PRINCIPALES ATAQUES INFORMÁTICOS QUE AFECTAN A LOS SISTEMAS DE INFORMACIÓN DE LAS UNIVERSIDADES EN COLOMBIA

EDUARDO SOLORZANO RAMOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
AÑO 2024

PRINCIPALES ATAQUES INFORMÁTICOS QUE AFECTAN A LOS SISTEMAS DE INFORMACIÓN DE LAS UNIVERSIDADES EN COLOMBIA

EDUARDO SOLORZANO RAMOS

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

ASESOR
ING. CHRISTIAN REYNALDO ANGULO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
AÑO 2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con profundo sentimiento, dedico mi monografía a mis padres, cuya memoria reside ahora en el reino celestial, en la compañía divina de DIOS. Sin su presencia, este anhelado sueño nunca habría cobrado vida. Agradezco desde las entrañas de mi corazón los principios y valores que sembraron en mí durante mi infancia y adolescencia. Estos cimientos resultaron fundamentales para guiarme por los caminos del recto proceder y la justicia en esta existencia.

La influencia de mis padres fue mi brújula moral, marcando el rumbo de mis acciones y decisiones. Aunque las palabras resultan insuficientes para plasmar mi gratitud, llevaré conmigo sus recuerdos hermosos en cada paso de mi jornada. Estos recuerdos son mi tesoro más preciado, una luz que iluminará mi camino mientras pise esta tierra.

En mi corazón, este día se erige como el más gratificante, pues representa un paso gratificante en lo personal, profesional y laboral. Experimentar la esencia natural que la vida nos concede, la oportunidad de crecer y aportar a la sociedad, construyendo un mundo distinto con el esfuerzo constante, la dedicación incansable y el cuidado meticuloso, es una vivencia única.

En este proceso, discernir el conocimiento adquirido de manera honesta y humilde se convierte en el reflejo más genuino de la interacción entre seres humanos. Es un acto de autenticidad y respeto hacia los demás, una expresión de nuestro compromiso en compartir sabiduría y aprender unos de otros de manera sincera y sin pretensiones.

AGRADECIMIENTOS

Quiero expresar mis sinceros agradecimientos a mis padres, Eduardo Solórzano Villalobos (Q.E.P.D) y Virgelina Ramos Salazar (Q.E.P.D), por haberme brindado la valiosa oportunidad de existir. También, extiendo mi gratitud al todopoderoso por concederme la vida en este mundo. Tener la fortuna de disfrutar de la salud, la sabiduría y el amor, tres pilares fundamentales que contribuyen para llevar una vida plena y significativa.

A mis queridos hermanos y a mi amada, deseo expresar mi profundo agradecimiento por el apoyo inquebrantable que me han brindado tanto emocional como económicamente. Sus gestos y aprecio han sido mi gran fortaleza en momentos en que parecía que los desafíos dificultaban la realización de mis sueños. Sus voces de aliento resonaron fuerte cuando la adversidad intentó imponerse, y por ello les estaré eternamente agradecido.

Deseo extender mi más sincero agradecimiento a quienes hacen parte de la Universidad Nacional Abierta y a Distancia UNAD, así como a los tutores y asesores que han sido esenciales y fundamentales a lo largo de mi trayecto educativo. Sin embargo, quiero reservar un lugar especial de reconocimiento para los docentes, quienes han desempeñado un papel excepcional al convertirse en mi fuente de inspiración y en un auténtico modelo de vida.

A lo largo de esta travesía académica, estos dedicados educadores no solo han compartido su valioso conocimiento, sino que también me han guiado en la comprensión de cómo contribuir de manera responsable a la construcción de una sociedad más útil. Su influencia ha trascendido las aulas, moldeando no solo mis habilidades académicas, sino también mi sentido de compromiso social. Por esta razón, mi gratitud hacia ellos es inmensurable y perdurará a lo largo de mi vida.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

BACKUP: Copia de bases de datos en medio removible.

CONFIDENCIALIDAD: Probabilidad en que el sistema no falle en el futuro.

CORTAFUEGOS: Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situado en los puntos limítrofes de una red que tienen el objetivo o como complemento de actividades maliciosas como los ataques de phishing.

