METODOLOGÍAS PARA LA IDENTIFICACIÓN Y MITIGACIÓN DE VULNERABILIDADES INFORMÁTICAS GENERADAS POR LOS USUARIOS DEL SISTEMA PARA EMPRESAS PÚBLICAS Y PRIVADAS

JHON MAURICIO CAICEDO URBANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2021

METODOLOGÍAS PARA LA IDENTIFICACIÓN Y MITIGACIÓN DE VULNERABILIDADES INFORMÁTICAS GENERADAS POR LOS USUARIOS DEL SISTEMA PARA EMPRESAS PÚBLICAS Y PRIVADAS

JHON MAURICIO CAICEDO URBANO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Jhon Mauricio Caicedo Urbano
Asesor y Director:
Edgar Roberto Dulce Villareal

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Pasto., 20 de abril de 2021

DEDICATORIA

A mi familia: encabezada por mi padre, quien es el pilar central y quien siempre nos hizo un llamado a la responsabilidad, el progreso, el cariño a la familia y el esfuerzo en cada proyecto de nuestras vidas; a mis hermanos y hermanas, quienes dedicaron mucho de su tiempo en mí, con quienes sin duda, libramos muchas batallas para salir adelante y hacer las cosas de la mejor manera posible, sin olvidar jamás que somos una familia que se ha mantenido unida, comprensiva y afectuosa, demostrando que siempre estaremos ahí, los unos para los otros en cualquier instancia. Y por supuesto, también a mi madre, quien vive en nosotros sus hijos, en nuestros corazones, en nuestra memoria y la de todos los que la recordamos, a ella, solo espero que se sienta orgullosa por cada paso que hemos dado todos sus hijos.

A mi tío Segundo Lires y su esposa Rosita: gracias por creer desde un principio en mí, en prestarme su atención y por darme el apoyo inicial para empezar mis estudios profesionales; a veces solo necesitamos alguien que nos apoye en dar el primer paso y nos de la convicción para continuar un camino sobre la educación, tengo la fortuna de que mi vida sea bendecida con su apoyo. Doy las gracias a toda su familia y deseo absolutamente que su vida esté llena de felicidad y bendiciones, así como hoy puedo decir que es mi vida, llena de esperanza y oportunidades por sus manos que se extendieron hasta mí.

AGRADECIMIENTOS

Agradezco la Universidad Nacional Abierta y a Distancia por permitirnos alcanzar nuestras metas de esta forma, sin duda representa una gran oportunidad para muchos y es un honor hacer parte de esta gran familia; a mis tutores y asesores, quienes sin duda guiaron este proyecto por el mejor camino a través de su valiosa experiencia y sentido de acompañamiento docente, lo cual me permitió desarrollar mucho más mi calidad profesional y humana, por cada minuto de calidad prestado de su parte, muchas gracias.

A Leidy G. Timaná: de alguna forma, sembraste una poderosa semilla en mí. Esta concesión, es un reto hacia la superación y me ha permitido explotar muchas cualidades personales, como el espíritu competitivo que hoy me impulsa. A ti, te deseo lo mejor del universo, te admiro por lo que has logrado, por tus batallas, tu forma de ser y tus valores. Infinitas gracias por cada uno de los detalles que has tenido conmigo, sé que conforman una lista incontable; gracias por tu paciencia, espero de corazón, contar contigo en cada nuevo día que venga y poder prolongar siempre esos momentos y charlas de dos conciencias iguales, pero sin iguales entre otras a la vez.

CONTENIDO

pág.

LISTA DE CUADROS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZA INFORMÁTICA: definida como las causas y los elementos que pueden causar un incidente informático que perjudique el adecuado funcionamiento de estos o los intervenga sin autorización con fines ajenos a los de la organización[1].

AUDITORÍA: es un examen crítico y muy puntual del estado de todos los procesos y recursos informáticos que pretende identificar falencias o debilidades para proponer mejoras[2].

CIBERSEGURIDAD: corresponde a la seguridad digital que se aplica a los sistemas informáticos a través de la implementación de software, hardware o técnicas que pretendan su protección[3].

CIFRADO: procedimiento mediante el cual se transforma un mensaje volviendo ilegible su información para que no pueda ser accesible o legible por cualquier otro actor diferente al destinatario[4].

CONTROLES: conjunto de procesos y actividades relacionadas a la ejecución correcta de las actividades relacionadas con el uso de los sistemas informáticos, usualmente documentados y que permiten su auditoría[5].

CRIPTOGRAFÍA: área que se encarga del estudio de técnicas de cifrado y descifrado de datos e información a través de la codificación o decodificación efectiva del mensaje, permitiendo la protección en cuanto a la privacidad de su contenido[6].

---

[1] MARTINEZ FERREL Ernesto, Las amenazas informáticas. [en línea]. 2018. [Consulta: 3 de septiembre 2020]. Disponible en: https://sites.google.com/site/lasamenazaslainformatica/

[2] INDICE.MX. [Sitio web]. Auditorías de TI. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.indice.mx/nuestros-servicios/auditorias-de-ti/

[3] KASPERSKY. [Sitio web]. Qué es Ciberseguridad. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[4] WELIVESECURITY. [Sitio web]. Todo sobre cifrado: qué es y cuándo deberías usarlo. 2016. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2016/02/09/todo-sobre-cifrado-cuando-usarlo/

[5] ENTERPRISEIT. [Sitio web]. Controles generales de tecnologías de información. [Consulta: 3 de septiembre 2020]. Disponible en: https://enterpriseit.cl/controles-generales-de-tecnologias-de-informacion/

[6] BBC NEWS. [Sitio web]. Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.bbc.com/mundo/noticias-50862657

DATOS: elementos digitales de tipo numérico, alfanumérico o de cadena que en conjunto conforman la información a la cual se le da un significado o valor característico[7].

EMAIL: correo electrónico o digital creado con el objetivo de generar o recibir mensajes digitales creados a través de dispositivos electrónicos permitiendo una comunicación asincrónica, directa, eficiente y recursiva[8].

ESTÁNDAR: modelo o conjunto de características de uso general que permiten optimizar el funcionamiento, asegurar la protección y alinear los objetivos informáticos[9].

HACKING: proceso que se realiza mediante el empleo de herramientas y técnicas informáticas y sociales que permite acceder a información u obtener privilegios y recursos por métodos no establecidos o autorizados para ello[10].

HARDWARE: parte tangible de la computadora, que se puede manipular manualmente y que soporta el software[11].

INFORMACIÓN: conjunto de datos que tiene un valor o significado, se puede encontrar la información almacenada tanto en medios físicos como digitales[12].

INFRAESTRUCTURA TECNOLÓGICA: conjunto de dispositivos de cómputo y red, en algunos casos se considera el software como parte de esta infraestructura, además de sus elementos auxiliares y periféricos que tienen una entidad u organización. Se puede encontrar infraestructura de nube, e hiperconvergente[13] según el tipo de tecnologías implementadas en la entidad.

---

[7] RAFFINO María. Dato en informática. [en línea]. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://concepto.de/dato-en-informatica/

[8] INTERNET-DIDACTA. [Sitio web]. Qué es el E-Mail o Correo electrónico. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.internet-didactica.es/e-mail-correo-electronico/

[9] GESTIONYAUDITORIATI. [Sitio web]. Aplicación de Estándares de TI. 2012. [Consulta: 3 de septiembre 2020]. Disponible en: https://gestionyauditoriati.com/2012/09/07/aplicacion-de-estandares-de-ti/

[10] MALWAREBYTES. [Sitio web]. Todo sobre el hackeo 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://es.malwarebytes.com/hacker/

[11] CISET. [Sitio web]. Definición de Hardware. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.ciset.es/glosario/451-hardware

[12] LAMANNA Carlos. [blog]. Dato, información, sistema. En: Introducción a la Informática. s.f. Instituto Superior Nuestra Señora de la Paz. [Consulta: 3 de septiembre 2020]. Disponible en: https://datosuno.wordpress.com/unidad-1/introduccion/

[13] REDHAT. [Sitio web]. ¿Qué es la infraestructura de TI? 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

INGENIERÍA SOCIAL: conjunto de técnicas que permiten obtener información confidencial a través de la manipulación de los usuarios del sistema, usualmente a través de la investigación en redes sociales, blogs o comunidades digitales de la víctima[14].

INTERNET: también conocida como la red de redes, interconecta los países y las redes públicas, permitiendo compartir recursos e información[15].

ISO/IEC: organizaciones cooperativas que determinan normas y estándares internacionales para regular y guiar, tanto implementaciones como procesos y desarrollos de forma optimizada[16].

KALI LINUX: sistema conformado por un conjunto de herramientas informáticas avanzadas útiles para auditar sistemas y redes informáticos[17].

MAGERIT: metodología de análisis y gestión de riesgos informáticos que permiten generar controles y administrar la seguridad de la información[18].

MALWARE: software malicioso desarrollado con el fin de afectar los sistemas, robar la información o deteriorar el rendimiento de los recursos informáticos[19].

METODOLOGÍA: conjunto de estrategias útiles para cumplir un objetivo TI, en informática existen varias metodologías que incluyen normatividad legal vigente y controles[20].

OFIMÁTICA: conformado por software de oficina, contiene aplicaciones de uso común para la creación de documentos, presentaciones e informes[21].

---

[14] AVAST. [Sitio web]. Qué es la ingeniería social y cómo evitarla. 2020. [Consulta: 1 de noviembre 2020]. Disponible en: https://www.avast.com/es-es/c-social-engineering

[15] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Internet, ¿qué es? ¿para qué sirve? 2015. [Consulta: 15 de septiembre 2020]. Disponible en: https://www.enticconfio.gov.co/internet-que-es-para-que-sirve

[16] ISO. [Sitio web]. ISO/IEC Guide 60 (es). 2015. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:guide:60:ed-2:v1:es

[17] KALI. [Sitio web]. What is Kali Linux, and what is a Penetration Testing Distribution? 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.kali.org/features/

[18] WELIVESECURITY. [Sitio web]. MAGERIT: metodología práctica para gestionar riesgos. 2013. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[19] AVG. [Sitio web]. ¿Qué es el malware? Cómo funciona el malware y cómo eliminarlo. 2019. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.avg.com/es/signal/what-is-malware

[20] ZAGXA CONSULTING. [Sitio web]. Metodologías de TI. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.zagxa.com/metodologias-de-ti/

[21] EUROINNOVA. [Sitio web]. Qué es la ofimática. s.f. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.euroinnova.co/blog/11-4-18/manejo-de-la-ofimatica-con-el-curso-de-office

PHISHING: técnica de ingeniería social que utilizan estafadores para suplantar otra persona, entidad o empresa, mediante mensajes de correo electrónico que contienen formatos y estilos similares a los usados por el usuario o entidad verdaderos, con el objetivo de obtener información privada o sensible de la persona[22].

POLÍTICAS DE SEGURIDAD: conjunto de normas establecidas para garantizar el cumplimiento de las buenas prácticas de seguridad informática, con el objetivo de mitigar los riesgos y amenazas informáticas[23].

RED INFORMÁTICA: se la conoce como la integración e interconexión de dispositivos, computadoras, periféricos y elementos de red que permiten intercambiar información, datos o servicios de manera local o en el entorno de red configurado[24].

RIESGOS: es el grado de exposición que se tiene ante la materialización de una amenaza informática, usualmente se miden en factor del valor de la consecuencia a generar[25].

SEGURIDAD INFORMÁTICA: conjunto de estrategias, reglas, elementos y acciones que se pueden implementar en un sistema informático con el objetivo de garantizar la protección, a través de la privacidad, la integridad y la disponibilidad[26].

SISTEMA DE INFORMACIÓN: es un conjunto de datos y recursos integrados que permiten la administración de la información de forma eficiente de acuerdo a los parámetros establecidos para su recolección, procesamiento, almacenamiento o eliminación[27].

---

[22] INFOSPYWARE. [Sitio web]. ¿QUÉ ES EL PHISHING? s.f. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

[23] DISETE COMUNICACIONES. [Sitio web]. Qué son las políticas de seguridad informática y por qué tu empresa debe tener una. 2020. [Consulta: 20 de septiembre 2020]. Disponible en: https://disete.com/que-son-las-politicas-de-seguridad-informatica-y-por-que-tu-empresa-debe-tener-una/

[24] REDESZONE. [Sitio web]. Qué tipos de redes informáticas existen. 2019. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/tipos-redes-informaticas/

[25] DELOITTE. [Sitio web]. Riesgos de TI. 2016. [Consulta: 3 de septiembre 2020]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf

[26] UNIVERSIDAD INTERNACIONAL DE VALENCIA. [Sitio web]. Qué es la seguridad Informática. 20163. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

[27] UNIVERSIDAD DEL CAUCA. [Sitio web]. Aspectos Organizacionales de los Sistemas de Información. 2015. [Consulta: 3 de septiembre 2020]. Disponible en: http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm

SISTEMA OPERATIVO: software principal que permite la interacción entre el usuario y los componentes de hardware, el cual soporta y administra los mismos para el correcto funcionamiento de aplicaciones como las de tipo ofimático o de entretenimiento como reproductores de vídeo o vídeo juegos[28].

SOFTWARE: se lo identifica como toda la parte lógica e intangible de un equipo de cómputo, un dispositivo de hardware u otro de carácter físico, el cual permite la interacción entre el usuario y el sistema ofreciendo al usuario diversas funcionalidades o utilidades de carácter variado como de tipo ofimático o lúdico[29].

TECNOLOGÍA: se entiende como tecnología a la aplicación de la ciencia o del conocimiento científico, que permite realizar diversas actividades de manera rápida, organizada y eficiente a través de la implementación en conjunto de sistemas de software y hardware[30].

USUARIO: se reconoce como usuario, a toda persona que manipula un sistema o que hace uso de este para los fines con los que fue desarrollado a través de un dispositivo de hardware[31].

VIRTUALIZADO: entorno simulado que refiere a sistemas soportados virtualmente por medio de plataformas o software que permiten la instalación, administración o funcionamiento de diferentes servicios usualmente sobre servidores físicos[32].

Zero-day: son todas aquellas vulnerabilidades en los sistemas que se detectan antes de que el desarrollador provea una actualización que permita cubrir la vulnerabilidad[33].

---

[28] AREATECNOLOGIA. [Sitio web]. Sistemas Operativos. 2019. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.areatecnologia.com/sistemas-operativos.htm

[29] TIPOS. [Sitio web]. Tipos de Software. 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.tipos.co/tipos-de-software/

[30] UNIVERSIDAD NACIONAL DEL LITORAL. [Sitio web]. ¿QUÉ ES LA TECNOLOGÍA? 2018. [Consulta: 5 de septiembre 2020]. Disponible en: http://www.unl.edu.ar/ingreso/cursos/cac/21ot/#1484779044787-8891d599-6206

[31] ENCICLOPEDIA CUBANA. [Sitio web]. Usuario (Informática). 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.ecured.cu/Usuario_(Inform%C3%A1tica)

[32] VMWARE. [Sitio web]. ¿En qué consiste la virtualización? 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.vmware.com/co/solutions/virtualization.html

[33] OFICINA DE SEGURIDAD DEL INTERNAUTA. [Sitio web]. ¿Qué es una vulnerabilidad Zero Day? 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.osi.es/es/actualidad/blog/2020/08/28/que-es-una-vulnerabilidad-zero-day

RESUMEN

La seguridad informática en la actualidad ha tenido un crecimiento exponencial derivado de la necesidad que ha causado la demanda tecnológica alrededor de todo el mundo, esto debido también a que la expansión de las redes y el alcance de la tecnología, ha traído consigo un acercamiento de tecnologías a la mano para cada ser humano, y esto a su vez, ha generado consigo el crecimiento de amenazas informáticas generadas por usuarios maliciosos de la red con propósitos ya identificados a nivel mundial como ilegales e inaceptables para el propósito del bienestar de los demás usuarios de la tecnología y las redes informáticas.

Es por esto que se iniciará por realizar una breve introducción y análisis de los sistemas informáticos y la tecnología que hoy se tiene a la mano, para esto se debe tener en cuenta no solo los recursos empresariales más comunes, sino también los dispositivos y servicios que cada persona podría tener; posteriormente se realizará una identificación de las principales amenazas a las que se está expuesto con el uso de estos servicios, sistemas y dispositivos, de la mano de una metodología de gestión de riesgos para entornos organizacionales como es MAGERIT y de normas internacionales como ISO/IEC 27002 que permiten identificar riesgos y de igual forma definir buenas prácticas y controles que pretenden reducir los riesgos y amenazas informáticas a los que a diario son expuestos los usuarios de los sistemas de las organizaciones, a los cuales no solo se debe pretende educar para resguardar la información de la entidad, sino también para su beneficio personal en el uso de la internet y la tecnología.

.

ABSTRACT

Computer security today has had an exponential growth derived from the need that has caused the technological demand around the world, this also because the expansion of networks and the scope of technology, has brought with it an approach of technologies at hand for each human being, and this in turn, has generated the growth of computer threats generated by malicious users of the network with purposes already identified worldwide as illegal and unacceptable for the purpose of the well-being of other users of technology and computer networks.

For this reason, we will begin with a brief introduction and analysis of the computer systems and technology available today, taking into account not only the most common business resources, but also the devices and services that each person may have; Afterwards, an identification of the main threats to which one is exposed with the use of these services, systems and devices will be made, using a risk management methodology for organizational environments such as MAGERIT and international standards such as ISO/IEC 27002 that allow identifying risks and defining good practices and controls that aim to reduce the risks and IT threats to which the users of the organizations' systems are exposed on a daily basis, These users should not only be educated to protect the entity's information, but also for their personal benefit in the use of the Internet and technology.

INTRODUCCIÓN

El creciente uso de las redes de internet, de las aplicaciones de software en recursos ofimáticos o incluso el para el acceso a material de entretenimiento, requieren cada vez más de un esfuerzo conjunto entre administradores del sistema y los usuarios, para garantizar la seguridad de la información que comparten, descargan o almacenan en la web o en sus equipos personales; por lo que a medida que las redes se expanden en el territorio nacional y llegan a distintos lugares también aumentan los riesgos presentes en las mismas. Con el paso del tiempo, nuevos usuarios malintencionados del internet se han formado aprovechando la vulnerabilidad más grande de los sistemas, los usuarios, quienes muchas veces sin reconocer los riesgos de acceder a una red pública o sin protección, comparten información confidencial, hacen uso de las aplicaciones bancarias o incluso entregan permisos de acceso y control total a las aplicaciones que instalan sin verificar en los equipos, y lo peor de todo, es que se da la oportunidad de vulnerar los sistemas de las entidades desde un punto pocas veces protegido.

Este es el caso que se pretende abordar en el presente trabajo, determinar las amenazas más importantes a las cuales se exponen los usuarios del sistema e identificar a través de metodologías de evaluación de riesgos, los controles más efectivos frente a estas amenazas, las cuales pueden ser muy perjudiciales si los usuarios de los sistemas no conocen ni pueden evitar a través de buenas prácticas informáticas y de la aplicación de metodologías eficientes dentro de la entidad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Desde que internet vio la luz en mercado del mundo y empezó a expandirse junto con la implementación de la World Wide Web (WWW) en el año de 1990, el crecimiento exponencial de las redes de internet y el uso de la tecnología han significado una serie de cambios en todos los aspectos de la humanidad, todo esto en una era donde la carrera tecnológica que hoy en día se vive, es impulsada por el consumo, la demanda, de nuevos dispositivos y aplicaciones más funcionales, rápidos y últimamente también más seguros.

Sin embargo, este desarrollo continuo y acelerado también ha predispuesto escenarios importantes que hoy en día son muy evidentes para ser ignorados, especialmente por las grandes organizaciones que claramente tienen en juego mucho en los sistemas informáticos. La seguridad informática nace la de necesidad de proteger la información y los sistemas de cualquier posible intrusión, entendiendo estas como las amenazas y los riesgos informáticos a los cuales se está expuesto por el uso de la tecnología; ya que como se ha visto a diario en las noticias, cada vez son mucho más frecuentes los ataques y con gran variedad de tipos de presentación, que van desde infiltraciones en sistemas, correos falsificados, y dispositivos alterados, hasta el uso de estrategias de comunicación y psicología en técnicas de ingeniería social.

En 1972, se creó y demostró el primer virus informático, a partir de ese día y con el auge del internet las amenazas informáticas se han extendido a tal punto que se puede identificar en la actualidad millones de estas, y a su vez se encuentran otras clases de amenazas que se diversifican, mutan o mejoran su efectividad para poder sobrepasar la “barrera” de seguridad que los sistemas ofrecen; sin embargo, dicha “barrera” de seguridad es controlada por el usuario, el cual al ignorar los riesgos a los que se enfrenta

y sus tipos, es el causante directo de la mayoría de infecciones o ciberataques exitosos, tanto en las organizaciones como en sus propios dispositivos y/o activos.

De acuerdo a la publicación "*Primera gran encuesta TIC 2017*" (2017) de MINTIC del gobierno de Colombia, el 68% de las empresas cuentan con acceso a internet, y de estas, el 83% no cuenta con protocolos de seguridad informáticos, lo que permitió ese mismo año un historico de aproximadamente 198 millones de ataques registrados y más de 542 mil incidentes informáticos. Esto evidencia claramente que las empresas no estan considerando los riesgos y que por ende, los usuarios de los sistemas tampoco no aplicarían las buenas prácticas recomendadas para navegar por internet y/o hacer uso de los sistemas involucrados.

1.2 FORMULACIÓN DEL PROBLEMA

Actualmente las organizaciones se han enfocado en el fortalecimiento de las infraestructuras y sistemas de software para garantizar la protección de su información, destinado de esta manera, recursos en la adquisición de hardware y software que provean a sus organizaciones de un alto grado de seguridad informática.

Sin embargo, existe otro aspecto que se ha descuidado en la mayoría de los casos o no se ha sabido trabajar para lograr incluirlo dentro de los planes y elementos que componen la Ciberseguridad de una entidad, se trata de los usuarios del sistema. De acuerdo con el informe anual publicado por las organizaciones "We are Social (2020)" y "Hootsuite (2020)", el "Digital 2020 Global Overview Report", actualmente existen alrededor de 4.5 billones de personas conectadas a internet, esto es cerca del 59% de la población de todo el mundo; lo que no solo representa el constante crecimiento de las redes y el uso de internet, sino que también representa el aumento de amenazas informáticas y de usuarios incautos que pueden caer sin siquiera saber lo que ocurre.

Lo anterior quiere decir, que a medida que las redes de internet se expanden y mejoran su accesibilidad, las amenazas informáticas también aumentan, puesto que las posibilidades de éxito de un riesgo informático aumentan según el número de usuarios de la red y según la capacidad y conocimientos de estos frente a dichas amenazas. Por esta razón, las organizaciones requieren en la actualidad que los usuarios de sus sistemas, conozcan las buenas prácticas de seguridad informática y las amenazas a las cuales se enfrentan al navegar en la web o usar un dispositivo móvil para compartir información incluso en sus redes sociales; pero esto es únicamente posible de realizar implementando metodologías que permitan reconocer esos riesgos a los que sus usuarios son más propensos a experimentar y así se pueda implementar una serie de controles que permitan cerrar cualquier posible brecha de seguridad generada por un usuario del sistema y que además dé el soporte y capacitación necesarias sobre el uso de las redes y los riesgos presentes en las mismas, ya que si el usuario de los sistemas no es formado correctamente para enfrentar algunos de estos riesgos y/o la organización no cuenta con estrategias metodológicas adecuadas para la gestión de riesgos, tarde o temprano se creará una puerta trasera que permitirá vulnerar todo el sistema.

De manera que una organización que pretenda establecer unas políticas de seguridad, debe en primera instancia identificar algunas metodologías importantes que permitan determinar los riesgos a los que se exponen los usuarios de sus sistemas para establecer políticas y procesos de capacitación adecuados para su personal; por lo que este sería el principal elemento a considerar, la implementación correcta de metodologías que permitan evaluar los riesgos a los que se exponen los usuarios con el fin de establecer acciones y controles que permitan mitigar estos riesgos.

2 JUSTIFICACIÓN

Cuando se implementa una metodología de gestión de riesgos, se implementan numerosos controles para el hardware y el software, así mismo algunas metodologías consideran la implementación de políticas de seguridad informática y políticas de uso de los recursos; estas políticas si bien tienen la finalidad de proporcionar elementos que fortalezcan la seguridad de la información, se ven incompletas si no se tiene en cuenta el factor humano, el cual, es un elemento fundamental en la seguridad informática y debe ser soportado y tenido en cuenta en toda la implementación del sistema de gestión de la seguridad informática.

Muy pocas veces se ha evaluado el entorno de riesgo al que se exponen los usuarios y se los ha capacitado para conocer y enfrentar dichas amenazas, ya que incluso, una aparente mínima acción como la publicación de una fotografía de entorno laboral en un sitio social puede permitir la construcción de una amenaza informática a través de las técnicas de ingeniería social y recolección de información. De manera tal que determinar a través la implementación correcta de metodologías de mitigación de riesgos, una estrategia de identificación ágil que permita evaluar los riesgos a los que se exponen los usuarios de los sistemas y establecer temas de capacitación básicos fundamentales, son un factor de extrema urgencia que se pretende estudiar en el presente trabajo teniendo en cuenta un enfoque principal a los usuarios quienes por medio de sus acciones podrían mitigar riesgos o generar un riesgo informático mayor.

Según el libro “Qué es la seguridad informática” Hugo D. Scolnik (2014). La sociedad vive en una guerra constante entre quienes atacan los sistemas y quienes los defienden, esta es una guerra silenciosa en la cual las víctimas son aquellas organizaciones y personas que de una forma u otra no dieron la atención necesaria a este asunto de la seguridad informática, aquellos que ignoran los temas o que piensan que por no tener gran cantidad de recursos económicos no serán el objetivo de ningún atacante; pero lo cierto es que

los ciberdelincuentes pueden lograr su cometido en muchos usuarios de los sistemas que ignoran elementos tan básicos como el uso de contraseñas seguras, aquellos que de contraseña en sus bancos o cajeros, usan su fecha de nacimiento, de un familiar o de compromiso, estas son las contraseñas más comunes y por lo tanto las más vulnerables. La integración adecuada de metodologías de evaluación de riesgos implementados por una organización, deben considerar el factor humano ya que este es considerado como el eslabón más débil de la seguridad informática, y teniendo en cuenta el creciente riesgo generado por usuarios maliciosos de la web, y el uso masivo de las redes informáticas, software de sistema y aplicaciones móviles en las cuales se han distribuido miles de amenazas informáticas, se ha generado una necesidad inmediata implementar estrategias de seguridad informática que permitan fortalecer este actor fundamental en las redes y los sistemas de la organización.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Estructurar un documento con los principales riesgos y amenazas informáticas a las que se pueden enfrentar los usuarios de los sistemas en empresas públicas o privadas, a partir de la aplicación de la metodología de evaluación de riesgos MAGERIT enfocándose en amenazas y vulnerabilidades identificadas, tendientes a la generación de estrategias de capacitación acompañadas por buenas prácticas.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar riesgos y amenazas informáticas más relevantes que enfrentan los usuarios de los sistemas en la actualidad, a partir de estudios realizados en Colombia y en el mundo.

- Determinar el impacto de los riesgos y amenazas informáticas más habituales que pudieran ser materializados por los usuarios del sistema, tendiendo como base la metodología MAGERIT.

- Reconocer estrategias de mitigación de riesgos informáticos para los usuarios de los sistemas a partir del análisis de vulnerabilidades identificadas enfocándose en la metodología MAGERIT.

- Proponer estrategias de capacitación acompañadas por buenas prácticas de seguridad informática en el uso de los sistemas e internet, teniendo en cuenta los objetivos anteriores.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La seguridad informática comprende un esfuerzo conjunto de casi todo el mundo con el objetivo de proteger la información digital de cada usuario activo de internet o del que al menos una vez haya pisado este mundo digital y a su vez haya dejado una huella en él. Se entiende por seguridad, como la ausencia de un riesgo en un entorno que provea los elementos de protección y bienestar, ausente de cualquier indicio de amenaza que pueda perjudicar dicho bienestar.

