplirá en una proyección planificada por un director especializado así lo afirma (Vanegas, 2014), además, el control mediante auditorias certifican la efectividad de las medidas y herramientas implementadas, socializadas mediante políticas y estándares de una compañía con estricto cumplimiento y acciones de mejora continuas (Davalos Suñaga, 2013).

También catalogado como ciberataque o hacker genera incumplimiento de las normas legales como se mencionó anteriormente aplicando ingeniería forense detectando huellas y rastros de los ataques exitosos, estas vulnerabilidades afectadas principalmente en las redes sociales apuntan a generar informes y detección de textos que conlleven a implicaciones legales o información confidencial, generalmente el atacante se encontrara a miles de kilómetros de su objetivo para ampliar los rastros huellas si llegase a dejar, como refiere (El tiempo, 2019).

La vulnerabilidad de firewall en los dispositivos y maquinas permite los accesos hasta en una cámara de los dispositivos con fines específicos de seguimientos o pornografía, estas afectaciones adicionales de software son peligrosas afectando la privacidad personal (Andres, 2018).

Por otro lado los dispositivos que se conectan generalmente a un computador como USB, unidades externas, teclados inalámbricos, impresoras, etc. conocidos como dispositivos periféricos las compañías u organizaciones con fines de automatizar y controlar las industrias implementan nuevas tecnologías permitiendo tumbar barreras y ampliando la vulnerabilidad del acceso para los objetivos del atacante, generando una afectación, estas pueden ser provocadas desde los fabricantes cuando por ocurrencias con beneficios lucrativos divulgan las vulnerabilidades de los equipos nuevos en el mercado (TECNOESFERA, 2018).

Las ideas opinadas anteriormente son el producto de los conceptos personales percibidos en los diferentes artículos registrados, agregando comentarios independientes a cada artículo respetando las redacciones de cada autor.

CONCLUSIONES

Los resultados mencionados anteriormente se concluyen que la seguridad informática se debe tener muy presente en todo lo que tiene que ver con las empresas tanto grandes, como pequeñas y también en el entorno de hogar, es decir, en todos los sectores o áreas, ya que, de esto depende lo que es prevenir y combatir cualquier riesgo que afecte tanto personal como económicamente y cada vez más se puedan hacer procesos más fácilmente para mitigar estos ataques.

Adicionalmente se aprecia que la mayor parte de vulnerabilidades se presentan a nivel de software, porque las protecciones son mínimas y las herramientas de ataques son más actualizadas vulnerando fácilmente los diseños de seguridad informáticos, entonces podemos concluir que los niveles de protección se deben centrar en blindar los accesos a los sistemas de información y metodologías de acceso a los diferentes aplicativos.

Teniendo en cuenta por último la seguridad informática es la medida de protección más alta con toda la información ya sea corporativos o personales, resaltando así que los datos hoy en día son la mayor prioridad para la humanidad por el riesgo que conlleva que alguna organización o persona que afecte los intereses de cada víctima, con todas las técnicas, prevención y protección informáticamente se conseguirá un mundo cada vez más seguro.