DISPONIBILIDAD: Probabilidad de que el sistema se encuentre funcionando en cualquier instante.

DATO: Representaciones simbólicas de topo numéricas, alfabéticas y algorítmicas de un determinado atributo o variable cualitativa o cuantitativa.

HACKER: Individuo con amplios conocimientos técnicos para detectar e identificar debilidades de seguridad (Vulnerabilidades) en los sistemas.

INTEGRIDAD: se refiere al mantenimiento de la precisión y consistencia de los datos, así como de los otros sistemas corporativos durante los procesos o el ciclo de vida del negocio.

VULNERABILIDAD: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta.

RESUMEN

Se llevará a cabo un exhaustivo análisis utilizando fuentes de información que abarquen casos relacionados con ataques informáticos dirigidos a los diversos sistemas de información presentes en las universidades de Colombia. Dicho análisis se realizará con un enfoque en el continuo desarrollo y evolución de las tecnologías informáticas, las cuales desempeñan un papel crucial en los ámbitos económico, político, social y personal.

En este contexto, resulta imperativo adoptar medidas cada vez más sólidas y efectivas para preservar no solo la disponibilidad, sino también la confidencialidad e integridad de la información en el entorno educativo. A medida que el tiempo avanza, se hace evidente la creciente demanda de salvaguardias robustas debido a la presencia constante y penetrante de las nuevas tecnologías.

Este análisis no solo considerará los aspectos técnicos de los ataques, sino que también explorará las implicaciones más amplias en términos de impacto institucional y comunitario. Al recalcar la importancia de salvaguardar la información en un entorno donde la dependencia de la tecnología es cada vez mayor, se busca generar conciencia sobre la necesidad de establecer estrategias integrales de protección cibernética.

En resumen, a través de un análisis fundamentado en casos reales, este estudio se propone ilustrar la compleja relación entre los ataques informáticos y la evolución tecnológica en el contexto de las universidades colombianas. Al hacerlo, se pretende a fomentar una postura proactiva hacia la ciberseguridad y a impulsar la implementación de medidas sólidas que resguarden la información para el funcionamiento de las instituciones educativas en el entorno digital actual.

SUMMARY

An exhaustive analysis will be carried out using information sources that cover cases related to computer attacks directed at the various information systems present in Colombian universities. Said analysis will be carried out with a focus on the continuous development and evolution of information technologies, which play a crucial role in the economic, political, social, and personal spheres.

In this context, it is imperative to adopt increasingly solid and effective measures to preserve not only the availability, but also the confidentiality and integrity of information in the educational environment. As time progresses, the growing demand for robust safeguards becomes evident due to the constant and pervasive presence of new technologies.

This analysis will not only consider the technical aspects of the attacks but will also explore the broader implications in terms of institutional and community impact. By stressing the importance of safeguarding information in an environment where dependence on technology is increasing, it seeks to raise awareness of the need to establish comprehensive cyber protection strategies.

In summary, through an analysis based on real cases, this study aims to illuminate the complex relationship between computer attacks and technological evolution in the context of Colombian universities. In doing so, it is hoped to promote a proactive stance towards cybersecurity and to promote the implementation of solid measures that safeguard vital information for the operation of educational institutions in today's digital environment.

INTRODUCCIÓN

Con el objetivo primordial de salvaguardar las organizaciones, en particular los sistemas de información de las universidades en Colombia, frente a las amenazas de ciberseguridad, se vuelve imperativo considerar la creciente magnitud y frecuencia de los ataques informáticos que han caracterizado los últimos años. Ante este panorama, se plantea la necesidad imperante de llevar a cabo un análisis de diversas fuentes de información que documenten los patrones de ataques más recurrentes dirigidos a los sistemas de información en las universidades colombianas.

Este análisis se perfila como un paso crucial para la adopción de medidas preventivas estratégicas, cuyo propósito es contrarrestar eficazmente las tácticas y utilizadas por los actores malintencionados en el ciberespacio. Al desglosar y comprender los tipos de ataques que han prevalecido en este contexto específico, se abre la puerta a la implementación de enfoques proactivos y personalizados que aborden las vulnerabilidades únicas que enfrentan las instituciones educativas.