La seguridad por tal motivo se enfoca en la gestión de riesgos, de manera que sea necesario el hecho de identificar las amenazas, estudiarlas y establecer acciones que permitan mitigar dichos riesgos encontrados. Así pues, se entiende que existen varias formas de tratar los riesgos, entre ellos se puede resaltar:

- ✓ Prevención del riesgo.
- ✓ Mitigación del riesgo.
- ✓ Trasferencia del riesgo.
- ✓ Aceptar el riesgo.

Puesto que ningún sistema es completamente seguro, según el profesor de computación Eugene Spafford "*El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de hormigón y sellado en una habitación recubierta de plomo con guardias armados…. y aun así tengo mis dudas*" marzo 1998[34], se requiere de un esfuerzo combinado entre todos los recursos y actores de la organización y los sistemas para

[34] SPAFFORD Eugene. "Computer Recreations of Worms, Viruses and Code War". Scientific American. marzo 1998, p. 110

generar un estado de mayor seguridad aun cuando de cualquier forma siempre existirá el modo de que se genere una pequeña amenaza mientras los sistemas estén activos o de alguna forma sean accesibles.

Por lo que realizar un análisis de riesgos no solo implicaría la implementación de software y hardware, sino que también requerirá de analizar el entorno en el que se desempeñan los usuarios de los sistemas, éste entorno a su vez, se mantiene siempre actualizado y por supuesto agresivo.

Sin embargo, como se mencionó anteriormente, la seguridad informática requiere del trabajo y disposición conjunta de los elementos que interactúan entre sí para generar la información, la cual a su vez se reproduce a tasas exponenciales y de momento no se prevé un final o decrecimiento. De acuerdo con un estudio realizado en 2020 por la empresa consultora Cumulus Media[35], en la que se estudia el comportamiento de los usuarios en internet (ver figura 1), se encontró que solo en redes sociales, se envían millones de mensajes, lo que genera un crecimiento en la demanda de recursos informáticos y ofrece un vistazo de cuan activos se puede llegar a ser en este universo.

Ahora a su vez, tanto usuarios como empresas han reportado de manera cada vez más frecuente un ciberataque, pasando de tener 7523 casos reportados al Centro Cibernético Policial en 2015, a más de 30 mil casos registrados en el 2019 sobre incidentes de Ciberseguridad en el país[36].

---

[35]Cumulus Media. (2020). [sitio web]. Reporte Anual – Sprout Social. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.annualreports.com/Company/sprout-social-inc

[36]Policía Nacional de Colombia. [sitio web]. Tendencias Cibercrimen Colombia 2019-2020. [Consulta: 4 de septiembre 2020]. Disponible en:
https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Figura 1. Internet en 60 segundos

Fuente https://lorilewismedia.com/

Por ende, es evidente que conformo internet crece y se expande, la información y las amenazas informáticas también lo hacen, dejando a razón de cada persona u organización, la importancia a través de la adopción de estrategias y buenas prácticas que puedan adoptar para encontrar esa seguridad informática. Cuando se evalúa la seguridad informática de una entidad, un sistema u otro, se debe contemplar la clasificación de estos en cuatro partes importantes para realizar un análisis adecuado de los riesgos que cada uno de ellos enfrenta[37]:

[37] ROMERO C. Martha, et al. Introducción a la seguridad Informática y el análisis de vulnerabilidades. Ed. Área de Innovación y Desarrollo,S.L. 2018. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

- ✓ Los usuarios.
- ✓ La información.
- ✓ La infraestructura
- ✓ Los Sistemas.

Los usuarios, quienes como se ha definido en este trabajo, son sin duda algunas el eslabón más débil de la cadena en lo que respecta a seguridad informática; pues estos son mayormente susceptibles a su entorno, respondiendo a emociones que motivan de una forma u otra sus acciones, permitiendo considerarse en ellos un mayor riesgo ante la manipulación de las tecnologías bien sea por cuestiones de desinterés, falta de precaución, desinformación o por intereses personales.

La información, la cual es el fundamento de toda la seguridad informática, la cual contiene un valor incalculable tanto personal como organizacionalmente, pues es esta la que se debe proteger en todos sus ciclos de vida, de generación y de almacenamiento. La infraestructura, la cual contiene todos los dispositivos físicos que componen la red y con los cuales interactúan a diario los usuarios de manera directa e indirecta, que requieren una protección y control de accesos físicos que asegure su uso únicamente al personal destinado.

Los sistemas, que en consideración, comprenden no solo el software de aplicación como por ejemplo las herramientas ofimáticas, o el sistema operativo de los equipos, sino también comprenden todos los protocolos que vienen con la implementación logística de una red informática y su programación Aunque en una organización con grandes implementaciones tecnológicas, la mayoría de los controles aplicados en el ámbito de la seguridad y gestión de riesgos informáticos contemplan un proceso de capacitación constante al personal de la organización[38], muy pocas veces se lleva a cabo una

[38] RUGE Jeison. Metodología para identificación y valoración de riesgos. 2012. [Consulta: 4 de septiembre 2020]. Disponible en: http://polux.unipiloto.edu.co:8080/00000744.pdf

implementación real y un estudio constante de estas capacitaciones a nivel administrativo. Esto permite generar una brecha que se convierte en una vulnerabilidad importante de los sistemas, pues que cabe recordar que el usuario es quien interactúa directamente con los sistemas y la información, la cual también es encargado de producir.

Es de conocimiento general entre los que estudian el campo de la Seguridad Informática, que existen muchos factores que se deben tener en cuenta a la hora de realizar una implementación un sistema de gestión de la seguridad informática [39]; muchas veces se piensa en primera instancia en la implementación del software o de su correcta configuración para establecer una seguridad informática robusta; otros podrían considerar la implementación del hardware adecuado que se encargue de realizar un monitoreo de la red y el comportamiento de los dispositivos entre otros; ciertamente todas las anteriores son consideraciones totalmente respaldadas y necesarias para garantizar la seguridad de nuestros sistemas.

Por lo anterior, la mayoría de las investigaciones se han centrado en estos elementos importantes en del área: información, sistemas, e infraestructura, siempre con el objetivo de determinar el mejor rendimiento, la mejor respuesta, la mayor estabilidad o el mejor alcance. Sin embargo, es importante profundizar también en la parte humana, el usuario, quien es pieza fundamental permitir mejorar la seguridad informática tanto en una organización como en su uso personal, puesto que, vista desde una perspectiva general, la seguridad informática, en sus buenas prácticas, le debe importar a cualquiera que tenga un equipo celular, o una cuenta bancaria[40]. Teniendo en cuenta lo anterior, es necesario dedicar un momento para analizar cuáles son los elementos que intervienen en la comunicación digital; así pues, se considera a grandes rasgos, que para transmitir un mensaje se necesita de un emisor, un medio o canal y un receptor.

---

[39] INTECO. Implantación de un SGSI en la empresa. 2020. [Consulta: 9 de septiembre 2020]. Disponible en:: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[40] SCOLNIK, Hugo D. Qué es la seguridad Informática. 2014. 1ra ed. Ciudad autónoma de Buenos aires. Argentina. Ed. Paidós

Hoy en día la seguridad informática se centraliza en nuestros equipos y el software que lo componen o que interactúan con ellos para llevar y recibir nuestros mensajes a través de los medios cableados o inalámbricos, cuyos datos usualmente viajan encriptados o cifrados, con lo cual se da prioridad a la actualización de los sistemas y el hardware disponible. Entonces se podría plantear la siguiente pregunta: "¿De qué o de quiénes depende garantizar la seguridad informática?, ¿hay que enfocarse en el software o el hardware?, o tal vez, otro elemento.

Como se mencionó inicialmente, si bien el software y el hardware son importantes en esta ejecución de tareas, también y en muchos casos es más importante el usuario del sistema, quien en es el único que finalmente puede liberar o evitar una amenaza informática en nuestros sistemas; de modo que las entidades deben identificar y reconocer metodologías que sugieran pasos para la recolección de información y evaluación de los resultados sobre las amenazas más importantes a las cuales se exponen los usuarios, y que permitan determinar de la profundidad de conocimientos básicos e importantes que necesariamente debe tener cualquier persona que labore en una entidad y que haga uso de las redes o los sistemas de la entidad, para finalmente establecer un método de capacitación y soporte adecuados para que el usuario del sistema tenga una mejor respuesta ante posibles amenazas informáticas.

Según el gran informático y hacker Kevin Mitnick: "Las organizaciones gastan millones de dólares en cortafuegos y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de la seguridad: la gente que usa y administra las computadoras."s.f. Lo anterior no solo es una idea cualquiera, desde hace mucho tiempo se ha considerado el error generado por el usuario, incluso existe una referencia popular que ha nombrado estos tipos de fallos como "error de capa 8" haciendo alusión a un octavo nivel en el modelo OSI en el cual se considera al usuario como un elemento de interacción con el sistema que puede generar errores en el sistema, o en nuestro caso a considerar, un usuario que pueda generar o materializar las

amenazas informáticas a las que todos los días se está expuesto en cualquier sitio donde haya una conexión a una red informática.

Es tanto así, que la mayoría de los ataques informáticos son posibles por la interacción del usuario con el sistema, según Kevin Epstein, vicepresidente de Threat Operations para Proofpoint. "*Más del 99% de los ciberataques depende de la interacción humana…*"[41] (2019. Proofpoint). Lo que quiere decir es en efecto, que uno de los elementos fundamentales y que requieren de un plan de acción por parte de los profesionales en este campo, es la identificación de riesgos, implementación de metodologías de evaluación, capacitación y el soporte adecuado a los usuarios del sistema, con el fin de mitigar un riesgo latente ante el crecimiento exponencial de amenazas informáticas a las que están expuestos cada uno de los usuarios y por ende todos los sistemas manipulados.

La idea central considera inicialmente identificar los riesgo en los cuales las metodologías más óptimas propuestas para gestionar la seguridad informática en las organizaciones, permitiendo sondear el conocimiento informático que dispone el personal de una empresa o entidad, posteriormente determinar los riegos a los cuales se exponen los usuarios en la actualidad, como por ejemplo el uso de redes sociales en entornos laborales, y finalmente en proponer el desarrollo de soluciones, técnicas y/o metodologías apropiadas que incluyan implementación de capacitaciones y soporte continuo a los usuarios del sistema para reforzar la respuesta de los mismos ante la posible interacción con una amenaza informática. Se pretende además desarrollar un método estándar de recolección y evaluación de información de vulnerabilidades en el entorno laboral y social por medio de la implementación de técnicas de capacitación y seguimiento, que pueda ser aplicado en cualquier entidad o empresa, con el fin de generar estrategias de resolución de riesgos informáticos.

[41] EPSTEIN Kevin. SUNNYVALE, Calif., Sept. 09, 2019 (GLOBE NEWSWIRE) -- Proofpoint, Inc. [Consulta: 10 de septiembre 2020]. Disponible en: https://www.globenewswire.com/

Finalmente, cabe mencionar que la aplicación de una metodología que permita identificar qué tan vulnerables se es en el talento humano de una organización, es algo que se hace cada vez más necesario teniendo en cuenta el ritmo acelerado al que crecen las denuncias por robos informáticos y la creciente demanda por la implementación de dispositivos y elementos electrónicos para el desarrollo de labores como el teletrabajo, lo cual permitirá ayudar a mitigar los riesgos de amenazas informáticas a las que se está expuesto y por ende a los propios sistemas.

4.2 MARCO CONCEPTUAL

4.2.1 Definición de conceptos

Para el desarrollo de la presente monografía se consideran algunos de los siguientes conceptos que se relacionan con el tema tratado:

4.2.1.1 Virus informático: Se define como una aplicación o fragmento de código en lenguaje base, desarrollado con el fin de deteriorar el buen funcionamiento de los sistemas, con la capacidad de corromper los archivos del sistema, acaparando recursos, modificando datos o alterando archivos perjudicando el buen funcionamiento del sistema[42]. Se pueden clasificar según el tipo de malware y las actividades que realiza en los sistemas, como por ejemplo aquellos con capacidad de copiarse a sí mismos en diferentes sitios que incluyen carpetas, dispositivos o sectores del sistema a infectar, todo ello sin el consentimiento o autorización del usuario.

4.2.1.2 Malware: El malware (abreviatura de “software malicioso”) se considera un tipo molesto o dañino de software destinado a acceder a un dispositivo de forma inadvertida, sin el conocimiento del usuario. Los tipos de malware incluyen spyware (software espía), adware (software publicitario), phishing, virus, rootkits,

[42] ÁLVAEZ P, et al. Virus Informáticos. Universidad de la Coruña. 2008. [Consulta: 11 de septiembre 2020]. Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

troyanos, gusanos, rootkits, ransomware y secuestradores del navegador[43].

4.2.1.3 Ransomware: Es un tipo de software malicioso cuyo objetivo es “secuestrar” información de una computadora[44] (a veces, el disco duro entero), con el objetivo de exigir a cambio dinero, informando al usuario que tiene un tiempo límite para realizar el pago o los archivos quedarán cifrados para siempre. Lo cual presiona al usuario a tomar una decisión apresurada a fin de no perder su información, sin embargo, el descifrado puede al final darse o no aún con el pago del rescate.

4.2.1.4 Vishing: Es una práctica criminal muy utilizada actualmente en la cual se hace uso del Protocolo Voz sobre IP (VoIP) y de técnicas de ingeniería social para engañar a personas[45] y obtener cualquier tipo de información delicada como puede ser información financiera o familiar, u otro tipo de información útil para el robo de identidad, descifrado de contraseñas o recuperación de estas.

4.2.1.5 APT: Por sus siglas en inglés “Advance Persistent Threat”: es un conjunto de técnicas que se implementan en un sistema como parte de un elaborado ciberataque que tiene proyección a largo plazo[46] (usualmente superan las semanas o los meses antes de ser descubiertos). De tal manera que se realiza una infiltración sigilosa de los sistemas o las redes informáticas, así pues, le es posible a los ciberdelincuentes extraer información constantemente sin que se sospeche de ello.

---

[43] UNIVERSIDAD JAÉN. Guía de Seguridad UJA Software malicioso. 2018. [Consulta: 13 de septiembre 2020]. Disponible en: https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%203.%20Malware.pdf

[44] ESET. [Sitio web]. Todo sobre el Ransomware. 2016. [Consulta: 13 de septiembre 2020]. Disponible en: http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo_Sobre_Ransomware.pdf

[45] BANCO SANTANDER. [Sitio web]. ¿Qué es Phishing, Smishing y Vishing? ¿Cómo protegerse?. [Consulta: 13 de septiembre 2020]. Disponible en: http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo_Sobre_Ransomware.pdf

[46] WRIGHTSON T. Advanced Persistent Threat Hacking. 2015. [Consulta: 13 de septiembre 2020]. Disponible en: http://index-of.es/Varios/Advanced%20Persistent%20Threat%20Hacking,%20The%20Art%20&%20Science...pdf

De manera tal que este tipo de ataques van acompañados de varias estrategias que permiten infiltrarse usualmente en una organización, institución o gobierno para obtener

información de manera sigilosa sin permitir evidenciar su presencia ni generar cambios evidentes en los sistemas permaneciendo oculto constantemente, puesto que, a mayor permanencia, más información podrá ser capturada.

Uno de los mejores ejemplos de APT es el virus Struxnet, el cual fue capaz de instalarse en los sistemas SCADA de algunos reactores nucleares en Irán, las cuales, por razones obvias, tienen implementados altos sistemas de seguridad, sin embargo, la infección de este ataque provocó grandes daños a los sistemas e incluso logró dejar sin corriente a parte del país[47].

Aunque estas amenazas estaban enfocadas inicialmente a grandes organizaciones, la digitalización y su creciente implementación en todo tipo de empresas junto con la exposición que se genera al permitir el traslado de información a través del uso de dispositivos como smarthphones y portátiles, ha permitido que este tipo de amenazas se instalen en todo tipo de organizaciones e incluso a personas naturales quienes realizan intercambio de datos entre sus equipos corporativos y personales, teniendo en cuenta además que muchas de las organizaciones no están preparadas para afrontar la amenaza o incluso desconocen su existencia.

4.2.1.6 Spear Phishing: Considerada como una modalidad de estafa a través del correo electrónico o de comunicaciones dirigidas a personas, organizaciones o empresas específicas. Tiene como objetivo el robo de información por medio del uso e instalación de software malicioso que espía o copia información del usuario. Funciona así: A un usuario le llega un correo electrónico aparentemente de una fuente segura como una entidad reconocida, al acceder a la solicitud del correo, se dirige al usuario a un sitio web falso que contiene malware, el cual se instala

[47] RIVADENEIRA E. STUXNET, La primera ciberarma. 2016. [Consulta: 13 de septiembre 2020]. Disponible en: https://revistamarina.cl/revistas/2016/2/efrederickr.pdf

en el sistema e inicia una recopilación de información, por ejemplo, de todo lo que se digite.

Hacking Ético: El hacking ético es aquel en el que se aplican ensayos o pruebas de vulneración de los sistemas o los recursos, bien sea por procesos de auditoría interna o externa, o test periódicos de seguridad, con el objetivo de encontrar vulnerabilidades o fallos de seguridad que pudieran ser explotados por un atacante real del sistema.

El Hacking ético de ninguna forma se relaciona con cualquier tipo de estafa realizada por internet a través del uso de las TIC o de los recursos informáticos con fines ajenos a los de la empresa. Al realizar hacking ético, todas las vulnerabilidades encontradas son reportadas a la organización con el objetivo de tomar medidas que permitan eliminar, mitigar o transferir el riesgo de que se materialice y así conservar un sistema más seguro[48].

4.2.1.7 Spoofing: El Spoofing se define como la suplantación de información El spoofing es una técnica de hacking que se basa en la suplantación de identidad de una fuente de información que el receptor cree conocida o segura, que se realiza con el fin de capturar datos o información de la víctima[49]. Existen numerosas técnicas de spoofing que implementan distintos software o dispositivos hardware, incluso las que se realiza por medios telefónicos que permiten incluso falsificar otra identificación de llamada. En redes informáticas se puede mencionar:

Spoofing IP: Consiste en realizar una configuración del traductor de direcciones de red NAT para que al momento de escribir o editar el paquete de datos no use la dirección IP

[48] SANCHEZ M. Hacking Etico: Impacto En La Sociedad. 2015. [Consulta: 13 de septiembre 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4919/00005096.pdf?sequence=1&isAllowed=y

[49] ZAPATA F. Detección de ataques de spoofing. 2013. [Consulta: 14 de septiembre 2020]. Disponible en: http://bibing.us.es/proyectos/abreproy/12163/fichero/PFC.pdf

propiamente asignada a la interfaz de red, si no que realice la modificación de acuerdo con un parámetro en este caso, de acuerdo a una IP que se le indique manualmente.

Spoofing DNS: Mediante el cual se modifica en el servidor DNS para que el tráfico se redirija a otros sitios web diferentes al oficial; esto se logra al modificar para determinado nombre de dominio la IP asignada, así, tras el equipo consultar el nombre de dominio, redirigirá el tráfico a la IP registrada en su tabla (previamente falseada), generando un riesgo para el usuario que podría revelar información privada.

Spoofing de Email: Haciendo uso de logotipos, sellos, estilos y emblemas, se genera un correo falso en suplantación de una entidad conocida como por ejemplo bancos, entidades públicas o incluso gobiernos, que se envía a una víctima con el fin de que esta acceda a la solicitud de información generada en el correo, acceda a sitios web malicioso o descargue archivos con malware.

4.3 MARCO LEGAL

El marco legal vigente en Colombia establece leyes sobre la protección de la información y los datos, donde se describen conductas y acciones penales a las que se puede incurrir por el mal uso de conocimientos informáticos, lo cual también es tratado por el código de ética profesional o deontológico para profesionales de la Ingeniería, donde se detallan los elementos causales de sanciones por parte del COPNIA y aquellas actividades que incurren el violación a la legislación Colombiana en el marco de la informática y la ingeniería.

Inicialmente se puede resaltar que el uso de los conocimientos informáticos de un profesional en ingeniería con fines ilegales, se consideran faltas graves al código de ética dispuesto por el COPNIA para Ingenieros y sus ayudantes en el cual de acuerdo con el

Código de Ética - ley 842 de 2003[50], un ejercicio ilegal como el phishing podría vulnerar los siguientes artículos:

- Artículo 32: Sobre prohibiciones generales a los profesionales, en el literal ***G***, el causar intencional o culposamente daño o pérdida de bienes, elementos, equipos, documentos por razón del ejercicio de su profesión, puede ser causal de suspensión de la tarjeta profesional para la profesión de su área.

- Artículo 53: En su literal **A,** donde se considera una falta grave al código y constituye una causal de cancelación de la matrícula profesional, el derivar de manera fraudulenta (independientemente del mecanismo empleado) el patrimonio de otra parte, generando de manera directa o indirecta consecuencias graves o pérdidas a la parte afectada.

También en el apartado sobre el tratamiento de la Información y Deber de Secreto, se podría incurrir en una falta grave en un ejercicio ilícito como el phishing, ya que se especifica en su numeral "***5.6***" el no utilizar los conocimientos informáticos avanzados adquiridos para saltarse ningún tipo de protección de seguridad, ya sean de la propiedad intelectual o de acceso a sistemas informáticos independientemente de si se emplean herramientas o software informático, o habilidades derivadas de la aplicación de ingeniería social que le permitan deducir o procesar las credenciales de acceso a un sistema o a la información, para ser vulnerado en cualquier aspecto (privacidad, disponibilidad, autenticidad).

Por otro lado, se debe tener en cuenta la legislación nacional, la cual castiga de manera efectiva cualquier intento o ejecución de actos ilegales a través del uso de las TIC; para lo anterior, el Congreso de la República de Colombia ha dispuesto una serie de

[50] COPNIA. [Sitio web]. Ley 842 de 2003. Diario Oficial No. 45.340. [Consulta: 18 de septiembre 2020]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

normativas a través de la Ley 1273 del 5 de enero de 2009[51]. Así pues, suponiendo una intrusión en un sistema de una organización, que implique una posible infiltración a los equipos informáticos, se puede decir que se incurre en varias faltas, las cuales de acuerdo con la ley 1273, se verían vulnerados algunos de los artículos, por ejemplo:

- 269A: Que castiga el acceso no autorizado al sistema informático, lo que pueden resultar en penas de 48 a 96 meses de prisión, además de multas que varían desde los 100 a 1000 SMLV.
- 269B: Al afectar o alterar el buen funcionamiento del sistema, lo que incurre en multas desde los 100 a 1000 SMLV y penas de 48 a 96 meses.
- 269C: Si se intercepta datos informáticos para que pudiesen lograr el acceso al sistema, lo que incurre en multas desde los 100 hasta los 1000 SMLV y prisión de 48 hasta 96 meses.
- 269D: Puesto que se genera un deterioro a la calidad del sistema, incurriendo en multas desde los 100 a 1000 SMLV y penas de 48 hasta 96 meses.
- 269E: Si se usa software malicioso para acceder a un sistema, lo que incurre en multas desde los 100 a 1000 SMLV y penas de 48 hasta 96 meses de prisión.
- 269J: Al realizar cualquier copia, modificación o eliminación de datos, que penaliza la transferencia no consentida de activos de información lo que incurre en penas de 48 a 120 meses de prisión y multas entre 200 a 1500 SMLV.

De esta manera se identifica que el acceso ilícito a un sistema informático sin autorización y con mucha más razón si se roba cualquier información o si se hace uso de software con fines maliciosos para la interceptación deliberada e ilegítima de datos informáticos sin autorización, se consideran faltas graves castigadas nacional e internacionalmente; puesto que el fraude informático se considera hoy en día una de las actividades criminales más realizadas alrededor del mundo.

[51] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. De la protección de la información y de los datos. Bogotá. Colombia. 2009. [Consulta: 14 de septiembre 2020]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

5 DISEÑO METODOLÓGICO

El desarrollo del presente trabajo, se basa en el diseño metodológico cualitativo, en el cual se iniciara por el proceso de exploración de las temáticas referentes a las vulnerabilidades informáticas que pueden experimentar los usuarios del sistema, para ello se realizará una aproximación a los temas relacionados más importantes que en la actualidad los usuarios y los sistemas deben afrontar o se encuentran más expuestos; posteriormente se realizará un análisis explicativo con el propósito de identificar características, propiedades o regularidades que permitan entender el modo de operación de las amenazas encontradas y finalmente se realizará una serie de recomendaciones y buenas prácticas de la mano de las metodologías de evaluación de riesgos más importantes para cada una de las problemáticas encontradas en el desarrollo de las temáticas involucradas. Para lo anterior, se hace uso de recursos bibliográficos que permiten documentar los riesgos y amenazas más comunes, permitiendo realizar un análisis documental y estadístico de la frecuencia de materialización de dichas amenazas con la ocurrencia de acciones realizadas por los usuarios de los sistemas.

Finalmente, cabe resaltar que el proceso investigativo hace uso prioritariamente de fuentes estadísticas que muestran una estado actual del país, por lo que se presentarán registros estadísticos recolectados por el gobierno Colombiano y sus entidades encargadas de vigilar, mantener y guiar el uso de las tecnologías de la información y las comunicaciones[52] (MinTIC), aunque por supuestos que se tendrán en cuenta también estudios a nivel global sobre el crecimiento tecnológico y la afectación de la seguridad informática así como de la correcta gestión de esta y el esfuerzo general por capacitar y fortalecer el que se conoce como el eslabón más débil de la seguridad informática, el usuario.

---

[52] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Iniciativas del sector TI en Colombia. 2020. [Consulta: 14 de septiembre 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Iniciativas/

6 DESARROLLO DE LOS OBJETIVOS

En primera instancia cabe resaltar que la seguridad informática tiene inmerso en su implementación, los controles y políticas que se adecuan a cada elemento que conforma el sistema informático; para ello hay que pensar que la seguridad informática se basa (a grandes rasgos) en los sistemas de seguridad en redes, bases de datos, páginas web, sistemas operativos, criptográficos, entre otros que se mencionan a continuación:

- Seguridad en redes informáticas: Esta comprende tanto las redes de datos como las de telecomunicaciones, independientemente de cuál sea el medio de transmisión[53]. Para implementar recursos de seguridad en estos sistemas de redes, es necesario tener en cuenta tanto la infraestructura de la red, hasta los parámetros característicos de la configuración de red que se les da a los dispositivos de comunicación, ya que aplicaciones como la segmentación de red permiten reforzar la red ante posibles intrusiones.

  Es necesario resaltar que la red informática, juega un papel muy importante en la seguridad de la información ya que esta permite la conexión a los sistemas de la organización, las bases de datos, Data Warehouse, servidores, etc., por lo que alojan y ayudan a administrar la información generada. Por lo que es necesario conocer la topología y/o estructura tanto física como lógica que identifique claramente el funcionamiento de la red, esto permite determinar qué elementos implementar para mejorar su funcionamiento a través de controles, políticas y configuraciones adecuadas según los requerimientos y características de la misma, puesto que de desconocer su estructuración, todos los datos que se transfieran a través de esta se encuentran vulnerables a distintas técnicas de hacking como el sniffing, el cual permite capturar paquetes de datos que viajan por la red de forma inalámbrica o

[53] SÁNCHEZ R. Seguridad en Redes. s.f. [Consulta: 16 de septiembre 2020]. Disponible en: https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

cableada, permitiendo el acceso a datos, contraseñas de usuarios o logrando escalar privilegios.

- Seguridad en BD - Bases de Datos: Las bases se definen como un elemento fundamental para el almacenamiento de la información y por ende, para toda la organización, debido a que es en ellas donde se agrupa y gestiona todos los datos encontrados en forma de registros de información que pueden ser de cualquier tipo y valor, convirtiéndose en el objetivo principal de los ataques informáticos.