REFERENCIAS



- Alarcon, D. M. (2019). Investigación Software inteligente y convergencia tecnológica. Universidad catolica.
- Álvarez, E. (2017). ¿Cómo protegerse de los virus, piratas informáticos y demás ataques? Computer Hoy.
- Alvarez, R. (2018). Atacar Sin Avisar. revista empresarial.
- Andres, R. (2018). Cómo evitar que te espíen por la webcam de tu portátil. Computer HOY.
- Arenas, I. (2018). Tendencias en ciberseguridad para el 2019. revista empresarial.
- Ballesteros, A. (2018). Vulnerabilidades Cibernéticas y su Impacto Organizacional. Revista Empresarial y Laboral.
- Barrera, D. (2013). Algunos consejos para proteger sus datos mientras navega en la web. Emprendices.
- BILBAO, D. (2020). ¿Cómo evitar el phishing y robo de cuentas? Dinero.
- Blanco, J. M. (2014). Gestión de Proyectos en el Grado en Ingeniería Informática sin tener en cuenta la seguridad informatica. aenui net.
- Contreras, A. C. (2003). DELITOS INFORMÁTICOS: UN IMPORTANTE. Ius et Praxis.
- Correa Henado, G. (2017). Revisión y diagnóstico sobre las condiciones de calidad en los programas de Ingeniería de Sistemas en Colombia. Revista iberoamericana de educación superior.
- Cuesta García, Y. (2013). Curso Informática para la gestión del Cuidado. Diseño, experiencias y resultados de su primera edición. scielo.
- Davalos Suñaga, A. F. (2013). AUDITORIA DE SEGURIDAD DE INFORMACIÓN. Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia.
- Digital, R. (2018). 10 Amenazas del Ciberdelincuencia para el 2019. revista empresarial.
- El tiempo, R. (2019). Gobierno israelí niega vínculos con programa demandado por espionaje.
- Empresarial, R. (2017). El cibercrimen, una Amenaza Virtual muy Real. revista empresarial.
- Galilea, D. (2020). Las ciberamenazas de las que más debe cuidarse este año. El tiempo.
- García Urra, F. (2013). Dispositivos eléctricos y monitorización remota. Revista uruguaya de cardiología.
- García, V. (2020). Los ataques DNS superan los 6 millones de euros anuales. REVISTA BYTE TI.
- Gemma, G. J. (2016). Los directivos no saben combatir la ciberdelincuencia de un modo eficaz. Cuadernos de Seguridad.
- González Guitián, M. V. (2008). Las bibliotecas universitarias: breve aproximación a sus nuevos escenarios y retos. scielo.
- Hurtado, L. (2012). e-Informatica UMSA. Revistas bolivianas.
- Invitado, A. (2019). Consejos de seguridad para dispositivos Android. Emprendices.
- Juanes, G. G. (2016). Los directivos no saben combatir la ciberdelincuencia de un modo eficaz. Cuadernos de seguridad.
- Lázaro, M. (2017). EEUU culpa a Corea del Norte del virus global WannaCry. Computer Hoy.
- Llanes, R. P. (2018). Estrategias de comercio electrónico y marketing digital para pequeñas y medianas empresas. scielo.
- Manky, D. (2018). La inteligencia de amenazas es una necesidad crítica. revista empresarial.
- Manky, D. (2019). Las tácticas que amenazan su seguridad informática. El tiempo.
- Mejía Apaza, W. (2009). Auditoria Forense. Revistas bolivianas.
- Mejía Miranda, J. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. Revista Ibérica de Sistemas e Tecnologías de Informação.
- Mendoza Huarahuara, M. M. (2009). Delitos informatico. revistas bolivarianas.
- Miranda Cairo, M. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana de Ciencias Informáticas.



REFERENCIAS



- Miranda, J. M. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. SCIELO.
- Muñoz, M. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. Revista Ibérica de Sistemas e Tecnologías de Informação.
- Navarro, M. (2020). No podían faltar: cibercriminales se aprovechan del COVID-19. BYTE TI.
- Osmany Valdés Pug, Iván, M. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. scielo.
- Palazón, F. J. (2016). Trend Micro Deep Discovery – Protección de la red. Byte TI.
- Patiño, L. (2018). ¿Por qué todos están actualizando sus políticas de privacidad? El tiempo.
- Redaccion digital. (2018). 10 Amenazas del Cibercrimen para el 2019. Revista empresarial.
- Redhat. (2020). Redhat. Recuperado el 2020, de <https://www.redhat.com/es/topics/cloud-computing/what-is-public-cloud>
- Rodríguez González, D. (2011). Interdisciplinariedad entre la Medicina General Integral y la Informática Médica relacionada con el desarrollo de una revisión bibliográfica. scielo.
- Rojas, E. (2011). Revisión sistemática sobre tratamiento de adicciones en México. scielo.
- Saenz, J. M. (2016). Los directivos no saben combatir la ciberdelincuencia de un modo eficaz. Cuadernos de seguridad.
- Saez, J. M. (2019). En 2018 se registraron más de 33.000 incidentes de ciberseguridad en entidades del sector público. byte ti.
- Saez, N. (2019). Wefender, primer sistema de Seguridad WiFi as a Service. byte TI.
- TECNÓSFERA. (2018). Descubren vulnerabilidad en macOS Mojave que pone en riesgo sus datos. El tiempo.
- Tecnosfera, R. (2019). Gobierno israelí niega vínculos con programa demandado por espionaje. El tiempo.
- TI, R. B. (2020). El phishing financiero creció un 9,5% en el último trimestre de 2019. revista bite TI.
- Valencia Duque, F. J. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. scielo.
- Vanegas, G. (2014). Hacia un modelo para la gestión de riesgos de TI. Revistas científicas de America.
- Velásquez Durán, A. M. (2019). Las tácticas que amenazan su seguridad informática. el tiempo.
- Zambrano, A. M. (2015). La importancia de la seguridad informática. Revista de Logística Logo.
- Zapata, C. A. (2010). La preservación de documentos vitales: aproximación a la situación actual en el Distrito Capital. scielo.