Al identificar los patrones recurrentes y las tácticas preferidas por los atacantes, será posible afinar las estrategias de defensa y adaptar las políticas de ciberseguridad en función de las amenazas reales y emergentes. Este análisis informará la toma de decisiones fundamentadas, permitiendo a las universidades en Colombia fortalecer sus capacidades de detección, respuesta y recuperación en caso de incidentes de seguridad.

El primer ataque informático en la historia se da en la Universidad California, Berkeley, el mismo se efecto en el año de 1988 donde a través de un malware, diseñado para realizar ciberataques, se logró perpetuar el ataque informático a más de 6.000 computadoras, alrededor de 60.000 que se encontraban en el Instituto de

Tecnología de Massachusetts (MIT).Este virus fue denominado como “Gusano Morris, el entonces famoso virus no genero daños en ninguno de los archivos de los computadores, pero si conllevo al retraso de las operaciones dentro del centro académico durante varios días. Berkeley no fue la única víctima de este ataque, también fueron afectadas Harvard, Princeton, Stanford, Johns Hopkins, la NASA y el Laboratorio Nacional Lawrence Livermore.[1]

En el trasegar de la historia y la evolución tecnológica, hemos sido testigos de la emergencia constante de nuevos virus y amenazas que han planteado serios riesgos para la seguridad de la información en las organizaciones. Esta realidad ha impulsado un proceso de constante reinvención en las infraestructuras tecnológicas, motivando la adopción de arquitecturas innovadoras en el mercado tecnológico y el potenciamiento tanto del software como del hardware.

Es de anotar que para el año 2021 en Colombia se registraron más de 23.000 noticias criminales, es decir, el 30% más que en el mismo periodo del 2020, convirtiéndose los ataques informáticos en una de las nuevas modalidades de delitos en crecimiento en el país, en Colombia las cuidades más afectadas en las que se encuentran Bogotá con 8.355 casos, seguida Medellín 1.664 y Cali con 1569[2] ataques.

Para el año de 2022, se reportaron en Colombia más de 54.121 denuncias por ataques informáticos, además alrededor de 10 empresas informaron que fueron víctimas objeto de hackeos[3]. El caso más reciente se presentó con la compañía

[1] Sitio web 20 Bit. "Estamos bajo ataque": se cumplen 34 años del 'gusano Morris', el primer malware de la historia [En línea] (02 de noviembre del 2021) https://www.20minutos.es/tecnologia/ciberseguridad/estamos-bajo-ataque-se-cumplen-34-anos-del-gusano-morris-el-primer-malware-de-la-historia-5073273/

[2] Revista Semana. El año de los ciberataques en Colombia, estas son las alarmantes cifras [En línea] (02 de julio del 2021) [consultado: el 02 de julio del 2021] Disponible en: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

[3] La república. Las empresas que han sido blanco de ciberataques en Colombia en el último año [En línea] (25 de enero del 2023) [consultado: 25 de enero del 2023] Disponible en: https://www.larepublica.co/empresas/las-empresas-que-han-sido-

farmacéutica Audifarma, la cual fue atacada en su infraestructura tecnológica, esto conllevo a que tomaran acciones tempranas y tuvieron que deshabilitar los servidores con la finalidad de proteger la información de los servidores y de todos sus usuarios.

Por otra parte, el caso más reciente se presentó el 18 de marzo del 2023 en donde, los servidores de la Universidad Nacional de Colombia fueron víctimas de ataques informáticos, allí se detectó la indisponibilidad de los servicios ya que algunos de los servidores se encontraban inaccesibles producto del ataque informático[4].

Es así, como actualmente existen múltiples formas de ataques de ciberseguridad y que a través de estos pueden explotar las vulnerabilidades de los sistemas de información. Principalmente estos ataques se han convertido en una combinación de ataques tecnológicos combinados con ingeniería social ya que esta última es una de las formas más recurrentes por los ciberdelincuentes para perpetuar los ataques.

blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667#:~:text=Entre%20enero%20y%20octubre%20de,que%20fueron%20objeto%20de%20hackeos.