  De manera que la seguridad en las bases de datos debe incluir un estudio puntual de todos los sistemas y los proceso involucrados, así como de los usuarios que interactúan con ellos[54], por lo que el objetivo principal de la implementación de la seguridad en las BD, será controlar el acceso y los permisos que se tengan sobre las mismas para las acciones de consulta, registro, modificación y borrado, así como también determinar herramientas, estrategias y prácticas que permitan proteger las bases de datos de consultas o acceso no autorizados.

- Seguridad en Páginas Web: Hoy en día, internet ofrece millones de páginas web a las cuales se puede acceder, desde sitios sociales y de comercio hasta plataformas del estado o de gobiernos internacionales, debido a que una de las tendencias más grandes en la actualidad, es la de ofrecer servicios y recursos a través internet en los sitios web; sin embargo, se debe tener en cuenta que cuando un sitio se encuentra en línea o sobre la web, la cantidad de usuarios que puedan consultarlo puede rondar los millones en un mismo día, esta exposición convierte a las páginas web como otro de los objetivos principales de ataques informáticos, que incluyen técnicas de spoofing en intentos de suplantación con el objetivo de robar información, por supuesto que de

---

[54] DÍAZ V. Seguridad en Bases de datos y aplicaciones Web. s.f. [Consulta: 4 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/62886/4/Seguridad%20en%20bases%20de%20datos_M%C3%B3dulo%201_Introducci%C3%B3n.pdf

lograrse con éxito un ataque de este tipo, trae consigo el desprestigio que genera haber sido víctima de este tipo de intrusiones[55]. De manera tal que, si se tiene cualquier entono montado sobre la web, es necesario establecer controles como por ejemplo la validación de los datos permitidos en los formularios con el objetivo de evitar inyección de código.

- Seguridad en Sistemas Operativos: Los sistemas operativos hoy en día tiene un alcance mucho mayor al de "los sistemas que tienen las computadoras de los usuarios", hoy en día los sistemas operativos que proteger, se encuentran tanto en equipos de cómputo, como servidores y teléfonos inteligentes. Por este motivo se debe ampliar el concepto y se debe tener en cuenta que cada configuración, control, normativa u reglamento, debe cubrir todos los dispositivos de la entidad que tengan un sistema operativo, en ellos es necesario configurar el consumo de recursos, la gestión de cuentas y el modo de conexión entre otras cosas, lo cual tiene el propósito de evitar las famosas "puertas abiertas" o accesos vulnerables a intrusiones a través de los puertos de comunicación que se tengan habilitados[56].

  En los sistemas operativos es muy importante la gestión de usuarios, ya que en estos de define el control que tenga cada uno de ellos para realizar cambios en los equipos, obtener acceso a rutas de red y recursos como impresoras o servidores almacenamiento, al igual que el privilegio para realizar configuraciones especiales como el acceso remoto entre otros. Si bien, todas estas opciones permiten dar soporte adecuado a los usuarios y el acceso rápido a los servicios o recursos compartidos, pueden generar una gran amenaza si no se tiene en cuenta las correctas configuraciones para su uso, recordando que no hay sistema totalmente seguro, pero

[55] INCIBE. [Sitio web]. Protección de la página Web. s.f. [Consulta: 18 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/62886/4/Seguridad%20en%20bases%20de%20datos_M%C3%B3dulo%201_Introducci%C3%B3n.pdf

[56] LÓPEZ, G. Servidores seguros. 2020. [Consulta: 18 de septiembre 2020]. Disponible en: https://pccito.ugr.es/~gustavo/ss/teoria/seguridad/seguridad.pdf

es posible reducir los riesgos si se implementa de manera adecuada cada uno de estos sistemas; de igual manera es necesario configurar los servidores, con el objetivo de permitir o denegar servicios, protocolos de comunicación o acceso a rutas según el perfil y rol de cada usuario.

- Sistemas Criptográficos: La criptografía es sin duda una de las técnicas de seguridad con respecto al cifrado que se debe tener muy en claro y aplicada de manera obligatoria, especialmente en los casos en que se realice un trasporte de información, como por ejemplo claves de acceso o archivos importantes de una organización. El objetivo de usar una encriptación o cifrado de datos, es lograr codificar los mensajes/archivos a enviar, lo cual evitará que el contenido sea expuesto o visualizado por cualquiera diferente al destinatario[57], evitando de esta manera que, si se llegase a copiar el archivo o en el caso de la red a capturar un paquete de datos, este sea leído perdiendo su privacidad y poniendo en riesgo la seguridad de la información.

  La criptografía tiene varias aplicaciones directas, como en las redes de datos sobre protocolos de seguridad y cifrado como HTTPS, SSL, SSH, entre otros, los cuales cifran la información que viaja por la red para que, si es capturada por un Sniffer, esta no sea legible directamente. También es posible cifrar archivos y discos duros completos para proteger su acceso, aunque también es una técnica empleada por hackers a través del Ransomware para cifrar el contenido de los discos y solicitar a cambio de la contraseña de cifrado un pago específico que usualmente se hace en consignaciones o a través de monedas digitales como los bitcoins[58].

---

[57] PABÓN, J. La criptografía y la protección a la información digital. s.f. [Consulta: 25 de septiembre 2020]. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

[58] MALWAREBYTES. Cryptojacking. 2018. [Consulta: 25 de septiembre 2020]. Disponible en: https://es.malwarebytes.com/cryptojacking/

6.1 IDENTIFICAR RIESGOS Y AMENAZAS INFORMÁTICAS MÁS RELEVANTES QUE ENFRENTAN LOS USUARIOS DE LOS SISTEMAS EN LA ACTUALIDAD, A PARTIR DE ESTUDIOS REALIZADOS EN COLOMBIA Y EN EL MUNDO

Actualmente existe técnicamente una infinidad de vulnerabilidades para todos los dispositivos electrónicos usados, si algo tiene un componente electrónico, es vulnerable y por lo tanto hackeable[59], antes de iniciar con los informáticos en los equipos de cómputo, se presenta dos breves historias de hacking con el objetivo de introducir al lector y generar conciencia de la capacidad que tiene este tipo de prácticas de las cuales tanto organizaciones como el personal en general deben dejar de ignorar:

6.1.1 Todo es Hackeable:

6.1.1.1 Hacking a marcapasos:

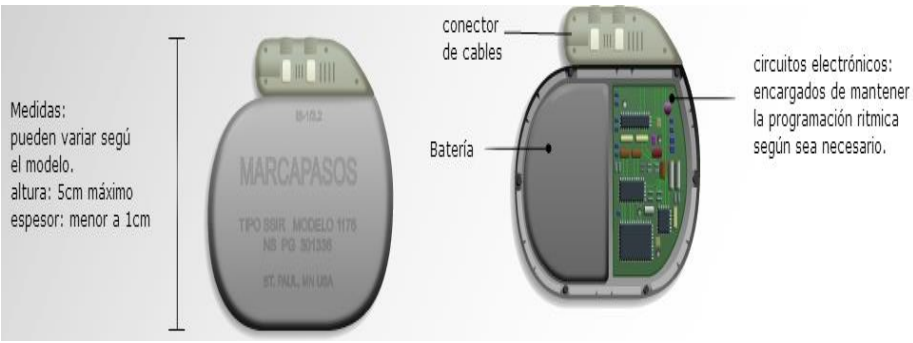
Como se puede evidenciar durante el transcurso de las últimas décadas, cada vez más dispositivos se conectan a internet para enviar y recibir datos o actualizaciones. Entre algunos de estos dispositivos, se encuentran algunos muy poco convencionales, por ejemplo, algunos equipos médicos como marcapasos (figura 2), los cuales actualmente permiten recopilar información sobre su estado y el de su portador, así como también permiten modificar o ajustar su configuración y funcionamiento.

Debido a esto, y teniendo en cuenta que cualquier dispositivo conectado a la red o con capacidad de recibir señales electromagnéticas, es posible inferir que este puede ser un blanco fijo de ataques informáticos.

---

[59] DANS, E. *Everything is hackable: get over it.* 2015. [Consulta: 24 de septiembre 2020]. Disponible en: https://medium.com/enrique-dans/everything-is-hackable-get-over-it-a3ca75a0c093

Figura 2. Marcapasos Cardiaco



Fuente: http://cardiotech.com.sv/wp-content/uploads/2015/12/ANATOM%C3%8DA-DE-UN-MARCAPASO-CARD%C3%8DACO.jpg

El primero en darse cuenta o informar sobre este hecho fue el famoso hacker Barnaby Jack que en su momento trabajaba como director de seguridad de dispositivos integrados en la empresa IOActive. Fue reconocido por haber demostrado frente a un público asombrado la vulnerabilidad de unos cajeros automáticos de ATM de los cuales logró que despacharan billetes sin necesidad de ingresar claves o contraseñas de cuentas o del sistema (ver figura 3). Esto se logró ya que era posible acceder al sistema de los cajeros a través de los puertos de comunicación TCP por defecto o aprovechar la posibilidad de acceder físicamente al cajero e insertar una memoria que contuviera el virus,

Figura 3. Conferencia de Seguridad BlackHat. Las Vegas, Nevada 2010

Fuente: http://speedreadingfull.blogspot.com

Barnaby quien era un experto en seguridad informática y programador, también logró controlar otros dispositivos médicos como bombas de insulina y marcapasos[60]; la forma de hackeo inalámbrico de las bombas de insulina lo demostró interactuando con una bomba de insulina usada por un amigo y otra por un modelo que permitió evidenciar la activación de la bomba de insulina la cual entregó repetidamente hasta 25 unidades seguidas de insulina o también vaciar por completo todo el depósito de 300 unidades, lo cual resultaría letal para cualquier paciente, y solo requirió de una antena de alta ganancia que le permitía acceder al dispositivo médico a una distancia máxima de 90 metros.

De igual manera que lo hizo con las bombas de insulina, para controlar los dispositivos marcapasos Barnaby mencionó el uso de una antena de alta ganancia que le permitiera comunicarse con el marcapasos y sin necesidad de conocer el número de serie o modelo del mismo, lamentablemente falleció una semana antes de explicar el funcionamiento y demostración de su hallazgo; Barnaby explicaba que a través del uso de un sistema de comunicación inalámbrica que incluía una antena de alta ganancia, le era posible acceder al sistema del marcapasos a una distancia de hasta 15 metros.

En 2017 la compañía de seguridad WhiteScope publicó un resultado de evaluar cuatro de los dispositivos marcapasos de diferentes marcas más usados en todo el mundo; en su publicación menciona la detección de cerca de 8000 vulnerabilidades encontradas en estos dispositivos médicos que podría permitir recopilar información sobre el usuario del marcapasos e incluso permitir modificar el funcionamiento de este. Esto obligó a que compañías farmacéuticas como Abbot se vean obligadas a lanzar actualizaciones de software para corregir las amenazas, de manera que por ejemplo, todo aquel que tuviese marcapasos Accent,Anthem, Assurity, o Allure entre otros modelos, debían ir a un centro

---

[60] GAONA, K. Análisis de Vulnerabilidades de Ciberseguridad en Desfibriladores Cardíacos Implantados. 2018. [Consulta: 24 de septiembre 2020]. Disponible en: https://medium.com/enrique-dans/everything-is-hackable-get-over-it-a3ca75a0c093

médico para que lo actualicen y evitar la instalación de malware, aproximadamente 460000 pacientes sólo en EEUU debieron actualizar su firmware en 2017.

Según el reporte de WhiteScope, la mayor parte de las vulnerabilidades se encontraba en las librerías de los dispositivos y que las contraseñas usadas para actualizar el firmware de los mismos estaban inmersas en el mismo código, por lo que se facilitaba el proceso de introducir un firmware falso y cambiar el funcionamiento de los dispositivos; además cuando los marcapasos se conectaban con dispositivos de monitorización, no era necesario ingresar alguna contraseña de autenticación, lo que permitía el acceso y control total del dispositivo.

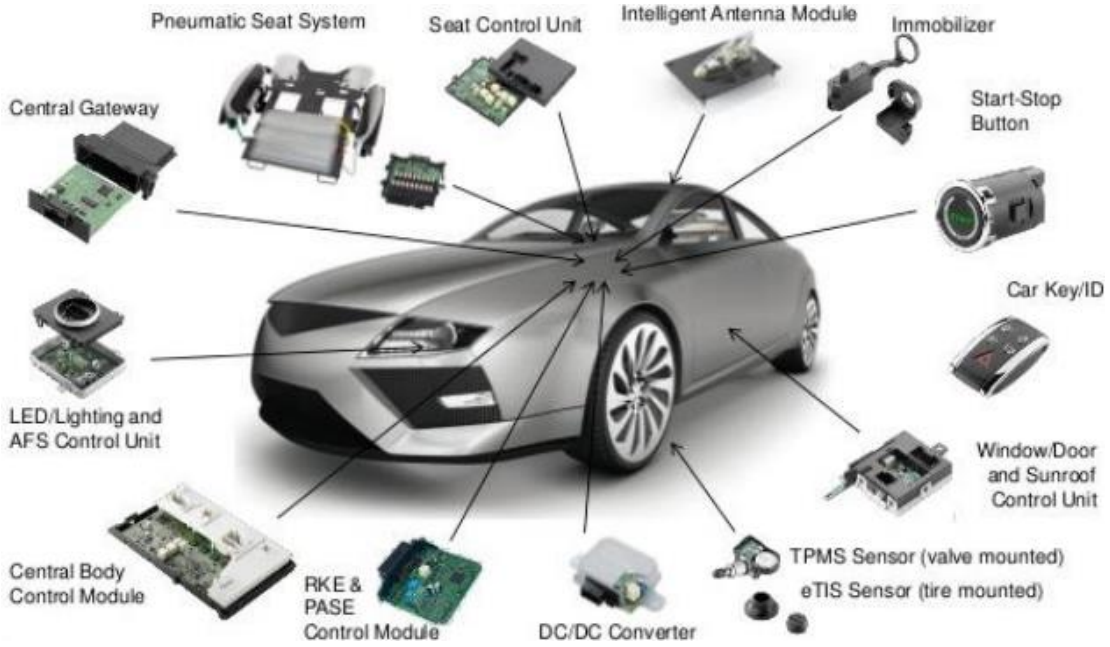
Se reportó también que no existía ningún o dispositivo o sistema que verificara que el servidor era genuino, y que la comunicación entre los dispositivos tampoco estaba cifrada, de hecho, algunos sistemas incluyen conexión USB que podría permitir introducir malware sin ninguna dificultad.

Por razones de seguridad y por la gravedad del asunto, no se especifica detalladamente las vulnerabilidades o el proceso de comprobación de las mismas hasta tanto las empresas no logren proteger dichas vulnerabilidades, sin embargo a la fecha no ha habido una respuesta contundente por parte de los fabricantes que permita resaltar la protección contra dichas amenazas puesto que requiere de un desarrollo mucho más complejo de los dispositivos médicos y la forma en que se comunican con un servidor o un monitor de información de los mismos.

6.1.1.2 Hacking en vehículos:

Se podría pensar que el hacking a vehículos[61] es algo muy actual ya que con la llegada de la IoT (Internet de las Cosas) millones de dispositivos, aparatos y demás han logrado comunicarse con la internet, y así mismo se podría inferir que los vehículos, quienes actualmente manejan un alto nivel de tecnología y conectividad (ver figura 4) podrían presentar vulnerabilidades cibernéticas[62], pero lo cierto es que no es necesario que estos tengan tecnología avanzada o conectividad a internet,

Figura 4. Vectores de ataque a vehículos.



Fuente: https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3428-m22-04-car-hacking-over-can-bus-3/file.html

En 2010 un grupo de investigadores de las Universidades de Washington y San Diego (California) informaron sobre el control remoto obtenido en un vehículo Chevrolet Impala

---

[61] BAVERA, M. Car Hacking. 2015. [Consulta: 24 de septiembre 2020]. Disponible en: http://jeuazarru.com/wp-content/uploads/2015/11/CarHacking.pdf

[62] TELERO, W. Seguridad en los autos con sistemas de apoyo a la conducción. s.f. [Consulta: 4 de septiembre 2020]. Disponible en: http://polux.unipiloto.edu.co:8080/00002675.pdf

mod. 2009, aprovechando sus vulnerabilidades inalámbricas, logrando manipular controles del auto como radio, parabrisas, apagado/encendido del motor y frenos; General Motor tardó 5 años en ofrecer una actualización y/o solución al problema.

Posteriormente Charlie Miller y Chris Valasek, dos investigadores estadounidenses, lograron controlar por medio de las vulnerabilidades del sistema de radio funciones vitales del Jeep Cherokee mod. 2014, logrando controlar funciones de radio, aire acondicionado, sistema de frenos y motor; esto se logró incluso con un conductor dentro del auto en pleno movimiento. Por lo anterior fue necesario actualizar el software de 1.4 millones de automóviles Jeep, Dodge y Chrysler.

Cabe resaltar que otros componentes del vehículo también pueden generar una amenaza, por ejemplo, el sistema de encendido sin llave, el cual ha sido reemplazado con un componente de seguridad electrónica conocido como inmovilizador para activar o desactivar el vehículo, sin embargo, se demostró que era posible desactivarlo aprovechando que no se implementó protocolos de criptografía y autenticación usadas en el transponedor RFID o de identificación por radio frecuencia.

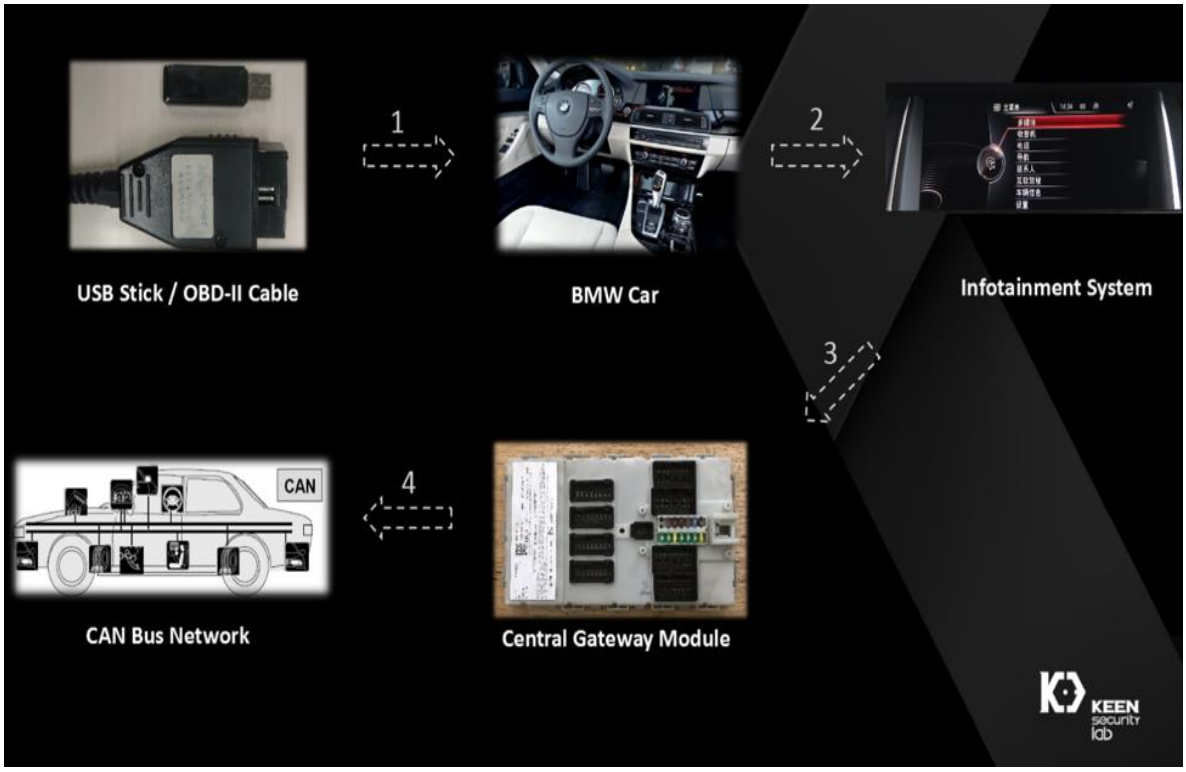
En 2010 La empresa Texas Auto Center reportó un incidente de seguridad en donde un exempleado disgustado, se infiltró en el sistema de inmovilización remota y desactivó el arranque de cerca de 100 vehículos. Luego en 2016 la policía del estado de Virginia logró tomar el control de un Chevrolet Impala 2012 y de un Ford Taurus mod. 2013, los cuales fueron controlados sin necesidad de que tuvieran una conexión a la red, simplemente aprovechando el control de a través de radio, logrando impedir el cambio de marchas, aumento de velocidad, y el encendido y apagado por completo del motor.

Entre los años 2017 y 2018 un grupo de investigadores de Keen Security Lab. Reportaron cerca de 14 vulnerabilidades (ver figuras 5 y 6) identificadas en las unidades de cómputo de los todos los vehículos de la concesionaria BMW, por medio de las cuales era posible controlar la unidad de control electrónica (ECU), la unidad de control telemático que

gestiona la telefonía y la posibilidad del bloqueo y desbloqueo de puertas remoto[63]. Algunos de los modelos que tenían mayor afectación por estas vulnerabilidades son:

- ✓ BMW i Series.
- ✓ BMW X Series.
- ✓ BMW 3 Series.
- ✓ BMW 5 Series.
- ✓ BMW 7 Series.

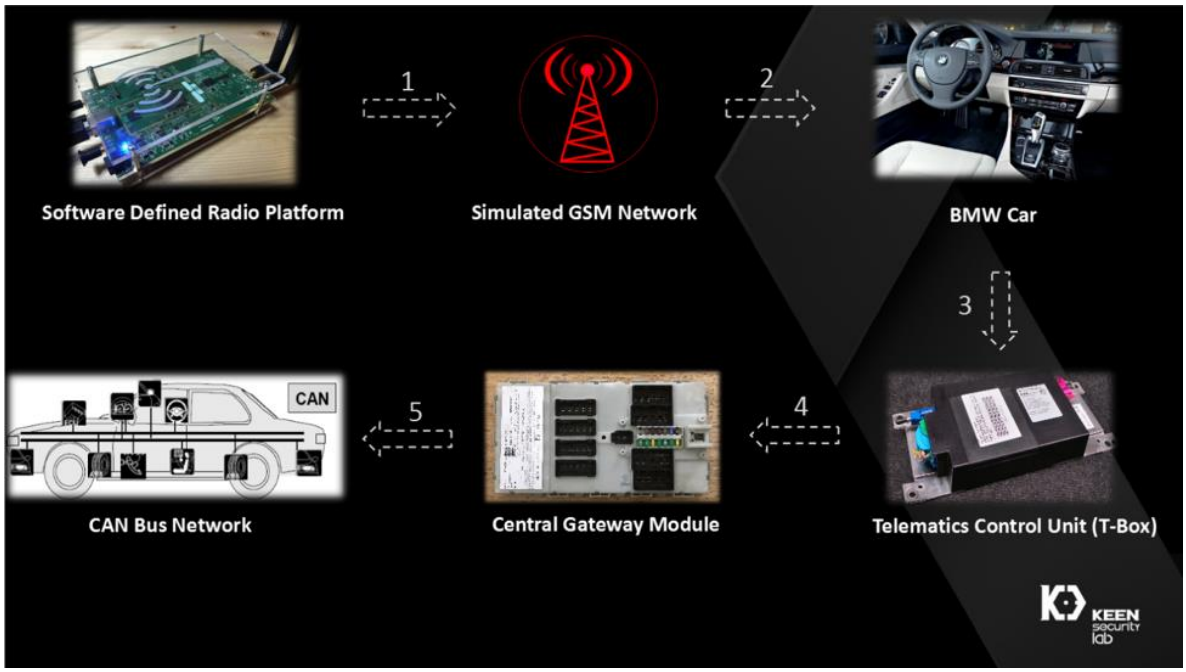
Figura 5. Cadena de Ataque local a vehículos.



Fuente: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

[63] KEENLAB. [Sitio web]. Experimental Security Assessment of BMW Cars. 2018. [Consulta: 24 de septiembre 2020]. Disponible en: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

Figura 6. Cadena de ataque remoto a vehículos.



Fuente: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

Recientemente, el mismo grupo investigador Keen Security Lab demostró el hackeo del vehículo Tesla Model S, al cual se logró explotar múltiples fallas de seguridad en su software más reciente, lo que les permitió tomar el control total del vehículo, esto incluía desbloqueo de puertas, acceso al control de pantalla, apertura del maletero, posicionar asientos, plegamiento de retrovisores, entre otros; aunque se especificó que se requería que el vehículo esté conectado a un punto de acceso Wifi el cual se encontraba controlado y que se accediera al navegador web del auto. De igual forma se demostró las vulnerabilidades usando los modelos Tesla S P85 y el modelo 75D, mencionando que estas vulnerabilidades se encontraban en la mayoría de los autos de la marca. Cabe resaltar que ante las vulnerabilidades reportadas por el equipo investigador Keen Security, Tesla tardó 10 días en lanzar un parche (firmware v7.1 (2.36.31)) para proteger las vulnerabilidades encontradas. Actualmente existen reportes de vulnerabilidades a los nuevos vehículos inteligentes, los cuales han sido incluso interferidos por punteros láser, los cuales afectaban el correcto funcionamiento del vehículo.

6.1.2 Amenazas Sobre Las Redes Informáticas:

Para iniciar con la identificación de vulnerabilidades, se procede a mencionar los que actualmente son los tipos de ataques más comunes en redes informáticas y en los cuales se pueden ver mayor mente inmersos los usuarios de los sistemas. Las fallas en la seguridad de las redes son muy comunes cuando es el usuario final el que desconoce los tipos de ataques o las vulnerabilidades que se puede crear a partir de una acción u omisión, ya que, en algunos casos, los administradores de la red también pasan por alto muchas implementaciones al desconocer las buenas prácticas informáticas o de seguridad que permiten mejorar el sistema de seguridad informático.

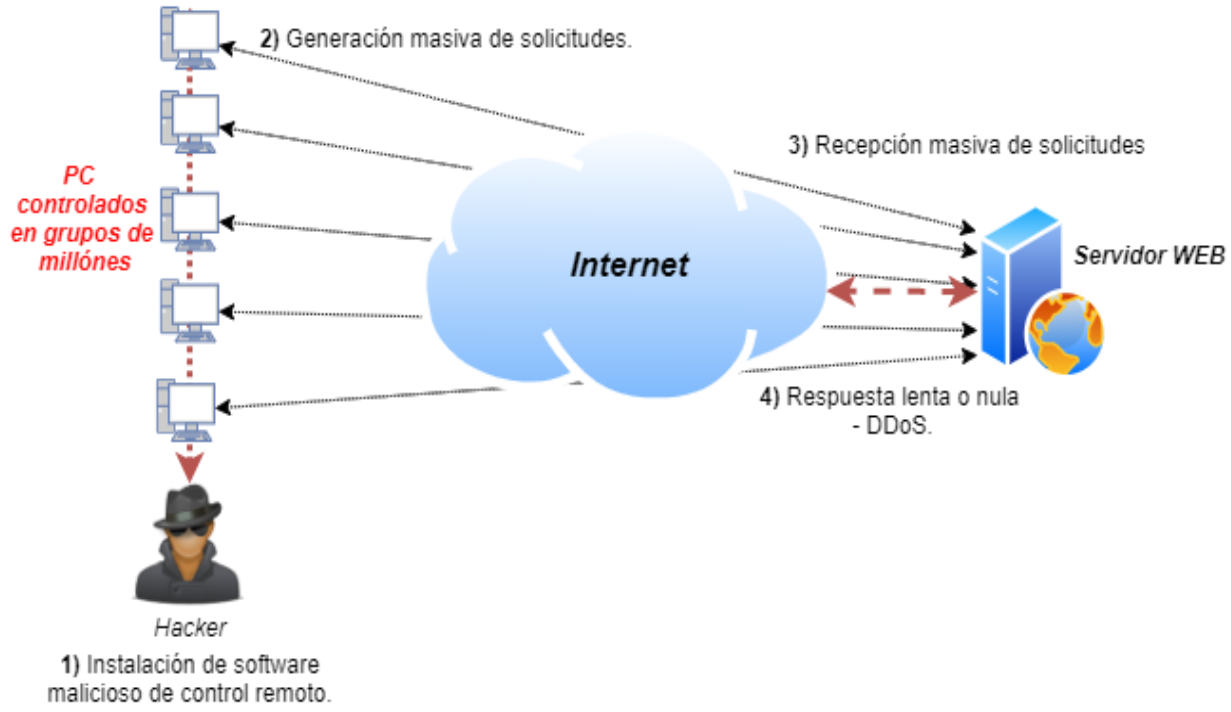
Básicamente se puede resaltar que la mayoría de ataques que se presentan a la red informática o sus recursos, se presentan por la falta de implementación o seguimiento de las políticas de seguridad de los datos he informáticas de la entidad, en donde uno de los mayores inconvenientes es la vulnerabilidad ante la ingeniería social que permite a un intruso un acceso u obtención de permisos / credenciales de accesos a la red y sus recursos; entre los ataques más comunes identificados a través del uso de la red y/o de internet se puede mencionar:

6.1.2.1 Ataque DoS (Denial of Services):

El ataque de denegación de servicio se puede clasificar en interrupción, intercepción, modificación y fabricación, que impide el correcto acceso a un recurso determinado[64], dentro de los ataques activos de interrupción. Tienen como objetivo reducir la disponibilidad de un determinado activo en el sistema mediante la realización de un ataque bien a la fuente de información, bien al canal de transición, o incluso a ambos, a continuación, se muestra un diagrama simple de este tipo de ataques en la figura 7.

[64] VERDEJO, G. Seguridad en redes. Cap. 2. Denegación de servicio: DOS / DDOS. s.f. [Consulta: 24 de septiembre 2020]. Disponible en: https://www.cs.upc.edu/~gabriel/files/DEA-es-2DOS-DDOS.pdf

Figura 7. Diagrama: Ataque DoS a través de Spoofing.



Fuente: El autor.

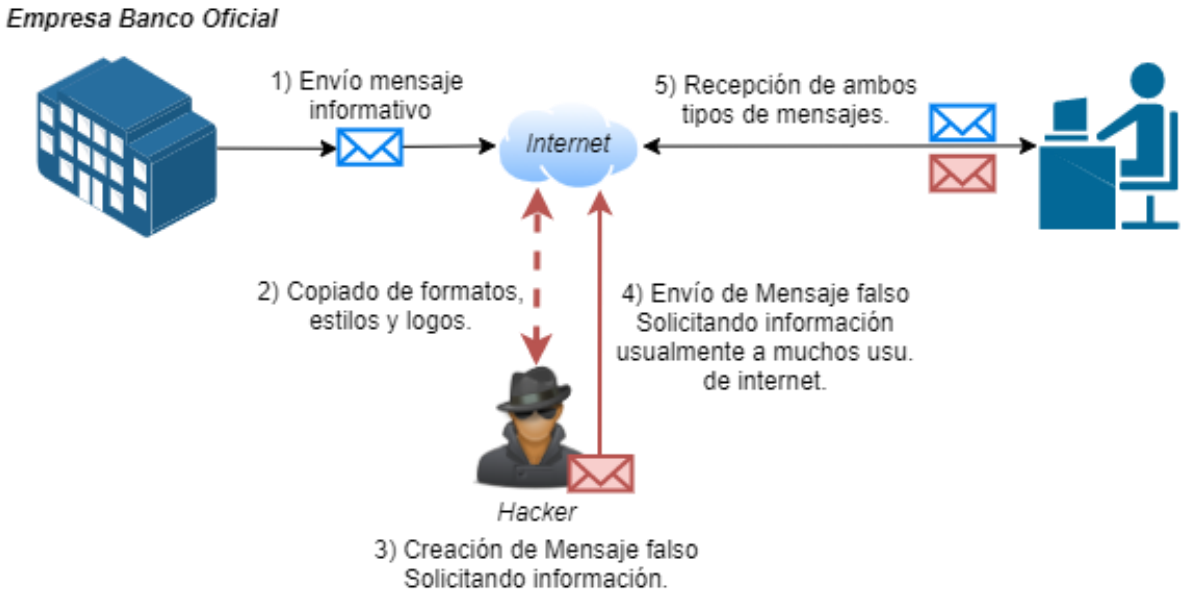
En la figura 7, se evidencia que el atacante, en primera instancia, identifica varios equipos vulnerables en la web e instala software para su posterior control remoto; una vez se tenga suficientes equipos controlados, se realiza un ataque masivo a un servidor web, el cual no podrá bloquear todas las solicitudes ya que vienen de orígenes diferentes y reales, por lo que tendrá una respuesta lenta a las solicitudes y posteriormente se denegará el servicio prestado por el servidor.

Aquí también cabe mencionar el *Ataque DDoS (Distributed Denial of Service),* el cual es una ampliación del ataque DoS es el llamado ataque distribuido de denegación de servicio por medio de un flujo intensificado de información desde varios puntos de conexión, lo que resulta congestionaste para la red y finalmente en la pérdida o caída del servicio.

6.1.2.2 Phishing:

El “Phishing” se considera como una técnica que permite aprovechar vulnerabilidades en el usuario final del sistema, por medio del engaño a los usuarios de Internet o de la red, suplanta una identidad que proviene de una empresa fiable, comúnmente de una página Web bancaria o corporativa para obtener una información determinada, usualmente credenciales de acceso al sistema[65] como se muestra en la figura 8. Haciendo uso de logotipos, sellos, estilos y emblemas, se genera un correo falso en suplantación de una entidad conocida como por ejemplo bancos, entidades públicas o incluso gobiernos, que se envía a una víctima con el fin de que esta acceda a la solicitud de información generada en el correo, acceda a sitios web malicioso o descargue archivos con malware.

Figura 8. Diagrama: Ataque Phishing.



Fuente: El autor.

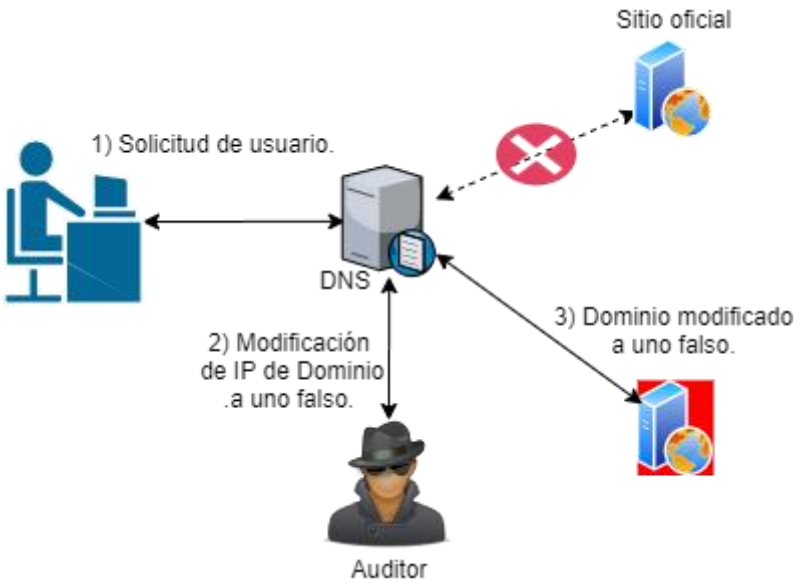
[65] SÁNCHEZ J. Métodos y técnicas de detección temprana de casos de phishing. 2019. [Consulta: 24 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf

En el anterior diagrama (figura 8) se puede observar que el atacante, aprovecha los mensajes informativos enviados a sus usuarios para copiar su estilo y logos, de esta manera el atacante genera un mensaje similar y lo envía solicitando información de validación o acceso, por lo que al usuario responder a dicho mensaje falso, revela información confidencial.

6.1.2.3 Spoofing DNS:

Mediante el cual se modifica en el servidor DNS para que el tráfico se redirija a otros sitios web diferentes al oficial; esto se logra al modificar para determinado nombre de dominio la IP asignada, así, tras el equipo consultar el nombre de dominio, redirigirá el tráfico a la IP registrada en su tabla (previamente falseada) como se indica en la figura 9, generando un riesgo para el usuario que podría revelar información privada[66].

Figura 9. Diagrama: Ataque spoofing DNS.



Fuente: El autor.

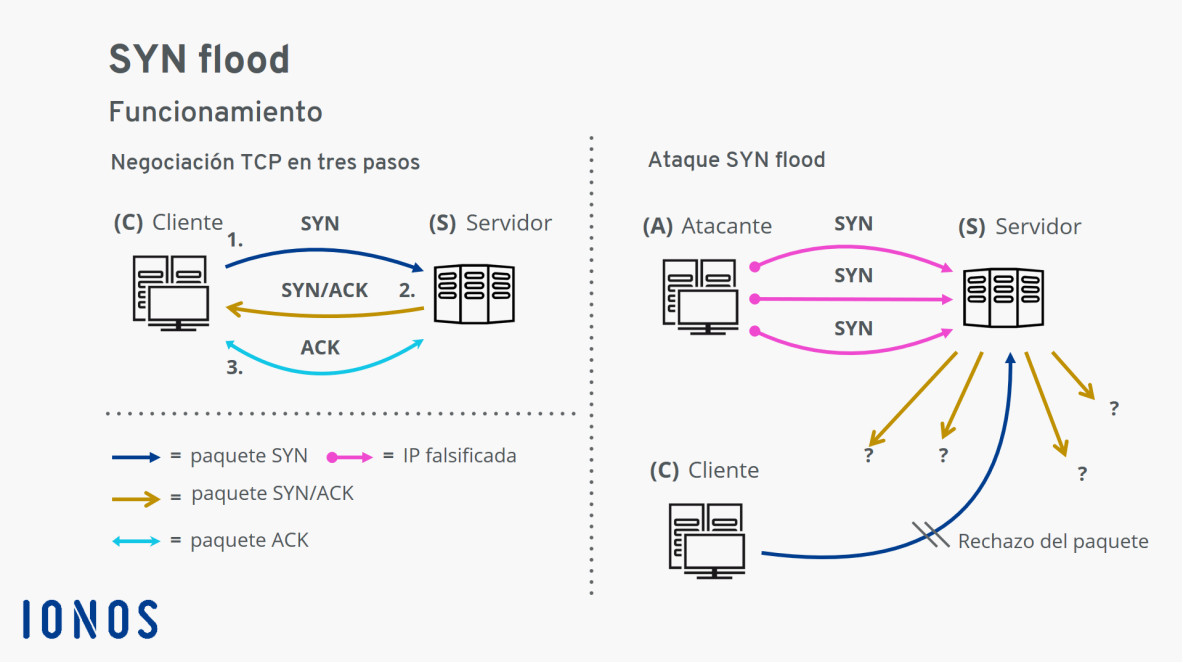
[66] HAMMUD E. Seguridad en servidores DNS. 2014. [Consulta: 24 de septiembre 2020]. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/21853/Tesis%20Elihu%20.pdf?sequence=1&isAllowed=y

Como se puede ver en la figura 9, cuando el usuario realiza la solicitud de contacto con determinado sitio web, el atacante ha modificado previamente la información del DNS para que, ante la solicitud realizada por el usuario, se lo redirija a la página configurada por el atacante.

6.1.2.4 Ataque de saturación de SYN:

Este ataque consiste en inundar la tabla de conexiones Iniciales del servidor, no permitiendo la creación de conexiones legítimas. El "ataque SYN" (también denominado "inundación TCP/SYN")[67] consiste en saturar el tráfico de la red (denegación de servicio) para aprovechar el mecanismo de negociación de tres vías del protocolo TCP. Dicho mecanismo permite que cualquier conexión a Internet "segura" (una que utiliza el protocolo TCP) se realice. En la figura 10, se muestra el esquema descrito:

Figura 10. Funcionamiento SYN.



Fuente: https://www.ionos.es/digitalguide/servidores/seguridad/syn-flood/

[67] IONOS. [Sitio web]. SYN flood: variantes y medidas defensiva. 2020. [Consulta: 24 de septiembre 2020]. Disponible en: https://www.ionos.es/digitalguide/servidores/seguridad/syn-flood/

6.1.2.5 SQL Injection:

La inyección de SQL es una técnica de gran impacto reconocida por el ingreso de sentencias de código SQL, realizada especialmente por programadores avanzados del lenguaje en mención; su objetivo principal tiene como finalidad la obtención de información por parte del servidor atacado[68], en respuesta a la ejecución del código ingresado, el cual devolverá datos que permitan escalar privilegios y/o lograr la captura de información del sistema instalado, para lograr infiltrarse en él. De manera tal, que este tipo de ataques permite al hacker extraer información de las bases de datos, donde incluso puede llegar a obtener accesos de administrador con lo cual el atacante puede realizar un alcance mayor en la ejecución de sentencias e incluso acceder a su entorno de configuración.

Las amenazas de este tipo generan una afectación alta en los sistemas, por ellos se consideran amenazas de alto riesgo, puesto que pueden afectar la funcionalidad de los servicios, su privacidad, su autenticidad al permitir modificarse y su disponibilidad. Es posible verificar si un sistema es vulnerable a inyección de SQL a través de software de análisis o también, se puede realizar una pequeña prueba usando el apóstrofe (‘) después de la id.

Entonces se retornará unos resultados, donde, sí se refiere un error en la consulta SQL, se comprobará que dicho sistema es vulnerable. Pero si no se recibe un error de ese tipo, se puede deducir que el sistema no es vulnerable a esta amenaza, sin embargo, es recomendable implementar buenas prácticas en programación que permitan realizar una validación de formularios web y los permisos para consultas por usuarios.

---

[68] CLARKE J. SQL Injection Attacks and Defense. 2da Ed. 2012. [Consulta: 4 de septiembre 2020]. Disponible en: https://doc.lagout.org/security/SQL%20INJECTION%20SECOND%20EDITIOn/SQL%20INJECTION%20SECOND%20EDITIOn.pdf

A continuación, se incluye un ejemplo práctico de cómo ensayar la vulnerabilidad con el objetivo de que se identifique dichos errores y se implemente los controles adecuados. Suponiendo el siguiente formulario básico (figura 11), se debe realizar lo siguiente:

Figura 11. Formulario ingreso de usuarios.

Fuente: El autor.

- ✓ Completar los campos usando el comando:
  " OR ""=" sobre los campos de usuario o contraseña.
- ✓ Debido a que es una sentencia conocida por el servidor, esta se ejecutará como:
  SELECT * FROM
  Users WHERE Name ="" or " "=" " AND Pass ="" or ""=""

El resultado del proceso de sentencia permitirá hacer consultas o escalar para regresar información de credenciales de acceso de administrador[69]. Otro ejemplo podría ser con la declaración del SELECT, agregando una variable (txtUserId) a una cadena de selección. La variable se obtiene de la entrada del usuario (getRequestString), como se ve en el siguiente ejemplo:

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

[69] RACCIATTI. Técnicas de SQL Injection. V.1.5. 2012. [Consulta: 4 de septiembre 2020]. Disponible en: https://doc.lagout.org/security/SQL%20INJECTION%20SECOND%20EDITIOn/SQL%20INJECTION%20SECOND%20EDITIOn.pdf

6.1.2.6 Smishing:

El smishing se trata de una técnica o actividad criminal en la cual se hace uso de mensajes de texto (SMS) que son enviados a celulares o dispositivos móviles con red telefónica[70] y en los cuales se solicita información personal al usuario. Algunas otras técnicas de smishing no solicitan directamente información a la víctima, sino que aplican técnicas de ingeniería social, informan que ya se está inscrito en un plan de consumo y que, si se quiere cancelar el mismo, se debe acceder a un determinado enlace, por lo que la víctima al enterarse del posible "cobro" que pueda generarse a su cuenta, intentará cancelar dicha suscripción accediendo al enlace o enviando datos personales para cancelar la supuesta suscripción. El objetivo de este tipo de delito es recopilar información personal para con ella, lograr realizar recuperación de contraseñas de sitios web o bancarios y así realizar gastos o retiros, o realizar directamente préstamos o compras a nombre de la víctima.

Identificar este tipo de mensajes requiere de atención en los detalles y estructura del mismo mensaje, incluso se debe verificar en número fuente de este, ya que por ejemplo SMS provenientes de números como 5000, identifican mensajes enviados desde una computadora a un teléfono, y que por lo general el mensaje solicitará una "autenticación de usuario" por medio del ingreso de nombres, cédula, y/o contraseña.

Este tipo de ataques es muy sencillo y, de hecho, los usuarios tienden a confiar más en los mensajes de texto que en los e-mails que reciben, por lo que la probabilidad de éxito es mucho más alta, permitiendo lograr acceder a información personal.

---

[70] MARTÍNEZ C. Seguridad por capas frenar ataques de Smishing. 2018. [Consulta: 24 de septiembre 2020]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiyj9ndhq7tAhVCnOAKHXLtDUgQFjAAegQIBRAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6255067.pdf&usg=AOvVaw2DyOgV0GnKbXk0KyX_L4Tc

Basta con seleccionar un objetivo, o incluso una base de datos de objetivos o números de teléfono, y enviar un mensaje de texto con una oferta, oportunidad u oferta laboral para solicitar información y utilizarla.

Por ejemplo, se podría crear el siguiente SMS:

"*Bienvenido!*
Claro Colombia te da la bienvenida a tu plan
personal de Redes Sociales Ilimitadas + llamadas VoIP
ref.43075579261 por valor de $40.000 pesos COP mensuales
descontados de tu saldo activo a partir de la fecha.
Para cancelar la suscripción accede al siguiente
enlace o responde este mensaje con tu número de cédula
seguido de tu nombre + la palabra "*SALIR*"."

O incluso son muy conocidos los mensajes con descuentos, los cuales también podrían ser usados de este modo:

"*Estimado Usuario*
Acceda a responder unas breves preguntas sobre
Nuestros servicios, nos interesamos por mejorar para ti.
Si respondes esta pequeña encuesta, obtén un 30% de
Descuento en el saldo de tu próxima factura para que
sigas disfrutando de nuestros servicios. Link: fly.asdakfi-as.
No pierdas esta oportunidad.
Oferta Válida por dos días."

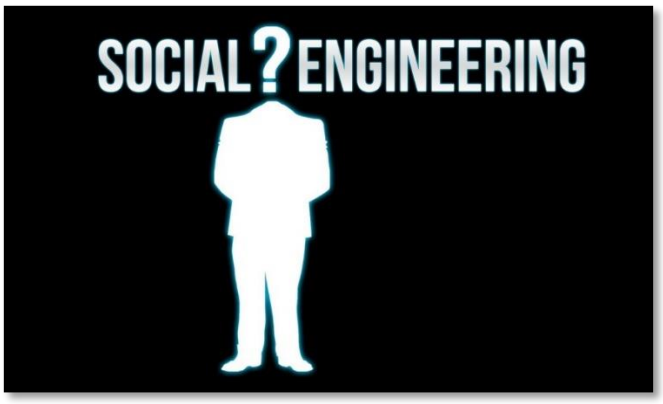
Básicamente la forma de evitar ser víctima de estas vulnerabilidades se encuentra en ser precavido con todo tipo de solicitudes de información personal, teniendo en cuenta:

- ✓ Verificar el número fuente de los mensajes.
- ✓ No suministrar información personal delicada o en exceso.
- ✓ No responder a ofertas, llamar directamente a los contactos de atención ofrecidos por la entidad.
- ✓ No acceder a enlaces web, o verificar la URL e identidad de esta.
- ✓ Hacer caso omiso a SMS sobre premios o regalos a los que no se haya inscrito o servicios a los que no esté registrado (llamar a la entidad para verificar).

6.1.2.7 Ingeniería Social

Sin lugar a dudas, esta es una de las amenazas más grandes a la que se enfrentan los usuarios, a su vez, considera un conjunto de técnicas que hacen uso de estrategias comunicativas y psicológicas para llevar a cabo su objetivo principal, que al igual que en los anteriores casos, será obtener información[71] de cualquier tipo, que les permita lograr posteriormente una intrusión o estafa, incluso teniendo como ventaja que se puede mantener el anonimato en todo momento facilitando estas actividades y generando la duda (figura 12 ilustrativa) de quienes pudieron realizar dichos trabajos investigativos.

Figura 12. Social Engineering.



Fuente: https://hackeruna.com

[71] SERRATO D. Estudio de Metodologías de Ingeniería Social. 2018. [Consulta: 4 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

Este tipo de ataques se componen de un conjunto de técnicas como phishing, vishing, pretexting, etc. que buscan recopilar la máxima cantidad de información del usuario, por ello se usa todo tipo de medios para contactar a la víctima, como por ejemplo el internet, teléfono, dumper diving (búsqueda de información en la basura que tira la víctima u objetivo) y la persuasión psicológica.

El conjunto de todos estos tipos de ataque ha generado que se establezca como una de las técnicas esenciales para que las otras modalidades de hacking funcionen de manera más efectiva[72], es por esto, que la ingeniería social se considera tan amenazante y difícil de detectar, ya que como se mencionó antes, en sí misma, considera muchos elementos técnicos y psicológicos que puede afectar al usuario de los sistemas.

Incluso es necesario resaltar el hecho de que puntualmente las redes sociales han permitido que se facilite la implementación de estos tipos de ataque basados en ingeniería social; esto debido a que el hecho de que se comparta información con un público muchas veces anónimo, permite al atacante con mayor facilidad recopilar información de su víctima para realizar con éxito cualquier otro tipo de ataque

6.1.2.8 Vulnerabilidades en Puertos De Red

Aunque los datos siguientes, no se consideran amenazas con las que los usuarios interactúan directamente, se decidió incluirlos ya que representan en sí mismos, las amenazas más comunes que se puede encontrar en dichos puertos de red; por lo tanto, se hace imprescindible su mención.

Los siguientes puertos descritos en el cuadro 1, se implementan por defecto para determinados servicios de red, por el software instalado o por el Sistema Operativo de

---

[72] PATARROYO S. Ingeniería social, una técnica subestimada por desconocimiento. s.f. [Consulta: 29 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

los equipos que tienen acceso a servicios web básicos[73], algunos de ellos son:

Cuadro 1. Puertos, Servicios y amenazas de red

Puerto	Servicio	Problema de Seguridad
8080	Web cache	Objetivo de ataques Dos, CGI, Buffer overflow, recogida de información, punto de acceso entre otros métodos de vulneración.
5432	Postgres	Vulnerable ante ataques de Fuerza bruta, uso de exploit para forzar credenciales de logins para obtener un Login de usuarios admin.
3306	MySQL	Por defecto sin contraseña de seguridad, para acceder a las bases de datos.
22	Servicio de Shell seguro (SSH)	Descuido en el manejo de claves por parte del usuario pueden ocasionar que personas inescrupulosas acedan a datos importantes que se manejan por este puerto.
21	FTP	Mayor Objetivo por intrusos. Vulnerable ante ataques DoS, Fuerza Bruta, Buffer Overflow.
23	Telnet	Objetivo de escaneos para obtener un login de acceso. Vulnerable ante Ataques DoS, Fuerza bruta, Buffer overflow, y Sniffeo.
53	DNS	Permite conocer el nombre de la máquina remota. Vulnerable ante: • Ataques DDoS: tráfico malicioso abundante que obstaculiza las peticiones legítimas. • Typosquatting: a construcción de un nombre de dominio falso casi igual al dominio objetivo real para configurar una variedad de ataques de phishing. • Secuestro de registros por el mal uso de contraseñas.
80	HTTP	Usualmente objetivo de Ataques CGI, DoS, Sniffer, Punto de acceso, Buffer overflow.
79	Finger (para información de contacto de usuarios)	Los crackers utilizan la información proporcionada por Finger para iniciar un ataque de ingeniería social en el sistema de seguridad de una compañía.

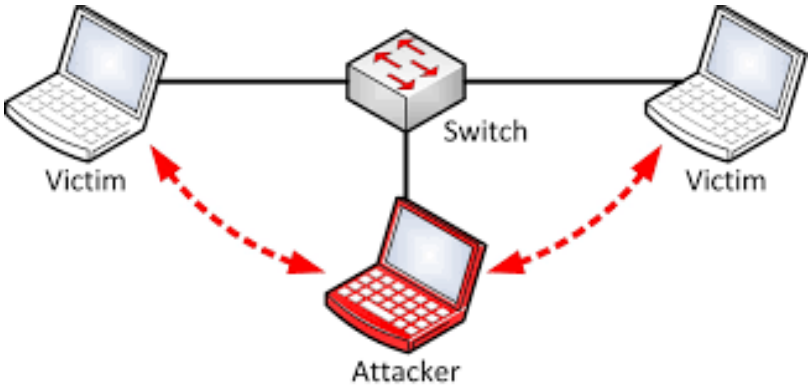
Fuente: El autor.

[73] CARVAJAL A. Introducción a las técnicas de ataque e investigación. 2017. [Consulta: 10 de octubre 2020]. Disponible en: http://acistente.acis.org.co/typo43/fileadmin/Articulos/TecnicasAtaqueComputacionForense.pdf

6.1.2.9 Sniffers

Igualmente complementando el elemento descrito anteriormente, no fuese posible la materialización de muchas de las amenazas detectadas en los puertos de red sin la ayuda de un Sniffer, es por esta razón que se menciona el mismo, Los sniffers, se pueden definir como un tipo de software que rastrea información de una red informática en búsqueda de paquetes de información determinados (ver figura 13) y con el objetivo de desencriptar la información contenida en los mismos[74]. La captura de información o tramas que viajan por la red se realiza por medio de una configuración especial que permite poner la tarjeta de red en un "modo promiscuo", con lo cual, todos los paquetes de datos que logra capturar el dispositivo no son desechados puesto que, aunque la MAC de destino no sea la especificada en la cabecera del paquete, el "modo promiscuo" permite almacenar dichos paquetes de datos para posteriormente tratar de desencriptarlos.

Figura 13. Diagrama Sniffer.



Fuente: https://hackingpills.blogspot.com/2017/09/bettercap-sniffear-nuestra-red.html

Implementar este tipo de herramientas en un proceso de análisis de seguridad en las redes de datos, permite identificar vulnerabilidades de la red, tanto en protocolos de trasferencia de datos como en difusión y alcance de la red, encriptación de datos, y

[74] NÓVOA M y PÉREZ O. Sniffers: Espías en la Red. s.f. [Consulta: 10 de octubre 2020]. Disponible en: http://index-of.co.uk/Tmp/SniffersPDF.pdf

protocolos de red; que, de acuerdo con el resultado obtenido de evaluar una red mediante este tipo de herramientas, permiten determinar fallas en la seguridad de estos y establecer propuestas o planes de seguridad alternativos que promuevan y refuercen la seguridad en las redes de datos; también se consideran una herramienta útil para determinar la cantidad de tráfico en la red y el tipo de información que se transmite entre otras utilidades.