[4] Revista Semana. Los detalles secretos del grave hackeo que sufrió la Universidad Nacional [En línea] (02 de abril del 2023) [consultado: 02 de abril del 2023] Disponible en: https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335/

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

A lo largo de la historia los servicios impulsados por las tecnologías han experimentado una evolución constante comienza a partir del siglo XX que la sociedad ha sido testigo de una transformación digital sin precedentes en la historia de la humanidad. Estos cambios han redefinido la forma en que interactuamos y se han manifestado de manera radical en la manera en que nos comunicamos, alterando profundamente las relaciones entre individuos.

Los avances tecnológicos han traído consigo una serie de transformaciones profundas, que han sido reconocidas como la cuarta revolución industrial. En este contexto, resulta esencial comprender y analizar los tipos de ataques que con mayor frecuencia afectan a los sistemas de información. Esta comprensión se convierte en un pilar fundamental para abordar las brechas en seguridad informática y para desarrollar estrategias que permitan contrarrestar eficazmente estas amenazas.

La continua proliferación de ataques perpetrados por ciberdelincuentes, que aprovechan diversas herramientas tecnológicas para acceder ilegalmente a los sistemas de información, exige una respuesta informada y proactiva. A medida que transcurren los años, la magnitud y sofisticación de los ataques han aumentado considerablemente, lo que hace que la seguridad cibernética sea más crucial que nunca.

En este contexto de constante cambio y riesgo digital, el análisis de las tácticas de ataque más frecuentes se convierte en un instrumento invaluable para la planificación de medidas preventivas y de respuesta. Al identificar las vulnerabilidades y patrones utilizados por los ciberdelincuentes, se posibilita la implementación de contramedidas efectivas y la promoción de una cultura de ciberseguridad más sólida en todas las capas de la sociedad.

La transformación tecnológica y la aparición de amenazas cibernéticas han reconfigurado nuestra forma de vida y la interacción social. La cuarta revolución industrial nos insta a mantenernos vigilantes, a comprender los riesgos y a actuar con determinación para salvaguardar nuestros sistemas de información ante las crecientes amenazas en este nuevo paisaje digital.

> ***ANCHUNDIA BETANCOURT,*** *Carlos E[5]. Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes El aumento de la conectividad a Internet provoca que cada vez más personas estén conectadas en un espacio público y transaccional, proporcionando una plataforma dinámica y de crecimiento que permite que avance la comunicación, la colaboración y la innovación; sin embargo, los ataques cibernéticos y el robo de información crítica se han convertido en una gran amenaza derivado de las consecuencias económicas y sociales que conllevan.*

A partir de lo expuesto, se hace evidente que la innovación tecnológica ha revolucionado la interacción social y ha fomentado una comunicación más directa entre organizaciones e individuos. No obstante, esta progresión tecnológica también ha dado lugar a una serie de ciberataques que han impactado las estructuras tecnológicas. Estos ataques no solo amenazan la integridad del sector educativo y gubernamental, sino que también comprometen la forma en que accedemos a la información.

En este contexto, nos encontramos con una diversidad de ataques informáticos que plantean riesgos para la confidencialidad, integridad y disponibilidad de la

[5] ANCHUNDIA BETANCOURT, Carlos E . Ciberseguridad en los sistemas de información de las universidades [Dialnet] 2017, Revista científica Dominio de la Ciencias file:///C:/Users/ESOLORZANOR/Downloads/Dialnet-CiberseguridadEnLosSistemasDeInformacionDeLasUnive-6102849%20(1).pdf

información. Las universidades en Colombia se enfrentan a la responsabilidad de investigar y adoptar medidas que permitan prevenir y mitigar estos ataques perpetrados por ciberdelincuentes. Estos ataques pueden poner en peligro el activo más valioso de las organizaciones e instituciones: la información.

En este sentido, es crucial establecer, mantener y mejorar constantemente la seguridad de la información. Dado el entorno de seguridad en constante cambio, resulta impracticable compilar una lista exhaustiva de todos los posibles ataques. No obstante, mediante estudios llevados a cabo por expertos en seguridad informática, ha sido factible identificar los ataques más comunes y representativos, contar con un nivel de seguridad que disuada la ejecución de estos ataques se convierte en una prioridad.