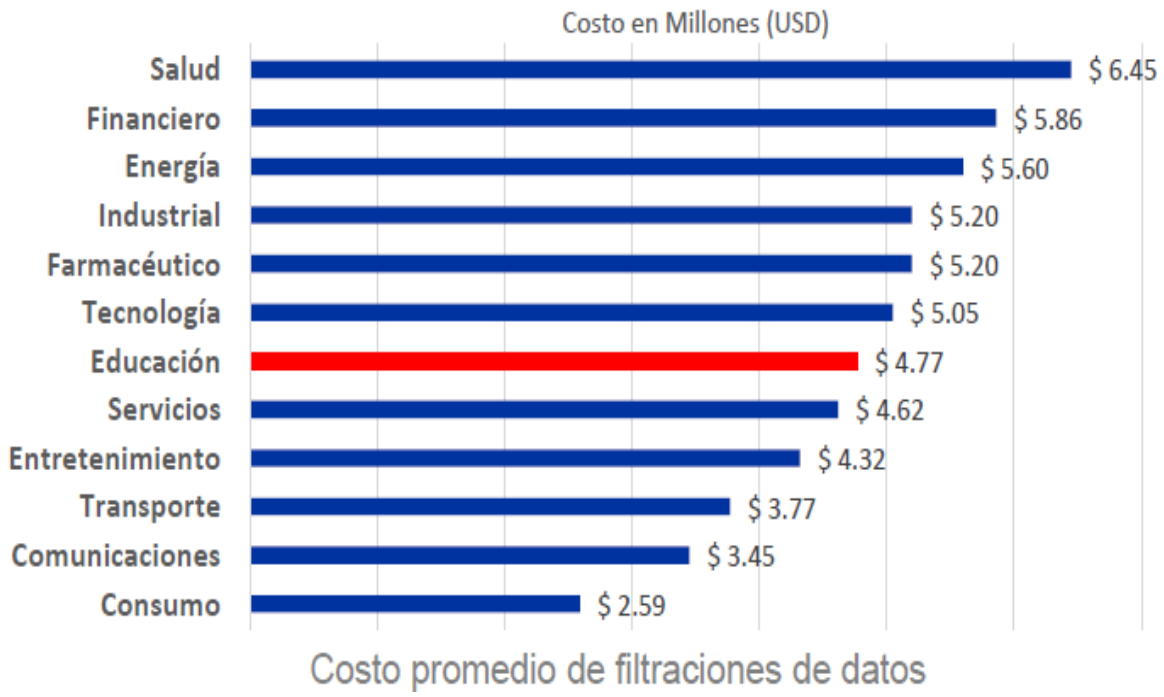
6.2 DETERMINAR EL IMPACTO DE LOS RIESGOS Y AMENAZAS INFORMÁTICAS MÁS HABITUALES QUE PUDIERAN SER MATERIALIZADOS POR LOS USUARIOS DEL SISTEMA, TENDIENDO COMO BASE LA METODOLOGÍA MAGERIT

6.2.1 Costos y Estadísticas del Cibercrimen

Claramente cada uno de los anteriores ataques informáticos, tiene un historial de daños y costos que, a la fecha, aún no dejan de sumar víctimas informáticas y pérdidas económicas para quienes sufrieron la vulneración, especialmente para aquellas organizaciones donde se perdió la mayor parte de la información.

Si bien en muchos casos, se ha dirigido la atención en mitigar los riesgos más probables, lo cierto es que tanto en Latinoamérica como en el resto del mundo, los esfuerzos siempre deberán ser constantes y crecientes para reducir la posibilidad de que una amenaza informática o riesgo se haga efectivo, y por ello se requiere no solo de suponer y mitigar los riesgos más probables, sino que es necesario cubrir cada vulnerabilidad encontrada o posible; aunque muchas veces se tenga la creencia de que no todos los sectores son foco de atención de los hackers, o que existen sectores que por no ser de primera necesidad, no son atractivos para ser vulnerados, lo cierto es que las investigaciones presentadas a continuación (ver figura 14), permiten observar que nada se escatima:

Figura 14. Costo promedio de filtraciones de datos.



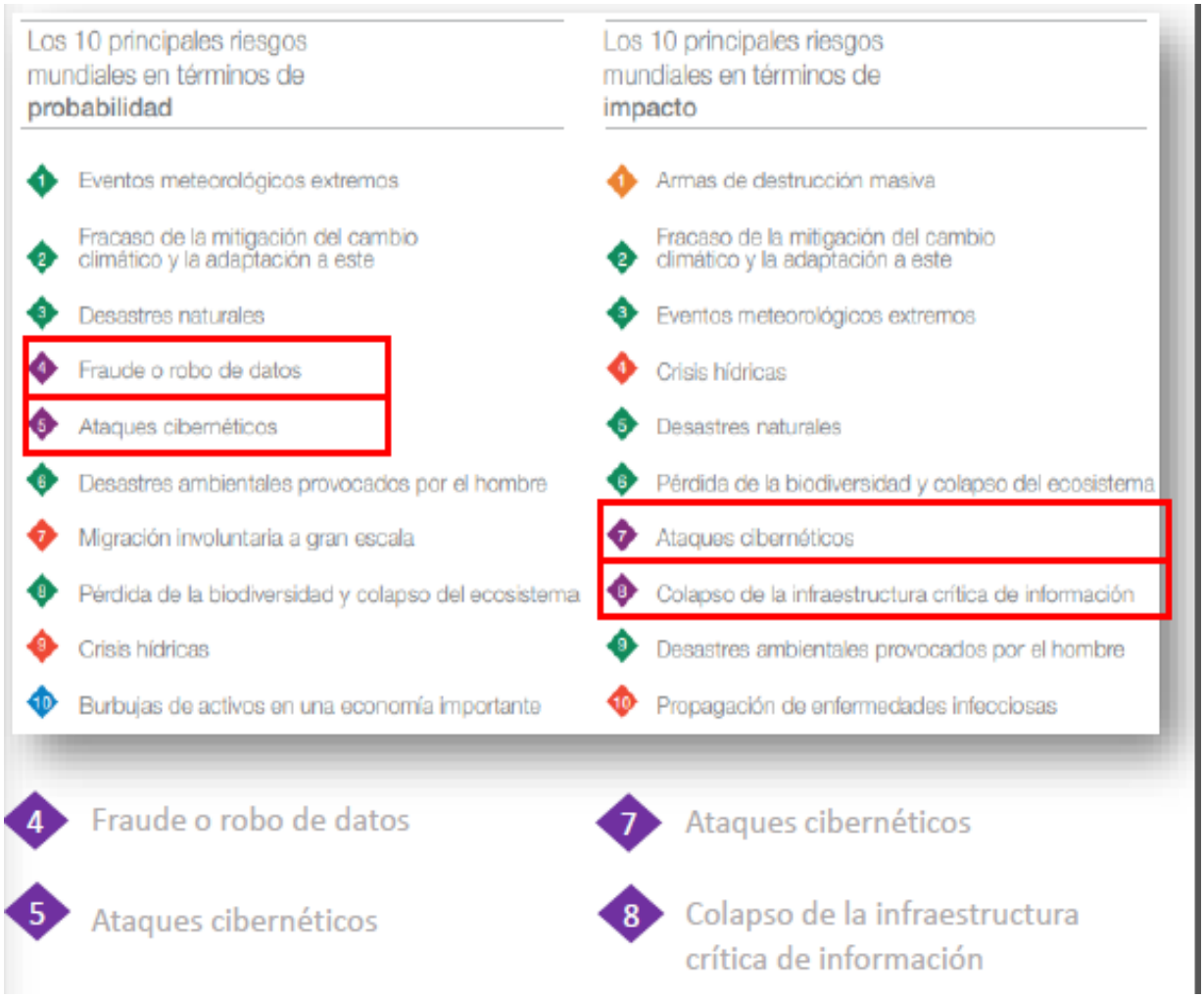
Fuente: Cost of date breach report 2019.

En el gráfico anterior (figura 14), se aprecia el costo promedio en millones de dólares derivado de las filtraciones de datos, en donde el coste más elevado está en el sector de la salud, con aproximadamente $6.45 millones de dólares en pérdidas para 2019, y para el sector de la educación $4.77 millones de dólares para el mismo año[75]. Lo que permite evidenciar que los riesgos informáticos están presentes para todos los sectores y para todas las personas.

Un estudio realizado por el World Economic Forum en 2019, socializado por la aseguradora SURA, determinó en qué posición se ubicaban el robo de datos a nivel de probabilidad e impacto; dando como resultado la siguiente gráfica (ver figura 15):

[75] IBM. [Sitio web]. Data breach. s.f. [Consulta: 10 de octubre 2020]. Disponible en: https://www.ibm.com/security/data-breach

Figura 15. Top Riesgos e impactos mundiales.



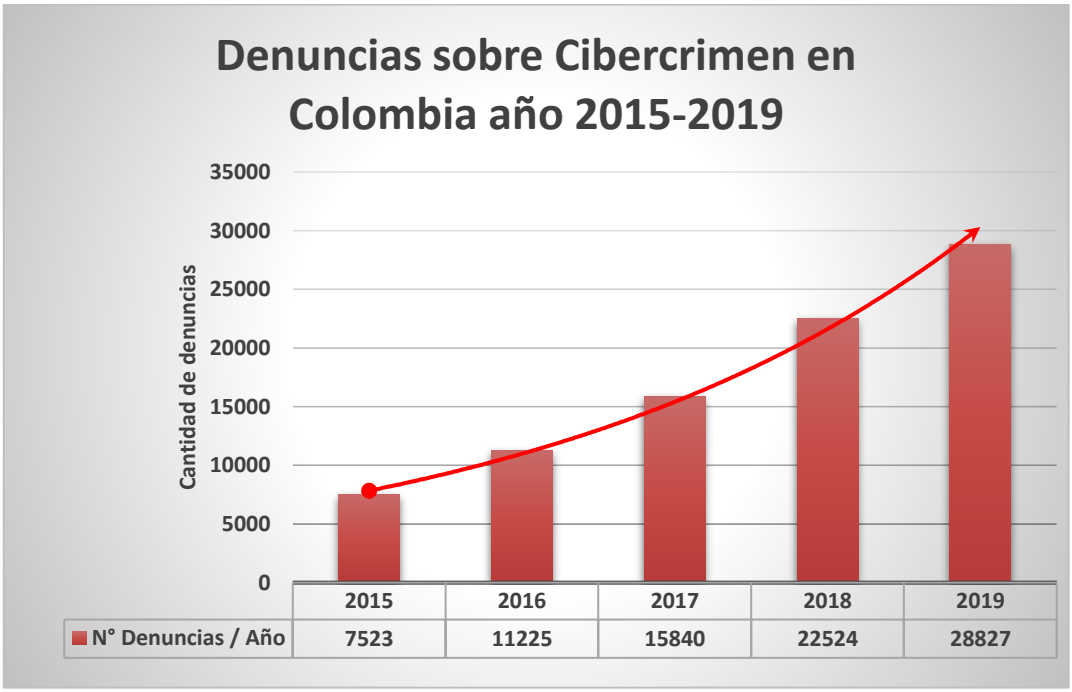
Fuente: Informe de riesgos mundiales 2019. World Economic Forum.

Por otro lado, solo en Colombia se reportaron 12.879 incidentes cibernéticos para ese mismo año, de ellos, el **42%** corresponden a temas de phishing, la suplantación de identidad o Spoofing ***28%***, el envío de malware se ubicó en un **14%** de los casos reportados y los fraudes a través de medios de pago en línea correspondió al ***16%*** [76].

[76] POLICIA NACIONAL DE COLOMBIA. PONAL. [Sitio web]. Tendencias Cibercrimen Colombia 2019-2020. 2019. [Consulta: 22 de octubre 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Si se realiza un estudio sobre el comportamiento de delitos reportados en lo corrido de los últimos 5 años en Colombia (ver figura 16), es posible evidenciar cuál ha sido la frecuencia con que este tipo de amenazas se han venido presentado:

Figura 16. Gráfico de Denuncias sobre Cibercrimen Colombia.



Fuente: El autor.

El gráfico anterior (figura 16) permite identificar un crecimiento de más del 280% en los casos de cibercrimen, los cuales pueden ser muchos más debido al desconocimiento de estas amenazas y de aquellas amenazas que a la fecha no fueron detectadas por el uso avanzado de técnicas, la falta de personal capacitado en el tema, falta de recursos informáticos u otros aspectos que excluyen de este reporte la realidad enfrentada. Sin embargo, es necesario resaltar que los métodos de dispersión de malware más reportados en Colombia[77], se presentaron a través de correos electrónicos:

[77] CENTRO CIBERNÉTICO POLICIAL NACIONAL. Tendencias Cibercrimen Colombia 2019-2020. 2019. [Consulta: 10 de octubre 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

- ✓ Dispersión de malware a través de emails de suplantación: 63%
- ✓ Dispersión de malware a través de sitios web: 32%
- ✓ Dispersión de malware a través de APPs móviles: 5%

Cabe resaltar que la mayoría de los delitos, si bien no todos, buscaban en la motivación económica, ya que los cibercriminales buscan la obtención de beneficios monetarios a través de la estafa, secuestro de información, robo de identidades o credenciales de acceso entre otros. Lo cual guía a identificar los principales riesgos a tratar en el contexto de la mitigación de las amenazas que se han encontrado.

6.2.2 Delitos informáticos de más afectación en Colombia:

Aunque es difícil determinar el verdadero impacto de los ataques informáticos registrados y de aquellos que seguramente permanecen en el anonimato debido a la complejidad de los mismos, se puede aproximar en base a los casos reportados y de acuerdo con los estudios y reportes presentados por el CAI virtual de la Policía Nacional[78], cuáles han sido los delitos que más afectaron la seguridad de la información, basándose en la regularidad de los ataques registrados en el país, los cuales, por razones claras, no son únicamente ataques provenientes de la misma región o país, sino que por estar una red interna conectada a internet, se expone a ataques provenientes de todo el mundo, tanto de organizaciones criminales como de actuaciones individuales; lo cual permite identificar:

a) ***Hurto por medio informático***: Se considera el delito informático más denunciado en el 2019, reportando hasta 31058 casos. Su principal objetivo fue identificar cuentas disponibles y saldo bancario de sus víctimas.

---

[78] POLICIA NACIONAL DE COLOMBIA. PONAL. [Sitio web]. Tendencias Cibercrimen Colombia 2019-2020. 2019. [Consulta: 22 de octubre 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

b) ***Violación de datos personales***: Con un total de 8037 casos, en donde se trató en forma no consentida la información de privada de las personas con fines de lucro.

c) ***Acceso abusivo a un sistema informático***: Donde se reportaron 7994 casos de intrusión a los sistemas operativos, de gestión y aplicación, haciendo uso de técnicas que permitieran ganar acceso a los sistemas, esto incluye el uso de herramientas de software destinadas para auditar los sistemas.

d) ***Transferencia no consentida de activos:*** Llegando a reportarse hasta 3425 casos, a través de la sustracción de dinero o transferencia de información por medios electrónicos.

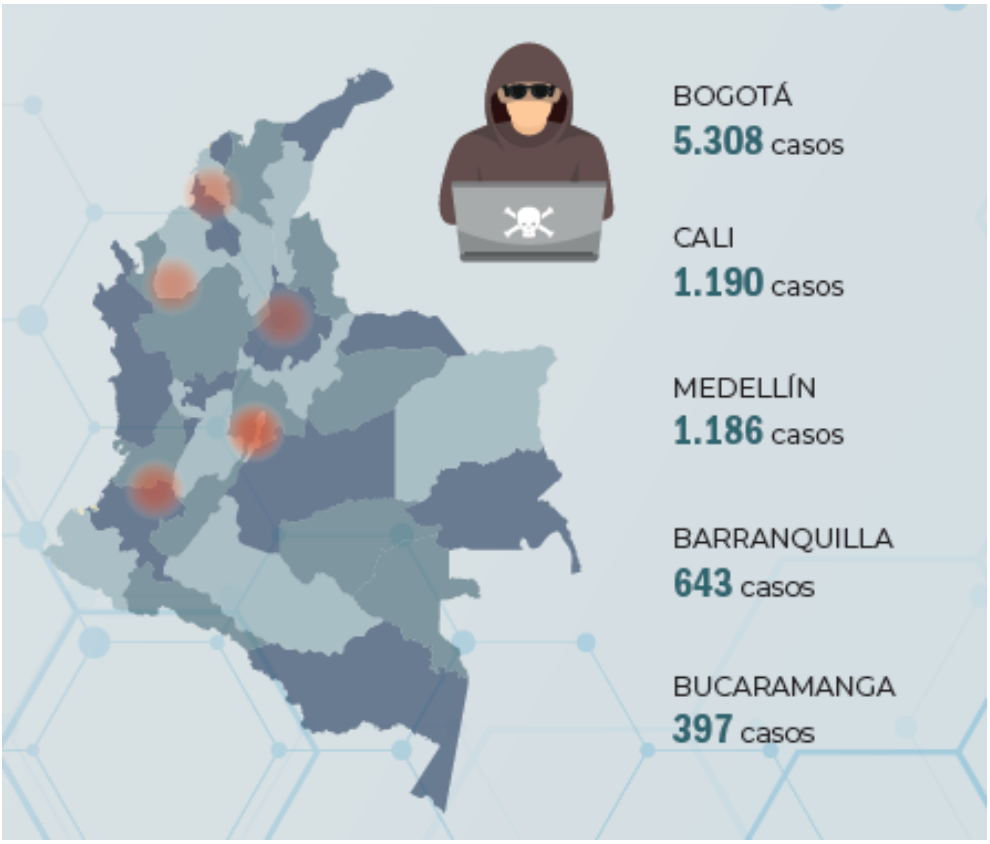
e) ***Uso de software malicioso*****:** Legándose a reportar hasta 2387 casos. En donde se reportan todo tipo de software de espionaje, sniffing, captura de información, análisis de vulnerabilidades, suplantación, explotación y creación de eventos o puntos de acceso no autorizados.

De lo anterior, cabe identificar que el hurto por medio informático es la amenaza más importante que se debe tratar, esta involucra directamente al usuario de los sistemas, ya que la información obtenida para materializar este tipo de amenazas solo es posible obtener a través de un descuido del usuario que permita revelar la información de acceso o por el uso inadecuado de los servicios e implementación de malas prácticas de seguridad informática.

Por otro lado, es necesario tener en cuenta el entorno del usuario, en este caso, se identifica que, en un entorno urbano, las amenazas informáticas serán más probables de suceder, debido a que también los sistemas se exponen a ser más visibles para la comunidad y por lo tanto más propensos a ataques. De acuerdo con los reportes generados por el centro cibernético de Colombia en su atención a las amenazas reportadas a sus instalaciones, en el año 2019, el 55% de los casos registrados, son provenientes o tuvieron como objetivo 5 ciudades principales del país, en donde se han reportado ***8729*** ataques distribuidos en las zonas de mayor densidad de población o

acceso a las tecnologías y las redes de comunicación como internet, en la figura 17, se puede identificar dicha cantidad de ataques reportados para el año 2019 :

Figura 17. Cantidad de ataques reportados a Nivel Nacional



Fuente: Cantidad de ataques reportados a Nivel Nacional.

Esto permite concluir que, si bien las amenazas informáticas son más probables de ocurrir en zonas con mayor densidad de población, se pueden presentar ataques en cualquier localidad, sin importar el tamaño de la organización. Además, se debe tener en cuenta que la tendencia de crecimiento de amenazas permite que se generen nuevos riesgos y modalidades de ataques los cuales pueden incluir ataques con inteligencia artificial, el uso de perfiles falsos en redes sociales para una difusión de malware más fácil, suplantación con tecnologías avanzadas como Deepfake para reemplazar audios, imágenes o vídeos, y el uso de vulnerabilidades no reportadas “Zero Day” en sistemas y software en general vendidos en mercados ilegales digitales.

6.2.3 Impacto del Ransomware:

El Ransomware ha sido sin duda uno de los malware que más ha afectado o vulnerado la seguridad de la información[79]; según el reporte anual entregado por la organización Sophos[80] realizado en 26 países a 5000 responsables de TI, el 51% de las organizaciones encuestadas en Latinoamérica fueron víctimas de este tipo de ataques, de ellas solo el 64% tenía un seguro contra este malware.

Este tipo de ataques comprenden diferentes cualidades que pueden ser útiles para detectarlos. A continuación, se presentan los vectores de ataques más comunes (ver figura 18) registrados para este tipo de ataque informático, los cuales identifican el modo mediante el cual se lograron infiltrar en los sistemas a través del suministro de información falsa como:

Figura 18. Vectores Ransomware.

Fuente: https://caivirtual.policia.gov.co/

---

[79] CAIVIRTUAL. [Sitio web]. Delitos en Colombia. [Consulta: 22 de noviembre 2020]. Disponible en: Https://caivirtual.policia.gov.co/

[80] SOPHOS. [Sitio web]. Sophos The State of Ransomware Latinoamerica. [Consulta: 22 de noviembre 2020]. Disponible en: https://www.sophos.com/es-es.aspx

Estos ataques se propagaron por medio de correos electrónicos que las víctimas interpretaron como información real y accedieron al contenido del mismo permitiendo el descargue e instalación del malware que afectó sus sistemas.

De esta manera, Colombia recibió un 30% de los ataques de Ransomware en toda Latinoamérica, de ellas el 717 reportaron que los ataques a sus sistemas fueron exitosos ya que incluso el 83% de estas, carecían de protocolos de seguridad de la información que facilitó la materialización de la amenaza[81].

Algunos de los tipos de Ransomware más detectados en Colombia fueron aquellos que cifraron los datos, pero permiten el uso del equipo; sin embargo, entre los más reportados se pueden destacar en general:

- ✓ ***Ransomware de Cifrado***: El cual cifra todos los documentos incluyendo imágenes y vídeos.
- ✓ ***Ransomware a dispositivos móviles:*** En el cual se cifra la información del dispositivo inteligente, infiltrándose a través de descargas no oficiales, viéndose principalmente afectado los sistemas de Android.
- ✓ ***Ransomware de Bloqueo de Pantalla:*** A través de un Winloker (aplicación de bloqueo) se bloquea la pantalla del sistema, permitiendo únicamente interactuar con una pantalla que informa sobre el bloqueo y solicita un pago monetario.
- ✓ ***Ransomware a MBR:*** El ransomware al Master boot record, permite bloquear por completo el acceso a disco duro, logrando incluso impedir iniciar el sistema operativo.
- ✓ ***Ransomware a servidores web:*** Cifra la información del servidor web, bloqueando todos los servicios y el acceso a archivos importantes de gestión a administración.

---

[81] CAIVIRTUAL. [Sitio web]. Delitos en Colombia. [Consulta: 22 de noviembre 2020]. Disponible en: https://caivirtual.policia.gov.co/

Este tipo de amenazas logró vulnerar tanto a organizaciones públicas como privadas, registrando para el año 2019 un mayor porcentaje de empresas privadas vulneradas. Con un coste promedio de reposición ante el ataque de $732.520 USD sin incluir pagos de rescate, la mayoría de las empresas víctimas lograron recuperar sus datos con copias de seguridad; de ellos 26% de las víctimas pagaron el rescate para recuperar sus datos, y un 1% pagó el rescate, pero no recuperó su información; finalmente solo el 24% de los ataques lograron ser detenidos antes de que se cifraran los datos según el reporte generado por Sophos frente al ransomware en Latinoamérica[82].

Esto reporte permite evidenciar que este tipo de ataques no discrimina ningún carácter, ubicación, ni tamaño de las organizaciones, volviéndolo altamente riesgoso ya que su alcance, estructura de código, desarrollo y modo de infección, permite su materialización en casi cualquier sistema de seguridad implementado mientras sea el usuario quien desconozca la amenaza. Por otro lado, llama la atención que, en base a los diferentes reportes consultados, no existe un único vector de ataque por ransomware; por el contrario, los atacantes implementan diversas técnicas o estrategias para vulnerar las carentes defensas logrando la intrusión. Ya que al final de cuentas, si una técnica de intrusión falla, pasarán a la siguiente hasta dar con una que les permita su cometido.

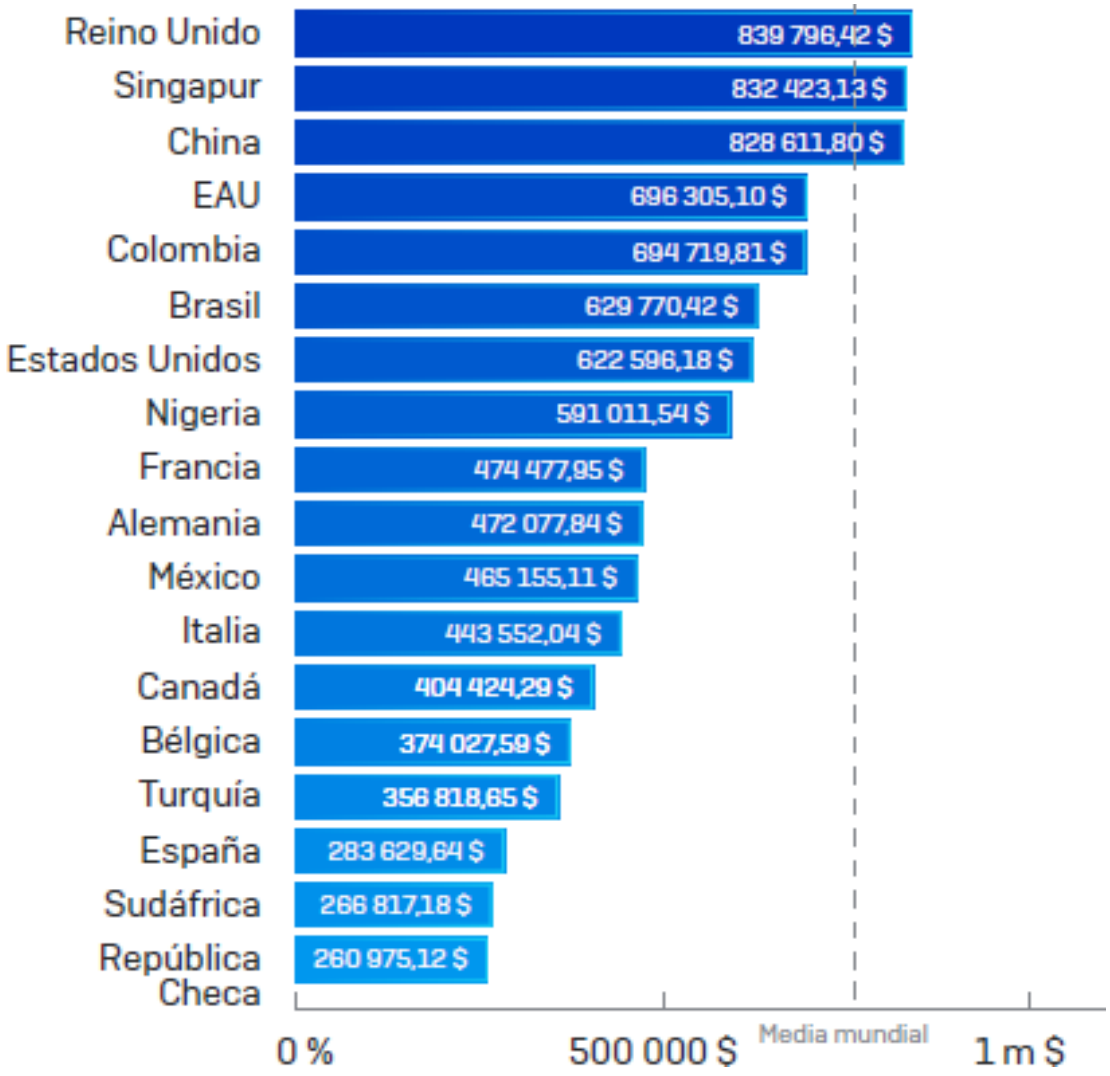
En Colombia, el uno de los ransomware más identificados es el denominado “SamSam”, el cual, por ejemplo, solicita montos de rescate entre $32 millones de pesos y más de $160 millones de pesos[83], usualmente el coste del pago del rescate puede duplicar los costos de remediación de este tipo de ataques. En la figura 19, se representa gráficamente el costo de remediación generado por el ransomware infiltrado, esto también representa una idea de la magnitud a nivel mundial de esta amenaza.

---

[82] SOPHOS. [Sitio web]. Sophos The State of Ransomware Latinoamerica. [Consulta: 25 de noviembre 2020]. Disponible en: https://www.sophos.com/es-es.aspx

[83] CAIVIRTUAL. [Sitio web]. Delitos en Colombia. [Consulta: 25 de noviembre 2020]. Disponible en: https://caivirtual.policia.gov.co/

Figura 19. Costo medio de remediación Ransomware en el mundo.



Fuente: Sophos Report 2020.

Estos datos demuestran que es necesaria la implementación de una defensa que permita una protección efectiva por capas, lo cual debe incluir no solo endpoints, sino también email, servidores, instancias en la nube, puertas de enlace de red y protocolos, así como también sobre la cadena de suministro. Puesto que centrarse en un único recurso, servicio o tecnología, representaría es una infección segura.

6.2.4 Impacto del Malware

Si bien al hablar de malware se abarca una gran cantidad de herramientas y/o software malicioso que tiene por finalidad corromper el correcto funcionamiento de los dispositivos y su software integrado, se ha decidido limitar la investigación netamente al malware que no se clasifica dentro de otro tipo de ataques informáticos como el ransomware o los ataques de DDOS en los cuales también se hace uso de cierto tipo de malware.

El incremento de dispositivos tecnológicos como computadores, tabletas, celulares, entre otros incluyendo aquellos que hacen parte del IoT (Internet de las Cosas), ha permitido que la difusión de contenido variado sea mucho más exitoso; así mismo, el malware ha tenido mayor éxito en su cometido. Para el año 2018, se reportaron cerca de 99 casos de ataques a través de malware; para el año 2019, se reportaron más de 700 casos[84]. Durante el último año, se reportó un incremento del 612% de incidentes relacionados con malware, por lo que se tendría un estimando de alrededor de 4284 casos, por supuesto, que esta cifra solo representaría una pequeña parte de los casos reales, algunos de los cuales no fueron reportados o que no fueron siquiera detectados.

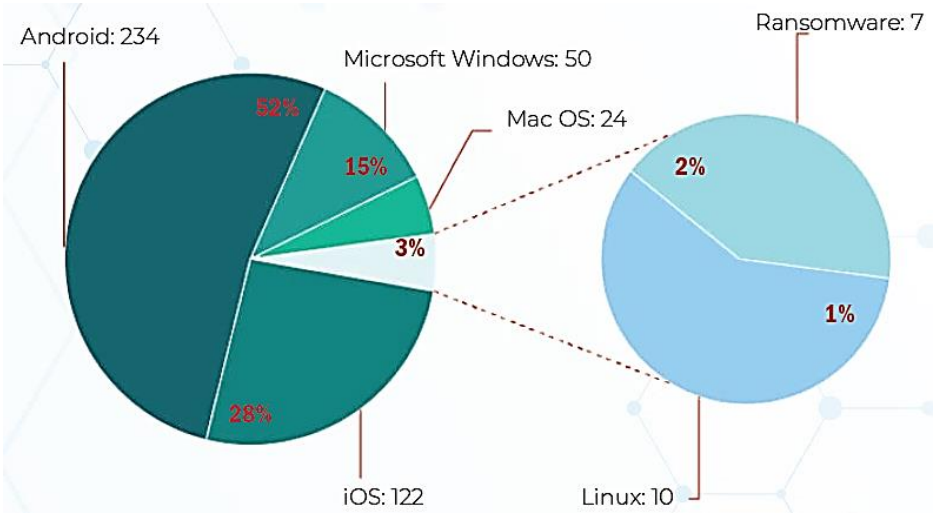
Debido a que el desarrollo de malware se mantiene en constante actualización, se ha logrado identificar cerca de 450 nuevas muestras de malware durante el año 2019, de estas, se reportó que cerca del 30% de amenazas podrían comprometer exitosamente los sistemas, como lo muestra la figura 20; el mismo reporte del centro cibernético policial, mostró que este tipo de amenazas fueron principalmente distribuidas a través de:

- ✓ Correo electrónico: 63%
- ✓ Redireccionamiento a sitios infectados: 32%
- ✓ Aplicaciones móviles: 5%

---

[84] CENTRO CIBERNÉTICO POLICIA NACIONAL. [Sitio web]. Informe tendencias de Cibercrimen 2019-2020. pp. 17-18. [Consulta: 1 de diciembre 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

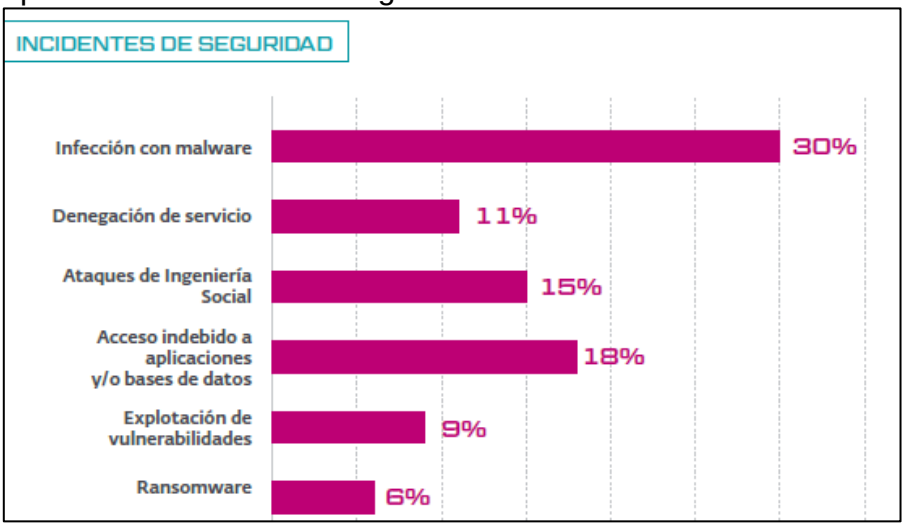
Figura 20. Muestras de malware analizadas en 2019 por Sistema Operativo.



Fuente: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

ESET, proveedora de protección antivirus, reportó en Latinoamérica, para el año 2020, que la mayoría de los incidentes de seguridad (figura 21), tuvieron que ver con la infección sobre malware[85]; como uno de los principales riesgos de seguridad a cubrir.

Figura 21. Reporte de incidentes de seguridad



Fuente: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

[85] ESET. [Sitio web]. Security Report LATAM 2020. [Consulta: 5 de diciembre 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

6.2.5 Impacto del ataque DOS (Ataque de denegación de servicio):

Debido a la creciente demanda por servicios ágiles y automatizados, las empresas e instituciones se han dedicado a prestar más servicios en línea, a través de sitios de consulta en portales web, tiendas digitales u otros servicios que requieren que estas entidades vuelvan públicos parte de sus infraestructuras tecnológicas en las cuales se soporta dichos servicios, lo cual representa un riesgo debido a la exposición pública hacia los internautas o usuarios de internet, entre los cuales, existirán usuarios mal intencionados que buscarán la forma de sacar provecho de sus conocimientos para afectar el funcionamiento del sitio web u obtener información no autorizada.

De acuerdo con el Centro cibernético policial de Colombia, en el transcurso del año 2019 se registraron cerca de 170 ataques exitosos de ataques DDOS que bloquearon directamente los servicios ofrecidos a los usuarios[86]. Para ello, se implementó en la mayoría de los casos botnet, los cuales se reconocen como un conjunto de equipos informáticos manipulados remotamente por un hacker para realizar dichos ataques de denegación de servicios. Debido a que estos equipos, son en la mayoría de casos equipos físicos de usuarios que, de hecho, no tienen ni idea de que su equipo personal forma parte de un “ejercito” de dispositivos controlado remotamente (generalmente un botnet se puede componer de más de 1 millón de dispositivos), fácilmente son manipulados para realizar solicitudes consecutivas a un servidor específico, con lo cual bloquean su funcionamiento al sobrepasar la capacidad de procesamiento de solicitudes del servidor, desbordando su memoria y terminando por bloquearse.

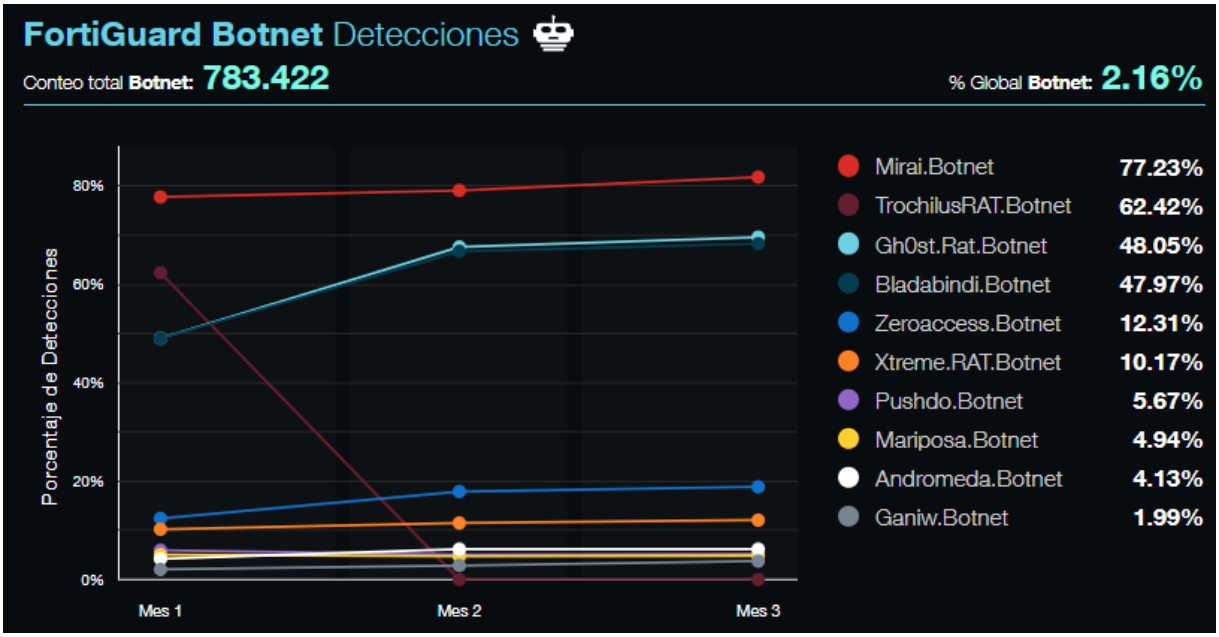
El portal web de la empresa Fortinet, la cual es una compañía líder en seguridad de red e infraestructura IT, presenta un reporte de los actuales reportes de botnet más comunes (ver figura 22).

---

[86] CENTRO CIBERNÉTICO POLICIAL. [Sitio web]. Informe tendencias de Cibercrimen 2019-2020. pp. 17-18. [Consulta: 7 de diciembre 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

En Colombia, para el primer trimestre del año 2021 se tienen los siguientes reportes:

Figura 22. Costo medio de remediación Ransomware en el mundo.



Fuente: https://www.fortiguardthreatinsider.com/es/bulletin/Q1-2021

Esto permite evidenciar que para el primer trimestre del año, fueron detectados cerca de 783.422 incidentes por los servicios se seguridad de Fortinet[87], sobre los cuales se evidencia que la mayoría de botnet detectados fueron los correspondientes al malware de Mirai, el cual, afecta principalmente en la red de internet a dispositivos como cámaras y routers que generalmente han sido mal configurados o cuentan con su configuración por defecto, lo cual le permite al malware instalarse en la memoria de los dispositivos para posteriormente ser manipulados remotamente. Usualmente, los atacantes suelen exigir pagos a través de monedas virtuales como el Bitcoin (entre 4 y 10 BTC) según los reportes obtenidos por el centro cibernético Policial de Colombia.

---

[87] CENTRO CIBERNÉTICO POLICIAL. [Sitio web]. Informe tendencias de Cibercrimen 2019-2020. pp. 17-18. [Consulta: 5 de diciembre 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

6.2.6 Impacto de la Ingeniería Social

La ingeniería social ha evolucionado durante cientos de años, ya que no es una técnica de la modernidad o únicamente digital como se puede llegar a pensar. Como se explicó anteriormente, este tipo de ingeniería implementa una o varias técnicas psicológicas y de análisis que permiten una recolección de información importante sobre la víctima, o también impulsan a un sujeto víctima a tomar decisiones u acciones "inconscientes", las cuales por supuesto, fueron planeadas o predichas por el atacante. Todo lo anterior, es posible precisamente gracias a ese previo estudio o recolección de información que permite adaptar el malware o cualquier ciberataque para que sea más exitoso, así pues, es acertado concluir que la ingeniería social es clave en el éxito de cualquier otra amenaza informática que un ciberdelincuente quiera utilizar.

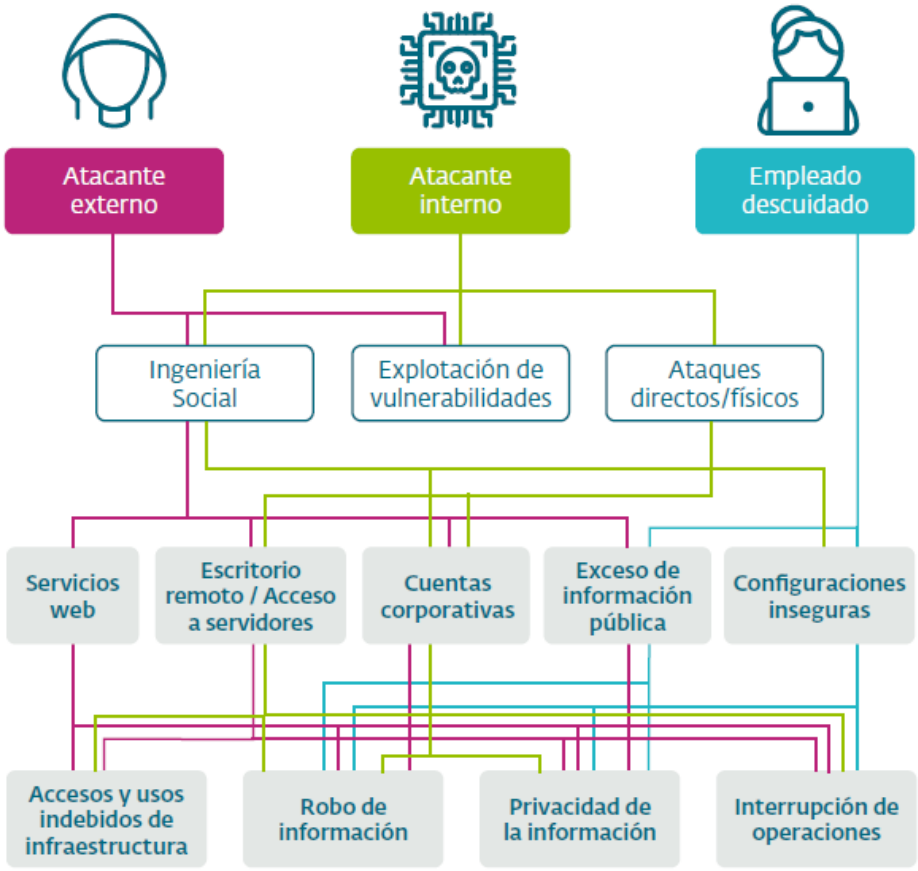
La Universidad Libre de Colombia, publicó un reporte en el que se informó que para el año 2019, se reportaron pérdidas por cerca de 6 millones de dólares a través del phishing en Colombia, dejando al país en el segundo puesto en Latinoamérica después de México[88], teniendo en cuenta que en Colombia al mes, se registran en promedio 187 denuncias por robo informático, de los cuales en su mayoría corresponden a la modalidad de phishing, que usualmente a través de correos electrónicos, engaña a las personas para que entreguen información privada como por ejemplo claves bancarias, números de tarjetas, nombres, número de cedula, contraseñas o incluso, pueden llegar a solicitar que se realicen movimientos financieros, bien sea para capturar datos o manipular directamente a la víctima por medio de amenazas de cortes de servicios o cuentas.

Es muy posible que la información que se publica en redes sociales como, por ejemplo: Facebook, Twitter y los blogs, faciliten este tipo de ingeniería que permita robar la identidad de la víctima o facilitar la recolección de información por parte del atacante.

[88] UNIVERSIDAD LIBRE DE COLOMBIA. [Sitio web]. Crecen los ataques de Phishing en Colombia. 2019. [Consulta: 8 de diciembre 2020]. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia

El ciberdelincuente también podría usar las identidades de la víctima para obtener todo tipo de artículos o servicios de consumo como teléfonos celulares, suscripciones, electrodomésticos, etc., dejándole a su víctima del fraude la deuda generada. En el siguiente diagrama (figura 23), se puede identificar a la ingeniería social, como uno de los pilares para la exploración de vulnerabilidades y base del éxito en los ciberataques, ya que un ciberataque bien dirigido, es aquel que conoce a su víctima y reconoce sus puntos débiles para explotarlos correctamente.

Figura 23. Ingeniería social – Base del éxito en los ciberataques



Fuente: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Aunque se entiende el riesgo que genera la ingeniería social, y este no tenga (de momento) un dispositivo o sistema que permita bloquearlo, es posible mitigarlo y/o establecer medidas de protección, como se verá más adelante.

6.3 RECONOCER ESTRATEGIAS DE MITIGACIÓN DE RIESGOS INFORMÁTICOS PARA LOS USUARIOS DE LOS SISTEMAS A PARTIR DEL ANÁLISIS DE VULNERABILIDADES IDENTIFICADAS ENFOCÁNDOSE EN LA METODOLOGÍA MAGERIT

6.3.1 Introducción a la Metodología MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) fue desarrollada para ayudar a las organizaciones a mejorar sus procesos y optimizar los recursos de información, incluyendo aquellos activos de IT, permitiendo la incorporación de tecnologías de forma creciente, enfocándose en el cumplimiento misional. Así, esta metodología permite la evaluación y control de los riesgos a los que puede estar sometida o enfrentarse una entidad, permitiendo además mitigar proponer controles para mitigar los riesgos o incluso para aceptarlos y proponer planes de acción y respuesta enfocados a dichos hallazgos, logrando identificar y abordar las vulnerabilidades con el objetivo principal de tratar los riesgos antes que sucedan y puedan generar graves afectaciones a la organización.

Esta metodología trabaja bajo los tres pilares de la seguridad de la información que se describe a continuación:

- ✓ Integridad: es la cualidad o característica de valides de los datos y la información, que permite garantizar además su completitud y por ende la fiabilidad de que su valor técnico no ha sido alterado, o sea, de que los datos y la información son lo que deben ser. La integridad también afecta directamente a las funciones y/o desempeño correcto de una organización
- ✓ Disponibilidad: se refiere a la disposición de los servicios a ser usados cuando sea necesario, tal que, siempre que se requieran, sean accesibles sin mayor dificultad; por ejemplo, si se tiene carencia de disponibilidad, se traduce en una interrupción del servicio en el momento que se haya solicitado o realizado su requerimiento. Esta afecta directamente a la productividad de una organización.

- ✓ Confidencialidad: es la propiedad que da privacidad a los datos o la información, es decir, que la información enviada llegue únicamente a las personas autorizadas o destinadas. Esta propiedad puede verse afectada por cuestiones que permitan fugas y filtraciones de la información, los cuales pueden derivarse de accesos no autorizados o controlados. La ausencia de la confidencialidad produciría una pérdida de confianza hacia la organización, e incluso puede suponer el incumplimiento de las leyes que protegen los datos y su manipulación por parte de las organizaciones, así como también de los compromisos contractuales relativos a la garantía del manejo y la custodia de los datos.

A estos pilares de la seguridad de la información, también se suelen considerar otros derivados[89], que se integran a la percepción de los usuarios de sistemas de información:

- ✓ Autenticidad: característica que determina la identidad puntual de quien se comunica, de tal manera que se valide que una entidad es quien dice ser, dicho de otra forma, que se garantice la fuente de la que procede la información. Ya que la información es susceptible a la manipulación del origen o el contenido de los datos. Es aquí donde se puede ver la suplantación de identidad como afectación a esta característica.
- ✓ Trazabilidad: es una propiedad que permite comprobar o monitorizar en cualquier momento quién hizo qué y en qué momento, con respeto a cambios, copias, consultas u otras actividades que conlleven a la manipulación de la información. Esta es una propiedad muy importante que permitirá analizar los incidentes, identificar en la línea de tiempo cualquier actividad, identificar a los atacantes y generar acciones de la experiencia. Por supuesto, que la trazabilidad debe ir de la mano con la integridad presente en los registros de actividad que avalan o constituyen una fuente de información real y válida.

[89] GOBIERNO DE ESPAÑA. [Sitio web]. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2012. Ed. Ministerio de Hacienda y Administraciones Públicas [Consulta: 15 de enero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

6.3.2 Valoración Cualitativa de las Dimensiones de la seguridad de la información

Aunque la metodología de MAGERIT se debe ajustar específicamente a las necesidades de cada organización, puesto que cada una tiene diferentes modelos de TI e infraestructura, así como también la información que manejan tienen distintos valores y grados de exposición, se propone trabajar de manera general con las amenazas informáticas más comunes a las que se enfrentan continuamente los usuarios de los sistemas como trabajadores de una entidad. De acuerdo con la metodología MAGERIT, se debe en primera instancia determinar sobre qué nivel de riesgos se va a trabajar la generación de estrategias de seguridad, y se procede a clasificar los activos de información teniendo en cuenta su autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad (ver cuadro 2), de esta manera:

Cuadro 2. Categorías y valoración del riesgo.

	INFORMACIÓN DE LOS ACTIVOS														
	DATOS DEL ACTIVO DE INFORMACION			DIMENSION					ATRIBUTOS						
No.	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros
1	[www] Página Web	Administrador	Servicios	MA	MA	MA	MA	MA	SI	NO	NO	SI	NO	NO
2	Servidor de impresión	Administrador	Servicios	A	A	A	A	A	SI	SI	SI	NO	SI	NO
3	Servidor de impresión	Administrador	Hardware	M	M	A	A	A	SI	SI	SI	NO	NO	NO
4	Equipos de Computo actividades	Administrador	Servicios	M	M	M	M	M	SI	SI	SI	SI	SI	SI
5	Equipos de Computo Registro y control	Administrador	Hardware	MA	MA	MA	MA	A	SI	SI	SI	SI	NO	NO
6	Equipos de Computo actividades	Administrador	Hardware	M	M	M	M	M	SI	SI	SI	SI	NO	NO
7	Teléfonos IP	Administrador	Hardware	B	B	B	B	M	SI	SI	SI	SI	SI	SI
8	Sistemas operativos win 10 Pro	Administrador	Software	B	B	A	A	A	SI	SI	SI	SI	SI	SI
9	Impresora HP LJ E serie 600	Administrador	Hardware	B	B	B	B	MA	SI	SI	SI	NO	NO	NO
10	Software antivirus (sin seguim)	Administrador	Software	B	B	B	MA	MA	SI	SI	SI	NO	NO	NO
11	Internet	Administrador	Comunicaciones	B	B	B	B	MA	SI	SI	SI	SI	SI	SI
12	Credenciales / contraseñas	Administrador	Datos	A	B	MA	MA	MA	SI	SI	SI	SI	SI	SI
13	Usuarios general del sistema	Administrador	Personal	B	B	MA	MA	MA	SI	NO	NO	NO	NO	NO

Fuente: El autor.

Para la valoración del riesgo se debe tener en cuenta las amenazas a las cuales se encuentra mayormente expuesto cada uno de los activos registrados y la información documentada que se suministre para su respectivo análisis. A partir de dicha información recolectada, se debe realizar una identificación de riesgos para cada activo, asociándoles las respectivas amenazas a las que se encuentran expuestos, asignándoles un valor de acuerdo con lo planteado en la "*tabla 1*"como se indica a continuación:

Tabla 1. Categorías y valoración del riesgo.

CATEGORÍA	VALORACIÓN DEL RIESGO
Riesgo Extremo (MA)	8, 9 y 10
Riesgo Alto (A)	6 y 7
Riesgo Medio (M)	5
Riesgo Bajo (B)	2,3 y 4

Fuente: El autor.

6.3.3 Valoración Cuantitativa de los riesgos

La valoración cuantitativa de los riesgos tiene en cuenta la valoración cualitativa de los riesgos realizada en el punto anterior; en base a dicha valoración, se asigna un puntaje (ver cuadro 3) teniendo en cuenta la siguiente relación para cada categoría de riesgo:

Cuadro 3. Valoración cuantitativa del riesgo

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: El autor.

Una vez se determina la valoración, se realiza un promedio de los resultados obtenidos para cada elemento según la integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad, obteniendo como resultado una valoración del riesgo para cada activo, como se ve en el siguiente cuadro (cuadro 4) desarrollado para ejemplo:

Cuadro 4. Clasificación de Activos según el nivel de riesgo

N°	Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
1	[www] Página Web	CRITICO	25	25	25	25	25	25
2	Servidor de impresión	IMPORTANTE	20	20	20	20	20	20
3	Servidor de impresión	IMPORTANTE	15	15	20	20	20	18
4	Equipos de Computo actividades acadé	APRECIABLE	15	15	15	15	15	15
5	Equipos de Computo Registro y control	CRITICO	25	25	25	25	20	24
6	Equipos de Computo actividades acadé	APRECIABLE	15	15	15	15	15	15
7	Teléfonos IP	APRECIABLE	9	9	9	9	15	10
8	Sistemas operativos win 10 Pro	IMPORTANTE	9	9	20	20	20	16
9	Impresora HP LJ E serie 600	APRECIABLE	9	9	9	9	25	12
10	Software antivirus (sin seguim)	APRECIABLE	9	9	9	25	25	15
11	Internet	APRECIABLE	9	9	9	9	25	12
12	Credenciales / contraseñas	CRITICO	20	9	25	25	25	21
13	Usuarios general del sistema	IMPORTANTE	9	9	25	25	25	19

Fuente: El autor.

6.3.4 Probabilidad de vulneración

Teniendo en cuenta que cada activo se encuentra ligado a una vulnerabilidad, se identifica la probabilidad de que se vulnere el activo teniendo en cuenta la amenaza identificada según la metodología MAGERIT, y asignando un valor de probabilidad de ocurrencia (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 prácticamente seguro) como se puede ver en el "*cuadro 5*". De manera que para cada activo se evaluará como en el siguiente ejemplo:

Cuadro 5. Probabilidad de vulneración

Nombre del activo de información	Valoración del Riesgo	Amenazas Metodología MAGERIT	Vulnerabilidades	Probabilidad de vulneración
[www] Página Web	25	[A24] Denegación de servicio	Ataques de DoS que sobrepasen la capacidad de respuesta del sitio web.	4
Servidor de datos	20	[A14] Interceptación de información (escucha)	Versión de software de SMBD desactualizada que pueda permitir ataques de inyección SQL	5
Servidor de impresión	18	[A11] Acceso no autorizado	La zona donde se encuentra el servidor no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona.	3
Equipos de Cómputo	24	[E8] Difusión de software dañino	Equipos mal configurados contra malware o que compartan archivos permitiendo la propagación de una amenaza como ransomware.	4
Sistemas operativos	16	[A4] Manipulación de la configuración	Los usuarios desconfiguran o modifican la configuración de sus sistemas con el fin de obtener accesibilidad o privilegios.	4
Credenciales / contraseñas	21	[A5] Suplantación de la identidad del usuario	La vulnerabilidad en las contraseñas, falta de actualización o falta de privacidad sobre las mismas, facilitan el robo de identidad.	4
Usuarios generales del sistema	19	[A30] Ingeniería social (picaresca).	Desconocimiento de los usuarios de las amenazas informáticas, técnicas de manipulación, estado de privacidad de datos e información de la entidad.	5

Fuente: El autor.

6.3.5 Calificación de Gestión

Teniendo en cuenta la alineación del Gobierno de TI, se procede posteriormente a identificar sobre las vulnerabilidades (fallas en uso del software o controles incompletos), controles de cambios de la información y sobre la infraestructura física, que permitan cumplir con los objetivos de la norma ISO 27001 (Requerimientos de implementación de un Sistema de Gestión de seguridad Informática - SGSI) e ISO 27002 (buenas prácticas sobre seguridad de la información) como se puede apreciar en el cuadro (6) siguiente:

Cuadro 6. Amenazas y Vulnerabilidades.