La revolución tecnológica ha propiciado una transformación en la forma en que nos relacionamos y compartimos información, pero al mismo tiempo ha desencadenado desafíos de seguridad. En este entorno dinámico, las universidades deben comprometerse a proteger la información y a estar al tanto de los ataques más pertinentes para implementar contramedidas efectivas. Solo así podrán asegurar la integridad y disponibilidad de la información vital en un mundo interconectado y en constante cambio.

En un entorno donde la evolución tecnológica en el ámbito educativo avanza a un ritmo vertiginoso, es imperativo adoptar una perspectiva de futuro. Más allá de los avances actuales, es crucial enfocarnos en el panorama del "Internet de las Cosas", que abarca no solo el ámbito educativo, como se mencionó previamente, sino también los aspectos económicos y sociales. Ante esta realidad en constante cambio, es esencial contemplar una visión proyectada y futurista.

La incursión en el "Internet de las Cosas" trae consigo un nivel sin precedentes de interconexión y automatización en todos los ámbitos de la sociedad. En este

contexto, la seguridad debe ser una prioridad primordial. Las implicaciones de la interconexión de dispositivos y sistemas son vastas, lo que potencialmente puede dar lugar a una mayor exposición a ciberataques y amenazas. Por lo tanto, es fundamental implementar medidas de seguridad asertivas que aborden los desafíos que surgirán en este futuro interconectado.

No solo se trata de asegurar la integridad y disponibilidad de la información en el ámbito educativo, sino también de salvaguardar los aspectos económicos y sociales que están intrínsecamente vinculados a esta transformación digital. La confianza en la tecnología y la ciberseguridad será un elemento central en la adopción exitosa de estas innovaciones.

A medida que nos adentramos en un mundo de interconexión y avances tecnológicos sin precedentes, es esencial adoptar una visión futurista y proactiva. La implementación de medidas de seguridad sólidas se convierte en un pilar fundamental para garantizar que el potencial beneficio del "Internet de las Cosas" se materialice sin comprometer la seguridad y la confidencialidad de la información. De esta manera, podremos abrazar las oportunidades que el futuro tecnológico tiene para ofrecer de manera segura y sostenible.

> ***TAPIA RANGEL**, **Edith; LEÓN MARTÍNEZ**, **Jorge**[6] "La inclusión de las TIC en la educación debe ir acompañada de una serie de lineamientos que definan un marco de referencia para la toma de decisiones respecto de las acciones que se deben realizar durante el proceso. Identificando así 3 dimensiones: (1) Información, vinculada al acceso, modelo y transformación del nuevo conocimiento e información de los entornos digitales; (2) Comunicación, vinculado a la colaboración, trabajo en*

[6] TAPIA RANGEL, Edith; LEÓN MARTÍNEZ, Jorge. Impacto de las TIC en la educación: Retos y Perspectivas [Dialnet] 2017 Universidad San Ignacio de Loyola, Vicerrectorado de Investigación y Desarrollo Dialnet-ImpactoDeLasTICEnLaEducacion-5904762.pdf

equipo, y adaptabilidad tecnológica; (3) Ética e Impacto Social, vinculado a las competencias necesarias para afrontar los desafíos éticos producto de la globalización, y auge de las TIC. “

Al observar el artículo mencionado anteriormente como punto de referencia, resulta evidente que se abordan diversas dimensiones esenciales que deben ser consideradas en los procesos que facilitan la identificación y transformación del paradigma de conocimiento e información hacia entornos digitales, esta transformación se vuelve fundamental para abordar con éxito una serie de procesos y desafíos tecnológicos.

El artículo proporciona una visión holística de los elementos interrelacionados que conforman la transición hacia la era digital. En este contexto, se destacan aspectos que abarcan desde la identificación de nuevos enfoques hasta la implementación de soluciones tecnológicas que permitan abordar los desafíos emergentes. Esta comprensión integral es esencial para enfrentar la complejidad inherente a la transformación digital.

En última instancia, el artículo ofrece una guía valiosa para establecer una base sólida en la que convergen el conocimiento, la información y la tecnología, al considerar estas dimensiones en conjunto, se crea un marco que puede abordar de manera efectiva los cambios en el entorno digital y superar los retos tecnológicos actuales y futuros.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son los factores de vulnerabilidad que inciden frente a los ataques informáticos en los sistemas de información de las universidades Colombia?

2 JUSTIFICACIÓN

A lo largo del presente trabajo de investigación, resulta esencial dirigir nuestra atención hacia las diversas medidas de seguridad que se han planteado en relación a los ataques informáticos dirigidos a los sistemas de información de las universidades en Colombia. Es fundamental comprender cómo estas medidas juegan un papel determinante en la preservación de la integridad y continuidad de estas instituciones educativas frente a posibles amenazas cibernéticas.

La investigación se enfoca en analizar cómo los ataques informáticos pueden tener un impacto disruptivo en el funcionamiento eficiente de las universidades. Estos ataques pueden generar interrupciones, afectar la disponibilidad de servicios esenciales y comprometer la confidencialidad de la información crítica. Por lo tanto, es crucial examinar detalladamente las medidas de seguridad existentes y cómo estas actúan como defensas vitales ante el panorama en constante evolución de las amenazas cibernéticas.

A través de este enfoque, se aspira a proporcionar una visión completa y perspicaz de cómo las universidades en Colombia están abordando la creciente amenaza de los ataques informáticos. Al identificar las medidas de seguridad más efectivas y sus aplicaciones prácticas, se contribuye a fortalecer la resiliencia de estas instituciones frente a los desafíos de seguridad cibernética. De esta manera, se fomenta un entorno educativo seguro y sin interrupciones que promueva el desarrollo continuo de la enseñanza y la investigación.

Es importante destacar que la era digital ha provocado una revolución en todos los ámbitos de nuestra vida cotidiana, introduciendo cambios significativos que se extienden por toda la sociedad. En este contexto, el sector educativo no queda excluido de esta transformación, siendo igualmente esencial en el conjunto de aspectos afectados por esta revolución tecnológica.

De manera innegable, la integración de las nuevas tecnologías en el ámbito educativo ha transformado los métodos de enseñanza tradicionales, introduciendo pilares innovadores en la educación. Entre estos pilares se destacan la programación, la robótica y la impresión 3D, que han emergido como componentes esenciales en la formación educativa moderna.

Hace algunos años, los estudiantes solo tenían la opción de acceder a la educación de manera presencial, ya que no existía ningún otro método que permitiera su acceso, pero la tecnología ha traído consigo una serie de herramientas que han revolucionado la forma en que se accede a la educación.

Es importante señalar que la integración de la tecnología en la educación presenta una serie de desafíos que deben abordarse de manera efectiva. Estos desafíos incluyen el fomento del trabajo colaborativo, la adaptabilidad a las tecnologías en constante evolución, la creación de sistemas evaluativos que se adecuen a las nuevas herramientas tecnológicas y la preparación de docentes dispuestos a guiar el uso significativo de los contenidos digitales. A través de estos esfuerzos, se está logrando un cambio de paradigma en la educación: los estudiantes ya no se están preparando exclusivamente para un mundo industrial, sino para un mundo impulsado por la tecnología y la información.

De igual manera, resulta evidente que el ámbito educativo está inmerso en un proceso de transición en consonancia con la evolución constante de la sociedad. En este contexto, la era tecnológica avanza a pasos agigantados, y es esencial que la educación también siga este camino de progreso. La integración de la tecnología en la educación no puede quedarse rezagada, sino que, por el contrario, debe contribuir de manera constante mediante aportes significativos.

La tecnología ha adquirido un rol fundamental en la educación, y su influencia es cada vez más evidente en todos los niveles de la sociedad. En este sentido, es

esencial que la educación no solo se adapte, sino que también adopte la tecnología de manera efectiva para garantizar la inclusión y el acceso a una educación de calidad. A medida que avanzamos en un mundo aparentemente tecnológico, es importante recordar que este entorno está en constante evolución y que eventos como la llegada del coronavirus nos demuestran cuán rápidamente pueden cambiar las circunstancias.

La educación está experimentando una transformación necesaria para mantenerse alineada con la era tecnológica en constante avance. La integración y adopción efectiva de la tecnología son esenciales para asegurar la calidad y la relevancia de la educación en un mundo que evoluciona rápidamente.