Amenazas Metodología MAGERIT	Vulnerabilidades	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión
[A24] Denegación de servicio	Ataques de DoS que sobrepasen la capacidad de respuesta del sitio web.	4	100	C	2
[A14] Interceptación de información (escucha)	Versión de software de SMBD desactualizada que pueda permitir ataques de inyección SQL	5	100	C	1
[A11] Acceso no autorizado	La zona donde se encuentra el servidor no cuenta con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona.	3	54	C	3
[E8] Difusión de software dañino	Equipos mal configurados contra malware o que compartan archivos permitiendo la propagación de una amenaza como ransomware.	4	96	C	3
[A4] Manipulación de la configuración	Los usuarios desconfiguran o modifican la configuración de sus sistemas con el fin de obtener accesibilidad o privilegios.	4	64	C	1
[A5] Suplantación de la identidad del usuario	La vulnerabilidad en las contraseñas, falta de actualización o falta de privacidad sobre las mismas, facilitan el robo de identidad.	4	84	C	2
[A30] Ingeniería social (picaresca).	Desconocimiento de los usuarios de las amenazas informáticas, técnicas de manipulación, estado de privacidad de datos e información de la entidad.	5	95	C	1

Fuente: El autor.

Donde:

- ***Cálculo del riesgo neto*** **=** (Valoración del riesgo * probabilidad de vulneración).
- ***Criticidad neta*** **=** (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 en adelante crítico(C)).
- ***Calificación de Gestión*** **=** (1 control no existe - 2 existe, pero no efectivo - 3 efectivo, pero no documentado - 4 efectivo y documentado).

6.3.6 Determinación de controles

De acuerdo con el Anexo A de la norma ISO 27002[90] se determinan que controles están implantados y cuáles no. Además, se propone en cada uno de ellos como se implantarían en la organización.

6.3.6.1 Controles implantados

Usualmente las entidades tienen una normatividad interna pero pocas veces se le hace un seguimiento adecuado o tienen el apoyo de las directivas para exigir su cumplimiento, lo cual perjudica el buen funcionamiento del SGSI y crea un ambiente permisivo para la ocurrencia de cualquier tipo de incidente informático. Por ejemplo, algunos de los controles que se puede identificar más comúnmente implantados (ver cuadro 7) son:

Cuadro 7. Controles implementados.

Tipo	Codificación	Título	Descripción
C	A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
C	A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
C	A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Fuente: El autor.

6.3.6.2 Controles sin implantar

Es importante definir de acuerdo con el nivel de riesgo sobre el cuál se va a trabajar, los controles necesarios para mitigar la vulnerabilidad o vulnerabilidades identificadas en los

[90] International Organization for Standardization. [Sitio web]. ISO/IEC 27002:2013. Buenas prácticas para gestión de la seguridad de la información. 2013. [Consulta: 17 de enero 2021]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

activos cuyos niveles de riesgo neto o criticidad, sean altos o considerables de acuerdo con lo inicialmente considerado en la aplicación de la metodología. Así, para los activos que se vienen trabajando en el ejemplo, se consideran los siguientes controles a implementar (ver cuadro 8), los cuales a su vez son útiles para para hacer frente a las amenazas previamente descritas en las que se resaltó el malware general, ataques DoS, ransomware e ingeniería social, entre otros:

Cuadro 8. Controles pendientes por implementar.

Tipo	Codificación	Título	Descripción	Propuesta para implementación
C	A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Formular políticas en apoyo de la dirección para la seguridad de la información y establecerla a toda la empresa empleados y a las partes externas pertinentes. Lo cual permitirá protegerse además ante ataques de ingeniería social.
C	A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Generar un manual de responsabilidades para el uso de activos con apoyo de la dirección para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. Lo cual permite proteger los activos de malware y ransomware.
C	A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Se debe crear una política de acceso con base en los requisitos del negocio y de la seguridad de la información apoyados desde la dirección. Permitiendo protegerse ante infiltraciones y suplantación de identidades de usuarios.
C	A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Diseñar en conjunto con el área de mantenimiento, dirección y aseguramiento de la calidad una política de zonas seguras y seguridad de la información. Con el objetivo de reforzar el control de acceso y el uso inadecuado o no permitido de cada activo.

C	A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Diseñar en conjunto con el área de mantenimiento, dirección y aseguramiento de la calidad una política de zonas seguras y seguridad de la información. Permitiendo mejorar la protección de los dispositivos de los usuarios y garantizando en mayor medida una recuperación oportuna ante la materialización de una amenaza.
C	A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Crear un documento para el seguimiento de los procesos, procedimientos y controles que permitan la mejora continua y brinden protección a la información.
C	A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Establecer y mantener un plan de seguridad en constante actualización y ajustado a las necesidades, permite reducir las brechas de seguridad y mantener un orden óptimo en la gestión de usuarios y la seguridad del sistema.
C	A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Exigir y velar por la privacidad en las credenciales de acceso, permite reducir infiltraciones y el éxito de ataques de ingeniería social.
C	A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Soportar la gestión de contraseñas, a través de software para su actualización y caracterización apropiada, permitiendo mejorar la robustez del sistema.
C	A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Crear un plan de restauración para la continuidad del negocio, permite responder adecuadamente a amenazas como el Ransomware, malware en general e incluso corrupción de datos o falsificación.

C	A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Establecer acuerdos de confidencialidad soportados con los usuarios para exigir y recordar los compromisos y mantener la privacidad de la información, permite reducir los riesgos de amenazas por ingeniería social, y robo de identidades entre otros.

Fuente: El autor.

Todos los controles descritos en el cuadro 8, junto con su codificación, pueden ser consultados en la norma ISO 27002[91], la cual establece los controles requeridos y recomendados en el Anexo "A" de esta norma, en la cual se encuentra una tabla de referencia con todos los objetivos de control; sin embargo, dichos controles no son obligatorios y pueden modificarse añadirse o eliminarse según la necesidad de la empresa. Cabe aclarar que no hay un límite de controles a seleccionar, cada organización puede determinar implementar tantos controles como quiera, el factor limitante radica en el presupuesto y en las políticas de la organización.

Una vez determinados los controles a implementar, se inicia su aplicación, por ejemplo, uno de los controles seleccionados para implementar es el control ***A9.1.1*** **-** Política de control de acceso, esta se encuentra dentro del dominio 9.1 Controles de acceso, cuyo objetivo es garantizar el acceso correspondiente mediante controles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, al consultar la norma ISO/IEC 27002:2013 control 9.1.1, se encontrará una guía de implantación para dicho control, así como también una breve descripción del control e información adicional como sugerencias al respecto de la política y el control.

[91] International Organization for Standardization. [Sitio web]. ISO 27002 A6 Organización de la seguridad de la información (normaiso27001.es). 2013. [Consulta: 20 de enero 2021]. Disponible en: https://normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion/

6.4 PROPONER ESTRATEGIAS DE CAPACITACIÓN ACOMPAÑADAS POR BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN EL USO DE LOS SISTEMAS E INTERNET, TENIENDO EN CUENTA LOS OBJETIVOS ANTERIORES

Si bien todas las amenazas anteriormente identificadas representan una parte de todas aquellas que actualmente se están viviendo, es claro que hay muchas que se desconocen, que están en desarrollo, o que a la fecha de hoy poco se han documentado por su complejidad o desconocimiento. Sin embargo, se ha sentado las bases de la seguridad informática, logrando establecer criterios mínimos y características específicas sobre la administración y el uso de las tecnologías, así como también se ha logrado identificar algunos vectores de ataque comunes entre diferentes amenazas, lo que permite tomar planes de acción que dificulten, anulen o mitiguen la materialización de los diferentes riesgos y amenazas informáticas.

Para lo anterior, se ha propuesto fortalecer el que se conoce como “el eslabón más débil de la cadena” en cuanto a la seguridad informática concierne, esto es, reforzando el conocimiento y habilidades de identificación de amenazas de los usuarios de los sistemas en una organización. De esta manera se propone el desarrollo de un temario de introducción sobre los riesgos a los que un usuario se enfrenta al usar dispositivos y servicios de internet, pues como se mencionó inicialmente, si algo está conectado a internet, es vulnerable, y requiere de protección, especialmente por quien administra o manipula dicho sistema o dispositivo; donde la idea central de todos estos procesos y actividades, estén encaminadas a la generación de una cultura informática adecuada.

Si bien únicamente la divulgación de conocimientos informáticos no permite crear una cultura informática sólida, se deben crear un conjunto de estrategias de concientización, evaluación, repaso y de apropiación que faciliten su implementación y eviten ser vistas como una actividad que genera más carga o afecta los procesos y actividades de la entidad, por esta razón, esta cultura puede representar un esfuerzo ingente para toda la administración e TI y las directivas de la entidad.

6.4.1 Definición de Temas de Capacitación

Con el objetivo de transformar a los usuarios como el mayor recurso de protección de los sistemas y no considerarlos el eslabón más débil de la organización cuando se trata de ciberseguridad. Se debe implementar una cultura de seguridad efectiva, lo cual debe significar el pasar del modelo tradicional de “acceder con cautela” a un nuevo pensamiento de “verificar antes de acceder”. Lo que se debe entender como una previa comprobación o validación de la fuente u origen de la información o archivo, que se debe tener presente con cualquier correo electrónico, archivo o comunicación, especialmente de un tercero, considerándolo peligroso hasta que sea validado correctamente.

Entre menos riesgos críticos se identifiquen, menos pérdidas financieras se podrán considerar ante un ciberdelito. Por lo tanto, cuando una entidad asigna fondos a la formación de concientización sobre seguridad informática, invierte en reducir las pérdidas, posibilitando un retorno de esa inversión. En otras palabras, la inversión en capacitación reducirá las posibilidades de que se produzca una infracción de seguridad porque un usuario crítico podrá reconocer buenas prácticas de seguridad.

Por supuesto, que adicionalmente si una empresa con personal consciente sobre seguridad informática tendrá una mejor imagen entre los consumidores, clientes o aliados, puesto que una empresa que es víctima de violaciones de seguridad perderá credibilidad como resultado de la publicidad negativa, independientemente del impacto real que pudiera causar la materialización de alguna violación en particular.

Hay que tener en cuenta también, que en la actualidad o en este preciso momento, las amenazas informáticas que son mitigadas por los esfuerzos de la entidad a través de la inversión en infraestructura de seguridad en sus empresas u oficinas, en conjunto con la administración y monitorización que pueda prestar el área de TI, no representan una garantía absoluta ante la materialización de una amenaza; especialmente si se considera además, que actualmente se ha visto impulsada la modalidad de teletrabajo, lo cual, por

supuesto, ha dado pie a incrementar el riesgo en la seguridad de la información ya que mucha de esta, se manipula en casa u hogar del trabajador, donde muy escasamente, por no decir en absoluto, se ve la infraestructura o los sistemas de seguridad y protección adecuados como por ejemplo sería un antivirus, software licenciado, firewall, parches de seguridad, protección de navegación y de email, entre otros.

Lo anteriormente observado, pretende resaltar la importancia que tiene la capacitación de los usuarios, puesto que a través de ellos está la primera y más importante defensa, y por esto, es importante que cada trabajador pueda reconocer determinados temas y a su vez, para la estrategia o metodología de capacitación se deben considerar:

- ✓ Uso correcto del internet: que permita a los usuarios reconocer sitios de riesgo, acceso a contenido oficial, seguridad en la navegación e identificación de anomalías en el funcionamiento de navegadores o exploradores web, entre otros.

- ✓ Manejo de la privacidad en redes sociales: lo cual, no debe representar en ninguna forma una restricción o prohibición en su uso personal, sino por el contrario, debe concientizar al trabajador sobre la importancia de la información y su privacidad, ya que al compartir contenidos, existe la posibilidad de revelar información sobre horarios, distribuciones físicas de un entorno y hasta servicios importantes que se usa como bancos, sitios web privados, sistemas, infraestructuras u otra información de identidad privados.

- ✓ Reconocimiento de los objetivos de ciberseguridad propuestos: todo el personal, debe reconocer que la ciberseguridad le incumbe y le compromete directamente, por esta misma razón, todo usuario o trabajador, debe apropiar los objetivos de mantener y garantizar el cumplimiento de los objetivos propuestos.

- ✓ Inclusión de todo el personal en el plan de seguridad, no solo directivas: la seguridad informática únicamente se puede estructurar si todo el personal conoce

sobre él, esto es, que cada usuario del sistema reconozca su importancia y su labor dentro del plan de seguridad informática, acogiendo su participación en el desarrollo de sus actividad fundamentadas en el plan de seguridad informático; no involucrar a todo el personal en el plan de seguridad, representaría indudablemente la creación de una vulnerabilidad en los sistemas que pueda afectar a toda la organización.

- ✓ Reconocimiento anti-phishing: ahora que el teletrabajo a aumentado, que más personas se encuentran en sus equipos, es muy común ver el crecimiento de las comunicaciones a través de los medios digitales, la mensajería electrónica, o el uso del correo electrónico, representa una herramienta muy importante para el desarrollo de las actividades laborales, y así mismo, es el medio ideal para ser contactados por terceros, bien sea ofreciendo servicios o premios, o también advirtiendo sobre las posibles pérdidas de los mismos; esto último, es sin duda alguna, una de las estrategias más comunes por los ciberdelincuentes, lo que hace importante que cada usuario tenga la capacidad de reconocer en la mayor medida posible dichas amenazas que pueden resultar en graves consecuencias para la seguridad de la información y de la organización.

- ✓ Importancia y establecimiento de la seguridad en contraseñas: además de resaltar las características que hacen segura o robusta una a contraseña, así como de su actualización periódica o constante, se debe concientizar sobre la importancia de la privacidad que se le debe otorgar, ya que el compartir cuentas, usuarios, privilegios o accesos, se ve como una práctica muy común y aceptable en muchas organizaciones, lo que en realidad representa una falla de seguridad grave que requiere de la privacidad en el uso de contraseñas.

- ✓ Concientizar sobre la ingeniería social: el manejo de la información debe entenderse también desde el punto de vista del valor de la información, muchas veces no se reconoce el alcance que puede ofrecer la manipulación es esta, y se

procede revelar o publicar información sin considerar la gravedad o alcance, lo que permite crear una brecha muy grande sobre la seguridad informática; depende en muchos casos de los usuarios del sistema, asegurar los tres pilares de la seguridad (integridad, disponibilidad, confidencialidad), pues son ellos quienes finalmente podrían de manera consciente o inconsciente revelar información delicada o exponerse y exponer a la entidad a una vulneración.

- ✓ Identificación de tipos de archivos básicos y peligrosos: con respecto al malware, es importante que el usuario esté en capacidad de reconocer directamente aquellas amenazas que muchas veces a simple vista se pueden detectar, pero esto solo es posible si los usuarios del sistema, son capaces de reconocer anomalías en los archivos recibidos, pequeñas comprobaciones como la extensión del archivo, peso, o ruta de enlace, podrían hacer la gran diferencia entre la instalación de un virus en toda la organización o la detección temprana de este.

- ✓ Uso de la mesa de ayuda, soporte y asistencia del área TI: si bien es cierto que determinadas amenazas requieren de conocimientos avanzados para detectarse o resolverse satisfactoriamente, también lo es que se debe ofrecer absoluta asistencia para atender las solicitudes o consultas de los usuarios, ya que es importante que ante la mínima sospecha, los usuarios sientan el acompañamiento inmediato de un profesional para guiar y atender las solicitudes, así, a modo de prevención, se propicia un ambiente digital más seguro.

- ✓ Proponer entrenamiento o repaso atractivo y entretenido: Capacitar al personal sobre temáticas que pueden resultar complejas de asimilar en algunos casos, requiere también de la implementación de herramientas que permitan la apropiación de conocimientos en forma entretenida, como por ejemplo presentaciones en PowerPoint, animaciones en Powtoon, cuestionarios lúdicos en Cerebriti, entre otros; ya que la idea no es relatar una clase de historia con complicadas terminologías técnicas, sino generar información puntual, fácil de

relacionar y poner en práctica para que se fundamente y consolide con el tiempo la cultura informática basada en buenas prácticas de seguridad de la información y la apropiación de los objetivos del plan de seguridad informática.

- ✓ Reforzar los mensajes importantes con revisiones y repetición: la práctica constante a través de la información clara, permiten crear hábitos entre los usuarios de los sistemas que al final de cuentas, proveen de seguridad, funcionalidad y rentabilidad en el desarrollo de las actividades y procesos, ya que si las capacitaciones se presentan como temas de un solo repaso, o una sola oportunidad, no se da la importancia necesaria a la implementación de las buenas prácticas, y su prioridad se vería disminuida por el desarrollo de otras actividades de los procesos de la organización; de allí que tras unos meses de haber realizado una única capacitación, muy pocos usuarios de los sistemas recodarán sobre los temas informados su aplicación o especialmente, su importancia y significado puntual.

- ✓ Crear un ambiente de refuerzo y motivación, no de presión, pero sí de responsabilidad: como se expuso anteriormente, cada día aparecen cientos de nuevas amenazas informáticas, las cuales son cada vez más robustas o de mayor capacidad de infiltración y afectación; lo cual se traduce en un esfuerzo constante por instruir al personal y evaluar la criticidad de un posible impacto[92], viéndose necesario un constante ajuste a las actividades y procedimientos de la organización, así como también a las políticas de la organización hacia sus empleados o usuarios del sistema, lo en algunos casos podrá ser percibido por los trabajadores, como una constante limitación que genera presión si no se han compartido y asimilado claramente los objetivos del plan de seguridad informática, cuyo objetivo siempre será el de proteger los activos e información y mitigar los riesgos a los que se está expuesto.

[92] ESET. [Sitio web]. Guía de Teletrabajo. 2020. [Consulta: 25 de enero 2021]. Disponible en: https://empresas.eset-la.com/novedad/guia-de-teletrabajo

6.4.2 Asociar buenas prácticas de seguridad informática

Tanto para los usuarios de los sistemas y recursos, como para el área de TI, es necesario adaptar una serie de buenas prácticas de seguridad informática que provean de mayor seguridad y mejor respuesta ante los posibles incidentes de seguridad, para ello, se describe a continuación algunas de las prácticas más recomendables que se pueden comprobar o implementar diariamente:

- ✓ Actualización de sistemas y aplicaciones: Muchas veces los usuarios de los sistemas consideran este tipo de actividades como una molestia para el desarrollo de sus actividades, pero contrario a esto, las actualizaciones de los sistemas operativos, de las aplicaciones como antivirus o del software de gestión de bases de datos, tienen la finalidad de cubrir vulnerabilidades encontradas y optimizar su rendimiento; de tal manera, que si las actualizaciones no se realizan periódicamente, es mucho más probable que un sistema sea vulnerado con mayor facilidad.

- ✓ Contraseñas seguras: establecer una contraseña de seguridad robusta o con las características adecuadas, permite que haya una mayor dificultad en su descifrado o captura, puesto que tanto la longitud de la contraseña, como la combinación alfanumérica y de caracteres especiales son supremamente importantes de implementar, además de el hecho de mantener la privacidad de la misma y realizar una actualización periódica (cada mes o cada dos meses) dependiendo del nivel de seguridad requerido, lo que permite que usuarios malintencionados o extrabajadores, no puedan hacer uso ilegal o no autorizado de los servicios, que en el peor de los casos dirigen la organización de ciberataques a la organización..

- ✓ Gestión de copias de seguridad: tanto el proceso de realizar copias de seguridad para respaldar la información, como el proceso de almacenamiento y restablecimiento, deben llevar una guía o lista de chaqueo que permita comprobar

regularmente que todos los procesos de copiado, almacenamiento y restauración, funcionen correctamente[93], de manera que una copia de seguridad sólo será útil cuando se tiene la garantía de que es posible recuperar lo perdido, y esta garantía solo se puede obtener a través de la comprobación y/o validación de los procesos de backup y restauración.

- ✓ Gestión de usuarios: La gestión de usuarios se convierte en una herramienta importante de seguridad informática, puesto que permite asegurar el acceso correspondiente a cada usuario según su perfil y también permite retirar o agregar permisos según sea la necesidad, de manera que si por ejemplo, un trabajador se retira de la organización, su usuario en el sistema y su línea de acceso también deberán ser deshabilitados para evitar cualquier posible acceso desautorizado o robo de identidad y credenciales de acceso; por otro lado, al prestar servicios a usuarios temporales, se debe llevar un registro que permita su remoción del sistema para liberar recursos y optimizar los servicios.

- ✓ Pruebas de Planes de Contingencia: aunque posiblemente esta no sea una tarea diaria, muchas veces suele ignorarse y al igual que comúnmente sucede con la realización de restauración de backup, no se suele comprobar su eficacia o funcionamiento correcto. Por este motivo se deben realizar “simulacros” en caso de que se materialice una amenaza informática. Es importante probar los equipos que se encuentren como respaldo, sistemas auxiliares, líneas secundarias para contingencia etc., debido a que, en algunos casos, se puede estar haciendo una copia de seguridad de una base de datos y el día en que se necesita realizar la restauración de la información “salvaguardada”, ésta no fue se realizó, no se programó correctamente, o no está copiando lo que se quería. De esta manera, ante un en caso de un incidente grave, es posible volver a la normalidad lo antes posible sin afectar mayormente los procesos de la empresa.

[93] INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Decálogo de buenas prácticas de seguridad en un Departamento de Informática. INCIBE. 2020. [Consulta: 27 de enero 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-departamento-informatica

Algunas otras buenas prácticas[94] básicas que los usuarios de los sistemas pueden aplicar directamente en el desarrollo de sus actividades son:

- ✓ No descargar actualizaciones desde sitios no oficiales o de dudosa reputación. Las actualizaciones de sitios no oficiales pueden significar un potencial riesgo de infección por malware.
- ✓ Deshabilitar la ejecución o reproducción automática de dispositivos USB. Los dispositivos USB representan un vector de ataque muy común para la propagación de malware, sobre todo, de gusanos o virus troyanos.
- ✓ Habilitar la visualización de archivos ocultos por el sistema. Puesto que la mayoría de los códigos maliciosos se ocultan como archivos del sistema con el mismo tipo de atributos.
- ✓ Habilitar la visualización de las extensiones de archivos para identificar el tipo de archivo descargado y no ser víctima de malware por la técnica común de la doble extensión de archivo.
- ✓ No abrir los archivos adjuntos de correos spam.
- ✓ Cuando se reciban archivos adjuntos, se debe prestar atención a las extensiones de los mismos, para evitar técnicas de engaño como la doble extensión o también de espacios entre el nombre del archivo recibido y la extensión del mismo.
- ✓ Evitar publicar la dirección de email o números de contacto en sitios web de dudosa reputación o públicos como foros, chats, blogs, entre otros. Esto minimiza la posibilidad de que dichos datos hagan parte de la base de datos de los spammers o ciberdelincuentes.
- ✓ No responder en ningún caso el correo spam, puesto que se confirma que la dirección está activa. Preferiblemente optar por ignorarlos y/o borrarlos.
- ✓ Evitar la difusión o reenvío de mensajes de tipo cadena, ya que su finalidad es la recolección de direcciones de correo activas, o difusión de información falsa o que carece de soporte real.
- ✓ Configurar el doble factor de autenticación y/o pregunta secreta, además, de una

[94] HURTADO, D. Manual de buenas prácticas de seguridad informática en redes domésticas. 2021. [Consulta: 5 de junio 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/39430/dfhurtadov.pdf?sequence=3&isAllowed=y

forma que no sea adivinable para fortalecer aún más la seguridad de la cuenta.

- ✓ Tener en siempre en cuenta que las entidades bancarias y financieras, en ningún caso no solicitan datos confidenciales a través de este tipo de medios electrónicos como correos o mensajes.
- ✓ Verificar siempre los correos que dicen ser emitidos por entidades y que brindan servicios u ofertas, o solicitan actualización de datos sensibles ya que por lo general son métodos de Ingeniería Social
- ✓ No hacer clic sobre enlaces, botones, imágenes o hipervínculos que aparecen en el cuerpo de los correos electrónicos sospechosos, ya que pueden redireccionar hacia sitios web falsos o montados en clonación, o hacia la descarga de malware.
- ✓ Verificar que la dirección del sitio web al cual se desea acceder o se ha ingresado comience con el protocolo seguro “HTTPS”. Lo que significa que la página web es segura y que toda la información depositada en la misma viajará de manera cifrada; los sitios con “HTTP” permiten la captura de información.
- ✓ En lo posible, comunicarse por teléfono directamente con la compañía para validar la información y para descartar la posibilidad de ser víctimas de un engaño, especialmente cuando se tenga dudas sobre la legitimidad de un mensaje.
- ✓ No compartir contraseñas, direcciones, números o fotos de tarjetas de crédito, o cualquier otro tipo de información sensible a través del correo electrónico, chats o sitios sociales, ya que la información podría ser interceptada y robada.
- ✓ Evitar el visitar sitios web con contenidos que, dependiendo el país, son identifican como ilegales, como por ejemplo los que ofrecen cracks, licencias y programas gratis que en realidad son de pago; ya que usualmente contienen malware.
- ✓ Impedir la ejecución de archivos y el otorgamiento de permisos de acceso o notificaciones desde sitios web en los cuales no se haya comprobado previamente si es necesario y si se solicitó dicho servicio.
- ✓ No realizar la instalación de complementos emergentes e innecesarios extras como barras de tareas, optimizadores del sistema, antivirus o que ofrecen diferentes servicios y premios u ofertas sin verificar previamente su autenticidad.

- ✓ Mantener activo y actualizado el software antivirus, puesto que esto permite detectar códigos maliciosos en tiempo real, actividad sospechosa y validar cada archivo descargado.
- ✓ Evitar en lo posible el acceso a servicios bancarios web desde lugares públicos o usando redes de navegación públicas como las de bibliotecas, cafés, hoteles y centros comerciales entre otros, para evitar que se capturen datos privados.
- ✓ Si se navega sobre conexiones a internet públicos, es recomendable eliminar el historial de navegación, acceso, archivos temporales, caché, cookies, contraseñas guardadas y formularios donde se haya ingresado datos.
- ✓ Deshabilitar o realizar la desconexión Wifi cuando no se esté usando, especialmente si se está conectado a una red de internet pública.
- ✓ Procurar en lo posible no publicar información sensible o considerada como confidencial, puesto que ciberdelincuentes o personas con malas intenciones pueden usar esta información con fines de beneficio propio.
- ✓ Evitar la publicación de fotografías o vídeos propios o de familiares. Puesto que pueden ser robados, manipulados y utilizados para complementar actos delictivos, incluso fuera del ámbito informático.
- ✓ Mantener la privacidad del perfil en las redes sociales.
- ✓ Si se tiende a aceptar contactos espontáneos, es recomendable verificar en lo posible su existencia o historia y que realmente son quien dice ser.
- ✓ Si se debe acceder a cuentas electrónicas personales desde lugares públicos, es recomendable deshabilitar la opción de inicio automático, y comprobar el almacenamiento automático de contraseñas, de esta forma no queda la dirección (ni la contraseña) grabada automáticamente, vitando que terceros inicien sesión de manera automática.
- ✓ Si se transporta información confidencial en estos dispositivos de almacenamiento extraíble, es recomendable cifrarla, existen herramientas gratuitas para ello. Así, en caso de pérdida o robo del dispositivo, la información no podrá ser vista por terceros.

6.4.3 Determinar planes de capacitación

La educación a través de la capacitación a los usuarios del sistema debe considerarse un pilar importante, en donde todos los usuarios logren una cultura y consciencia de los riesgos a los cuales pueden verse expuestos y cuáles son los cuidados y acciones preventivas que deben tener al ingresar a internet o interactuar con dispositivos y sitios ajenos a la compañía. Si el usuario no conoce los riesgos presentes en su entorno digital a los cuales expone la información de la empresa, e incluso la propia, es más probable que este sea más fácilmente víctima de muchas amenazas. Todos los usuarios del sistema deben comprender que así se esté por fuera de la oficina, el dispositivo desde el cual: trabaja, estudia o se divierte, puede representar una "puerta" a toda la organización y como tal los usuarios deben garantizar un uso adecuado.

Para lo anterior, es necesario que se realice planes de capacitación constantes, que permitan mantener el ejercicio de los temas establecidos en los objetivos de capacitación y que por supuesto, permitan ser sondeados, evaluados y reformados para lograr un alcance absoluto en el cumplimiento de los objetivos de capacitación, recordando, que el beneficio general de este esfuerzo pretende cuidar tanto a los usuarios como a la organización. A continuación, se menciona los pasos a tener en cuenta para establecer un programa de capacitación:

- **Formulación de la estrategia:** Teniendo en cuenta los objetivos estratégicos de la organización, sus necesidades de desarrollo y capacitación del personal, se formula una estrategia de capacitación en conjunto con las directivas.
- **Definición de los objetivos de la capacitación:** Los objetivos deber ser formulados en de acuerdo con su entorno tecnológico y los requerimientos de la organización. El objetivo principal será el generar una cultura a través de la concientización sobre el uso de la tecnología y sus riesgos inherentes y derivados del acceso a internet.

- **Elaboración del presupuesto:** Si se requiere de la asistencia de un tercero para la ejecución de los planes de capacitación o de la adquisición de elementos para tal fin, se deben definir los ítems identificados y establecer los costos de cada uno.
- **Definir el contenido temático:** de la sesión, curso, taller o seminario a trabajar, teniendo en cuenta los objetivos de la capacitación y los temas que serán desarrollados en la capacitación. Por ejemplo, se pueden definir los siguientes temas en diferentes sesiones que se pueden programar una vez a la semana cada una, como se puede evidenciar en la siguiente tabla (ver cuadro 9):

Cuadro 9. Distribución de temas por sesión.

Sesión	Vulnerabilidades	Amenazas
1	Contraseñas débiles	Accesos no autorizados
	Sistemas y dispositivos desactualizados	Ejecución de exploit.
2	Ausencia de protección en endpoint	Infección con código malicioso
	Conexión a redes públicas/desconocidas	Robo o captura de información, infección del dispositivo.
3	Falta de respaldo de información	Pérdida de dispositivos
	Dispositivos sin cifrado	Pérdida de la privacidad de la información

Fuente: El autor.

- **Disponer medios y recursos didácticos:** Se debe prever la necesidad de contar con los elementos y el soporte tecnológico idóneo para desarrollar la capacitación de una manera efectiva y visualmente agradable o entretenida. Esto incluye además la identificación del espacio necesario (aulas, salas de reunión o conferencia, aulas de proyecciones o laboratorios informáticos, etc.).
- **Determinar la duración y el cronograma:** Las sesiones no deben convertirse en largas jornadas que afecten el rendimiento y desarrollo normal de las actividades de la organización. Es recomendado también, desarrollar las sesiones en horarios donde no afecten el inicio o cierre de labores según la disposición analizada, a su vez, estas capacitaciones deben programarse dentro del horario de trabajo, de

modo que los trabajadores se sientan retribuidos por capacitarse y no sientan rechazo alguno por la capacitación. Por ejemplo, teniendo en cuenta el "*cuadro 9*", se podría programar algunas sesiones así (ver cuadro 10):

Cuadro 10. Distribución de horarios.

Sesión	Jornada	Vulnerabilidades	Amenazas
Semana 1	AM	Contraseñas débiles	Accesos no autorizados
	11 am - 12 am	Sistemas y dispositivos desactualizados	Ejecución de exploit.
Semana 2	PM	Ausencia de protección en endpoint	Infección con código malicioso
	5 pm - 6 pm	Conexión a redes públicas/desconocidas	Robo o captura de información, infección del dispositivo.

Fuente: El autor.

- **Seleccionar a los participantes:** Aunque es claro que la idea es capacitar a todo el personal en los temas seleccionados, se debe ordenar los grupos de trabajo en caso de que por fuerza mayor algunos no puedan asistir, de manera tal que se les permita elegir una segunda opción en otro horario o día de disponibilidad.
- **Seleccionar a los capacitadores:** Tanto si la organización cuenta con personal idóneo para realizar las jornadas de capacitación, como como cuando se contrata un tercero para ello, es importante saber quiénes son los capacitadores y cuáles son sus competencias para el desarrollo de estas actividades.
- **Realizar un sondeo de conocimientos:** Determinar los conocimientos previos con los que cuenta el personal sobre los temas a tratar, permite avanzar más rápidamente o profundizar en mayor detalle en algunos temas con el fin de agilizar las actividades a desarrollar y utilizar eficientemente el tiempo dispuesto.
- **Generar un sistema de evaluación:** Establecer un proceso de evaluación en función de los objetivos de la capacitación, que permita verificar la apropiación del conocimiento propuesto y el desarrollo o metodología de capacitación empleados. Para ello se puede considerar algunos criterios básicos como son:

- ✓ Reacciones. Cómo responde el personal de la organización después de la capacitación, referente a los temas tratados y al proceso en general.
- ✓ Aprendizaje. Cuánto conocimiento se apropió efectiva y evidentemente, y que habilidades y destrezas se han desarrollado.
- ✓ Comportamiento. Identificar si el personal tras la capacitación tiene una perspectiva diferente frente a los temas de capacitación, y si esta positiva (reconocimiento, difusión y socialización) o negativa (rechazo, comentarios negativos o que denoten una perspectiva de desinterés).
- ✓ Resultados o costo beneficio. Determinar el impacto de la capacitación en indicadores directamente relacionados con la misma, por ejemplo: en la reducción de incidentes de seguridad, llamados de atención, pérdida de información o filtrado de información reducido, mejoras en la productividad, avances en calidad, etc.

Esto permite generar un plan de capacitaciones orientado a la mejora continua, que apoya incluso diferentes implementaciones como la del teletrabajo, en donde claramente es crucial el uso de una cultura informática que permita la ejecución de dichas tareas con total seguridad y de la manera más eficiente para toda la organización.

Es clave considerar siempre los objetivos de la organización y por ende los objetivos de seguridad que juegan un papel importante en el desarrollo de las actividades normales de cada uno de los trabajadores, teniendo en cuenta además, que para que estas actividades sean exitosas, es necesario mantener un constante monitoreo del uso de los activos de información de la organización para detectar posibles riesgos o amenazas informáticas que pudieran materializarse, y en caso de detectar una nueva amenaza, gestionar oportunamente un plan de socialización que permita a todos los usuarios del sistema reconocer la vulnerabilidad y tomar acciones preventivas.

7 CONCLUSIONES

El desarrollo diario del malware y de las diferentes amenazas informáticas, permiten establecer a través de su estudio, que los usuarios de los sistemas se enfrentan a cientos de posibilidades de ser víctimas de ciberataques o de que su privacidad digital sea vulnerada; lo que refleja la necesidad urgente de la apropiación de medidas y salvaguardas en las organizaciones frente a estas vulnerabilidades, aunque a pesar de los esfuerzos de las organizaciones y los gobiernos, en la actualidad, los costos derivados de la reparación de daños causados por la materialización de los diferentes tipos de amenazas, siguen siendo demasiado altos en todo el mundo.

El impacto a nivel global hace que todo tipo de amenazas informáticas deban ser totalmente reconocidas y evaluadas por las organizaciones de manera constante y objetiva. Teniendo en cuenta que en la actualidad se puede comprobar, incluso en tiempo real, reportes sobre nuevas amenazas informáticas y que además es esto, Colombia se mantiene usualmente sobre el top 15 de los países más atacados del mundo, postulándolo como uno de los objetivos de ataques informáticos más preferidos entre los ciberdelincuentes, se puede concluir que es evidente que esta es una situación resultante de la falta de concientización tanto de las organizaciones como de forma personal por cada usuario de las tecnologías, lo que ha generado bajos índices de seguridad en la información y la ciberseguridad en las organizaciones.

Considerar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), que se soporte o haga uso de en una metodología de evaluación de riesgos como MAGERIT, debe ser una prioridad actual de toda organización, ya que esta facilitará una disposición eficiente hacia la implementación de planes, sistemas y recursos tecnológicos; que permitan salvaguardar y generar protección a la información y los activos de la organización, teniendo en cuenta que de verse vulnerados estos, no solo representa una perdida economía para la organización, sino que también afecta

directamente la imagen, la confianza y la funcionalidad de la organización ante sus clientes, aliados y proveedores actuales y los potenciales, así como también podrían verse afectados terceros a los cuales se les ofrece determinados servicios.

La seguridad informática debe importarles no solo a las empresas, sino también a entidades del gobierno, universidades, escuelas, hospitales, sociedades, fundaciones, y en general, a todo aquel que tenga un teléfono, un computador o una cuenta bancaria; pues de cualquier forma todos son objetivos potenciales de ser víctimas de la ciberdelincuencia. Por esto es importante implementar programas de capacitación constantes, tanto para los profesionales y administradores de TI, como para el personal en general, ya que de los usuarios del sistema es en todo caso, de quien más depende la seguridad de la información, de los sistemas, pues de ellos será el uso de los sistemas y la correcta manipulación de cada dispositivo e incluso de su mismo comportamiento en la web, ya que aunque el administrador provea de las últimas implementaciones tecnológicas de seguridad, no servirán de mucho si los usuarios serán quienes al final los deshabiliten, creen accesos vulnerables o desconfiguren los sistemas por intereses personales o por inconsciencia.

8 RECOMENDACIONES

Es importante iniciar por acordar la implementación de un Sistema de Gestión de Seguridad Informática (SGSI), bien sea adquiriendo la infraestructura tecnológica necesaria y el personal idóneo para su administración, como también es posible contratar los servicios de gestión a una entidad tercera que se encargue de ofrecer los servicios de seguridad de la información y ciberseguridad a la entidad.

En caso de que se disponga de los recursos y espacios necesarios para implementar, administrar y soportar el SGSI, es importante iniciar por implementar una metodología de evaluación de riesgos basada en normatividad de gestión de la seguridad de la información, ya que estas metodologías y normas, pretenden facilitar la implementación del SGSI guiando y generando recomendaciones que se pueden tener en cuenta a la hora de implementarlo en la organización, enfocándose en el modelo de negocio y los objetivos de la entidad con la finalidad de que su implementación no suponga un problema o resulte en afectación de los procesos y actividades de la entidad.

Tener conciencia sobre las buenas prácticas de seguridad informática, representa en sí misma una oportunidad evidente en la generación de una protección integral, pues este tipo de prácticas pretenden dificultar y/o eliminar idealmente la mayor parte de las vulnerabilidades detectadas hasta la actualidad, teniendo en cuenta que estas prácticas se enfocan mayormente al uso adecuado de los dispositivos y de la web, desde los cuales se inician muchas de las actividades de los ciberdelincuentes.

La gestión del correo electrónico corporativo, el uso de los equipos portátiles y celulares de la organización, deben estar siempre reglamentados sobre su uso, transporte y cuidado, ya que estos representan un riesgo mayor al tener la facultad de portabilidad que permite su traslado o manipulación fuera de la entidad; es por lo anterior, que se debe concientizar prioritariamente sobre los riesgos que conllevaría su pérdida o infiltración a través de la pérdida de control sobre el mismo.

Sin lugar a dudas, la tecnología desarrolla un papel muy importante frente a la respuesta contra amenazas informáticas, por lo que considerar establecer mecanismos de seguridad perimetrales, ayudará en gran medida a la detección oportuna de amenazas cibernéticas, muchas herramientas de gestión unificada de amenazas o también conocidas como UTM, integran de manera efectiva varias herramientas de protección que incluyen: firewall, antispam, antispyware, anti-phishing, filtrado de contenidos, uso de reglajes y funciones antivirus, permiten una respuesta y detección temprana de muchas de las amenazas cibernéticas a las que se ven expuestas las organizaciones, por lo que su implementación representa un gran soporte en protección de toda la organización.

Garantizar la capacidad de recuperación y continuidad del negocio frente a un ciberataque, debe ser uno de los objetivos principales de implementar un SGSI, para ello, es importante que se desarrolle la capacidad de ciberresiliencia, con lo cual se pretende gestionar de manera adecuada las respuestas ante los ciberataques y garantizar la continuidad del negocio, la seguridad de la información y la funcionalidad de las redes de la entidad; garantizando que la organización siga funcionando durante los ciberataques.

Independientemente de la complejidad de la amenaza, es importante que una organización siempre se prepare para responder ante la peor situación, lo cual por supuesto, dependerá no solo del equipo de respuestas ante amenazas informáticas, sino que se hace propicia la participación de todo el personal de la entidad, lo cual involucra a todo el personal y directivos, los cuales tienen papeles y responsabilidades sobre el plan de seguridad informática.

Finalmente, es importante lograr generar una cultura informática derivada de las buenas prácticas de seguridad aprendidas a través de la concientización que se genera con la implementación de planes de capacitación basados en el análisis de riesgos que puede resultar de la implementación de las metodologías de evaluación de riesgos como la presentada en este documento.

9 BIBLIOGRAFÍA

ÁLVAEZ P, et al. Virus Informáticos. Universidad de la Coruña. 2008. [Consulta: 11 de septiembre 2020]. Disponible en: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

AREATECNOLOGIA. [Sitio web]. Sistemas Operativos. 2019. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.areatecnologia.com/sistemas-operativos.htm

AVAST. [Sitio web]. Qué es la ingeniería social y cómo evitarla. 2020. [Consulta: 1 de noviembre 2020]. Disponible en: https://www.avast.com/es-es/c-social-engineering

AVG. [Sitio web]. ¿Qué es el malware? Cómo funciona el malware y cómo eliminarlo. 2019. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.avg.com/es/signal/what-is-malware

BANCO SANTANDER. [Sitio web]. ¿Qué es Phishing, Smishing y Vishing? ¿Cómo protegerse?. [Consulta: 13 de septiembre 2020]. Disponible en: http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo_Sobre_Ransomware.pdf

BAVERA, M. Car Hacking. 2015. [Consulta: 24 de septiembre 2020]. Disponible en: http://jeuazarru.com/wp-content/uploads/2015/11/CarHacking.pdf

BBC NEWS. [Sitio web]. Criptografía: qué es y por qué deberías usarla en tu teléfono para que no te espíen. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.bbc.com/mundo/noticias-50862657

CAIVIRTUAL. [Sitio web]. Delitos en Colombia. [Consulta: 22 de noviembre 2020]. Disponible en: Https://caivirtual.policia.gov.co/

CARVAJAL A. Introducción a las técnicas de ataque e investigación. 2017. [Consulta: 10 de octubre 2020]. Disponible en: http://acistente.acis.org.co/typo43/fileadmin/Articulos/TecnicasAtaqueComputacionForense.pdf

CENTRO CIBERNÉTICO POLICIAL NACIONAL. Tendencias Cibercrimen Colombia 2019-2020. 2019. [Consulta: 10 de octubre 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

CENTRO CIBERNÉTICO POLICIAL. [Sitio web]. Informe tendencias de Cibercrimen 2019-2020. pp. 1-18. [Consulta: 7 de diciembre 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CISET. [Sitio web]. Definición de Hardware. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.ciset.es/glosario/451-hardware

CLARKE J. SQL Injection Attacks and Defense. 2da Ed. 2012. [Consulta: 4 de septiembre 2020]. Disponible en: https://doc.lagout.org/security/SQL%20INJECTION%20SECOND%20EDITIOn/SQL%20INJECTION%20SECOND%20EDITIOn.pdf

COPNIA. [Sitio web]. Ley 842 de 2003. Diario Oficial No. 45.340. [Consulta: 18 de septiembre 2020]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

CUMULUS MEDIA. (2020). [sitio web]. Reporte Anual – Sprout Social. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.annualreports.com/Company/sprout-social-inc

DANS, E. Everything is hackable: get over it. 2015. [Consulta: 24 de septiembre 2020]. Disponible en: https://medium.com/enrique-dans/everything-is-hackable-get-over-it-a3ca75a0c093

DELOITTE. [Sitio web]. Riesgos de TI. 2016. [Consulta: 3 de septiembre 2020]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf

DÍAZ V. Seguridad en Bases de datos y aplicaciones Web. s.f. [Consulta: 4 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/62886/4/Seguridad%20en%20bases%20de%20datos_M%C3%B3dulo%201_Introducci%C3%B3n.pdf

DISETE COMUNICACIONES. [Sitio web]. Qué son las políticas de seguridad informática y por qué tu empresa debe tener una. 2020. [Consulta: 20 de septiembre 2020]. Disponible en: https://disete.com/que-son-las-politicas-de-seguridad-informatica-y-por-que-tu-empresa-debe-tener-una/

ENCICLOPEDIA CUBANA. [Sitio web]. Usuario (Informática). 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.ecured.cu/Usuario_(Inform%C3%A1tica)

ENTERPRISEIT. [Sitio web]. Controles generales de tecnologías de información. [Consulta: 3 de septiembre 2020]. Disponible en: https://enterpriseit.cl/controles-generales-de-tecnologias-de-informacion/

EPSTEIN Kevin. SUNNYVALE, Calif., Sept. 09, 2019 (GLOBE NEWSWIRE) -- Proofpoint, Inc. [Consulta: 10 de septiembre 2020]. Disponible en: https://www.globenewswire.com/

ESET. [Sitio web]. Guía de Teletrabajo. 2020. [Consulta: 25 de enero 2021]. Disponible en: https://empresas.eset-la.com/novedad/guia-de-teletrabajo

ESET. [Sitio web]. Security Report LATAM 2020. [Consulta: 5 de diciembre 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

ESET. [Sitio web]. Todo sobre el Ransomware. 2016. [Consulta: 13 de septiembre 2020]. Disponible en: http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo_Sobre_Ransomware.pdf

EUROINNOVA. [Sitio web]. Qué es la ofimática. s.f. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.euroinnova.co/blog/11-4-18/manejo-de-la-ofimatica-con-el-curso-de-office

GAONA, K. Análisis de Vulnerabilidades de Ciberseguridad en Desfibriladores Cardíacos Implantados. 2018. [Consulta: 24 de septiembre 2020]. Disponible en: https://medium.com/enrique-dans/everything-is-hackable-get-over-it-a3ca75a0c093

GESTIONYAUDITORIATI. [Sitio web]. Aplicación de Estándares de TI. 2012. [Consulta: 3 de septiembre 2020]. Disponible en: https://gestionyauditoriati.com/2012/09/07/aplicacion-de-estandares-de-ti/

GOBIERNO DE ESPAÑA. [Sitio web]. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2012. Ed. Ministerio de Hacienda y Administraciones Públicas [Consulta: 15 de enero 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

HAMMUD E. Seguridad en servidores DNS. 2014. [Consulta: 24 de septiembre 2020]. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/21853/Tesis%20Elihu%20.pdf?sequence=1&isAllowed=y

HURTADO, D. Manual de buenas prácticas de seguridad informática en redes domésticas. 2021. [Consulta: 5 de junio 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/39430/dfhurtadov.pdf?sequence=3&isAllowed=y

IBM. [Sitio web]. Data breach. s.f. [Consulta: 10 de octubre 2020]. Disponible en: https://www.ibm.com/security/data-breach

INCIBE. [Sitio web]. Protección de la página Web. s.f. [Consulta: 18 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/62886/4/Seguridad%20en%20bases%20de%20datos_M%C3%B3dulo%201_Introducci%C3%B3n.pdf

INDICE.MX. [Sitio web]. Auditorías de TI. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.indice.mx/nuestros-servicios/auditorias-de-ti/

INFOSPYWARE. [Sitio web]. ¿QUÉ ES EL PHISHING? s.f. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Decálogo de buenas prácticas de seguridad en un Departamento de Informática. INCIBE. 2020. [Consulta: 27 de enero 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-departamento-informatica

INTECO. Implantación de un SGSI en la empresa. 2020. [Consulta: 9 de septiembre 2020]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [Sitio web]. ISO 27002 A6 Organización de la seguridad de la información (normaiso27001.es). 2013. [Consulta: 20 de enero 2021]. Disponible en: https://normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion/

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [Sitio web]. ISO/IEC 27002:2013. Buenas prácticas para gestión de la seguridad de la información. 2013. [Consulta: 17 de enero 2021]. Disponible en: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

INTERNET-DIDACTA. [Sitio web]. Qué es el E-Mail o Correo electrónico. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.internet-didactica.es/e-mail-correo-electronico/

IONOS. [Sitio web]. SYN flood: variantes y medidas defensiva. 2020. [Consulta: 24 de septiembre 2020]. Disponible en: https://www.ionos.es/digitalguide/servidores/seguridad/syn-flood/

ISO. [Sitio web]. ISO/IEC Guide 60 (es). 2015. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:guide:60:ed-2:v1:es

KALI. [Sitio web]. What is Kali Linux, and what is a Penetration Testing Distribution? 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.kali.org/features/

KASPERSKY. [Sitio web]. Qué es Ciberseguridad. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KEENLAB. [Sitio web]. Experimental Security Assessment of BMW Cars. 2018. [Consulta: 24 de septiembre 2020]. Disponible en: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-

LAMANNA Carlos. [blog]. Dato, información, sistema. En: Introducción a la Informática. s.f. Instituto Superior Nuestra Señora de la Paz. [Consulta: 3 de septiembre 2020]. Disponible en: https://datosuno.wordpress.com/unidad-1/introduccion/

LÓPEZ, G. Servidores seguros. 2020. [Consulta: 18 de septiembre 2020]. Disponible en: https://pccito.ugr.es/~gustavo/ss/teoria/seguridad/seguridad.pdf

MALWAREBYTES. Cryptojacking. 2018. [Consulta: 25 de septiembre 2020]. Disponible en: https://es.malwarebytes.com/cryptojacking/

MALWAREBYTES. [Sitio web]. Todo sobre el hackeo 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://es.malwarebytes.com/hacker/

MARTÍNEZ C. Seguridad por capas frenar ataques de Smishing. 2018. [Consulta: 24 de septiembre 2020]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiyj9ndhq7tAhVCnOAKHXLtDUgQFjAAegQIBRAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6255067.pdf&usg=AOvVaw2DyOgV0GnKbXk0KyX_L4Tc

MARTINEZ FERREL Ernesto, Las amenazas informáticas. [en línea]. 2018. [Consulta: 3 de septiembre 2020]. Disponible en: https://sites.google.com/site/lasamenazaslainformatica/

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Iniciativas del sector TI en Colombia. 2020. [Consulta: 14 de septiembre 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Iniciativas/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Internet, ¿qué es? ¿para qué sirve? 2015. [Consulta: 15 de septiembre 2020]. Disponible en: https://www.enticconfio.gov.co/internet-que-es-para-que-sirve

NÓVOA M y PÉREZ O. Sniffers: Espías en la Red. s.f. [Consulta: 10 de octubre 2020]. Disponible en: http://index-of.co.uk/Tmp/SniffersPDF.pdf

OFICINA DE SEGURIDAD DEL INTERNAUTA. [Sitio web]. ¿Qué es una vulnerabilidad Zero Day? 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.osi.es/es/actualidad/blog/2020/08/28/que-es-una-vulnerabilidad-zero-day

PABÓN, J. La criptografía y la protección a la información digital. s.f. [Consulta: 25 de septiembre 2020]. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

PATARROYO S. Ingeniería social, una técnica subestimada por desconocimiento. s.f. [Consulta: 29 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

POLICÍA NACIONAL DE COLOMBIA. [sitio web]. Tendencias Cibercrimen Colombia 2019-2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

RACCIATTI. Técnicas de SQL Injection. V.1.5. 2012. [Consulta: 4 de septiembre 2020]. Disponible en: https://doc.lagout.org/security/SQL%20INJECTION%20SECOND%20EDITIOn/SQL%20INJECTION%20SECOND%20EDITIOn.pdf

RAFFINO María. Dato en informática. [en línea]. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://concepto.de/dato-en-informatica/

REDESZONE. [Sitio web]. Qué tipos de redes informáticas existen. 2019. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/tipos-redes-informaticas/

REDHAT. [Sitio web]. ¿Qué es la infraestructura de TI? 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

RIVADENEIRA E. STUXNET, La primera ciberarma. 2016. [Consulta: 13 de septiembre 2020]. Disponible en: https://revistamarina.cl/revistas/2016/2/efrederickr.pdf

ROMERO C. Martha, et al. Introducción a la seguridad Informática y el análisis de vulnerabilidades. Ed. Área de Innovación y Desarrollo,S.L. 2018. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

RUGE Jeison. Metodología para identificación y valoración de riesgos. 2012. [Consulta: 4 de septiembre 2020]. Disponible en: http://polux.unipiloto.edu.co:8080/00000744.pdf

SÁNCHEZ J. Métodos y técnicas de detección temprana de casos de phishing. 2019. [Consulta: 24 de septiembre 2020]. Disponible en: https://openaccess.uoc.edu/webapps/o2/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf

SANCHEZ M. Hacking Etico: Impacto En La Sociedad. 2015. [Consulta: 13 de septiembre 2020]. Disponible en:

SÁNCHEZ R. Seguridad en Redes. s.f. [Consulta: 16 de septiembre 2020]. Disponible en: https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

SCOLNIK, Hugo D. Qué es la seguridad Informática. 2014. 1ra ed. Ciudad autónoma de Buenos aires. Argentina. Ed. Paidós

SERRATO D. Estudio de Metodologías de Ingeniería Social. 2018. [Consulta: 4 de septiembre 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

SOPHOS. [Sitio web]. Sophos The State of Ransomware Latinoamerica. [Consulta: 22 de noviembre 2020]. Disponible en: https://www.sophos.com/es-es.aspx

SPAFFORD Eugene. “Computer Recreations of Worms, Viruses and Code War”. Scientific American. marzo 1998, p. 110

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. De la protección de la información y de los datos. Bogotá. Colombia. 2009. [Consulta: 14 de septiembre 2020]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

TELERO, W. Seguridad en los autos con sistemas de apoyo a la conducción. s.f. [Consulta: 4 de septiembre 2020]. Disponible en: http://polux.unipiloto.edu.co:8080/00002675.pdf

TIPOS. [Sitio web]. Tipos de Software. 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.tipos.co/tipos-de-software/

UNIVERSIDAD DEL CAUCA. [Sitio web]. Aspectos Organizacionales de los Sistemas de Información. 2015. [Consulta: 3 de septiembre 2020]. Disponible en: http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm

UNIVERSIDAD INTERNACIONAL DE VALENCIA. [Sitio web]. Qué es la seguridad Informática. 20163. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

UNIVERSIDAD JAÉN. Guía de Seguridad UJA Software malicioso. 2018. [Consulta: 13 de septiembre 2020]. Disponible en: https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%203.%20Malware.pdf

UNIVERSIDAD LIBRE DE COLOMBIA. [Sitio web]. Crecen los ataques de Phishing en Colombia. 2019. [Consulta: 8 de diciembre 2020]. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia

UNIVERSIDAD NACIONAL DEL LITORAL. [Sitio web]. ¿QUÉ ES LA TECNOLOGÍA? 2018. [Consulta: 5 de septiembre 2020]. Disponible en: http://www.unl.edu.ar/ingreso/cursos/cac/21ot/#1484779044787-8891d599-6206

VERDEJO, G. Seguridad en redes. Cap. 2. Denegación de servicio: DOS / DDOS. s.f. [Consulta: 24 de septiembre 2020]. Disponible en: https://www.cs.upc.edu/~gabriel/files/DEA-es-2DOS-DDOS.pdf

VMWARE. [Sitio web]. ¿En qué consiste la virtualización? 2020. [Consulta: 4 de septiembre 2020]. Disponible en: https://www.vmware.com/co/solutions/virtualization.html

WELIVESECURITY. [Sitio web]. MAGERIT: metodología práctica para gestionar riesgos. 2013. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

WELIVESECURITY. [Sitio web]. Todo sobre cifrado: qué es y cuándo deberías usarlo. 2016. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2016/02/09/todo-sobre-cifrado-cuando-usarlo/

WRIGHTSON T. Advanced Persistent Threat Hacking. 2015. [Consulta: 13 de septiembre 2020]. Disponible en: http://index-of.es/Varios/Advanced%20Persistent%20Threat%20Hacking,%20The%20Art%20&%20Science...pdf

ZAGXA CONSULTING. [Sitio web]. Metodologías de TI. 2020. [Consulta: 3 de septiembre 2020]. Disponible en: https://www.zagxa.com/metodologias-de-ti/

ZAPATA F. Detección de ataques de spoofing. 2013. [Consulta: 14 de septiembre 2020]. Disponible en: http://bibing.us.es/proyectos/abreproy/12163/fichero/PFC.pdf