Aunque la pandemia afectó a todos los sectores, es innegable que el sector educativo fue uno de los más impactados. Aunque se intentó paliar esta situación mediante el uso de tecnologías, esto demostró ser insuficiente. De hecho, se evidenció claramente que persisten importantes carencias en infraestructura, tanto física como tecnológica, en diversos sectores, incluido el ámbito educativo. Estas deficiencias se manifestaron de manera particular en áreas rurales, donde el acceso a la educación se vio fuertemente comprometido y, en consecuencia, no se logró concluir las clases como estaba previsto.

En el panorama actual, debemos anticipar cambios aún más trascendentales que la era tecnológica puede ofrecer. No obstante, es crucial reconocer que esta transformación solo se logrará a través de la sensibilización y la gestión del cambio. Innovar con nuevas herramientas y métodos de enseñanza es fundamental para impulsar un cambio efectivo hacia el futuro. La educación del mañana requerirá un enfoque adaptable y orientado a la tecnología, permitiendo que los estudiantes adquieran las habilidades necesarias para enfrentar los desafíos de un mundo en constante evolución.

En este contexto, el objetivo central del presente trabajo de investigación radica en analizar y evaluar la evolución de los ataques informáticos y su relevancia en la dinámica actual. Paralelamente, se aborda la importancia otorgada por los gobiernos en el proceso de implementación y avance de la educación a través de las tecnologías, adicionalmente se busca generar propuestas que contribuyan al desarrollo de diversos proyectos de administración tecnológica, con el fin de satisfacer las necesidades de la sociedad en su conjunto.

Este análisis profundo permitirá identificar cómo los ataques informáticos han evolucionado y adquirido una dimensión cada vez más crítica en la era digital. A su vez, se explorará cómo los gobiernos reconocen la importancia de impulsar la educación mediante la tecnología, como respuesta a las demandas cambiantes del entorno global y las oportunidades que la tecnología ofrece.

Es así, como se pretende abordar un enfoque propositivo, generando ideas y soluciones concretas que puedan contribuir al desarrollo y administración efectiva de tecnologías en el ámbito educativo y más allá. Estas propuestas buscan satisfacer las necesidades actuales y futuras de la sociedad en su conjunto, asegurando un impacto positivo en la calidad de la educación y en la vida cotidiana de las personas.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los principales ataques informáticos a los que se han visto expuestos los sistemas de información de las universidades en Colombia, a través de una revisión sistemática en fuentes oficiales, con el fin de generar estrategias de mitigación de riesgo que permitan brindar una protección adecuada a la información.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar fuentes de información relacionada frente a ataques informáticos y estrategias de protección adecuada para salvaguardar las infraestructuras tecnológicas.

- Explicar los diferentes ataques informáticos encontrados productos de la investigación y los cuales se presentan a los sistemas de información de las universidades en Colombia.

- Identificar estrategias de mitigación del riesgo que permita brindar protección adecuada a los sistemas de información frente a los ataques informáticos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En la actualidad, los ataques informáticos son un concepto ampliamente reconocido por la sociedad en general. A lo largo de los años, esta noción ha evolucionado, siendo los virus informáticos una de sus fuentes principales. Dentro del contexto histórico y en relación con el origen de los virus informáticos, como se señala Discovery[7], el programa Creeper, considera que el primer virus fue creado en 1971 Por Bob Thomas de BBN En realidad, Creeper fue diseñado como una prueba de seguridad para comprobar si era posible crear un programa capaz de replicarse. De cierta manera, lo fue. Con cada disco duro nuevo infectado, Creeper trataba de eliminarse a sí mismo del equipo anfitrión anterior. Creeper no tenía una intención maliciosa y solo mostraba un mensaje simple: "I'M THE CREEPER. ¡CATCH ME IF YOU CAN!" (Soy Creeper, ¡atrápame si puedes!).

En la contemporaneidad, se identifican cuatro tipos de ataques que presentan una recurrencia significativa en el ámbito informático. Estos ataques son utilizados con la finalidad ilícita de secuestrar información de manera ilegal. Entre estos, podemos destacar los más comunes.

4.1.1 Phishing: Este tipo de ataques resalta la importancia de mantener una actitud vigilante al interactuar con correos electrónicos y mensajes de texto, verificando siempre la autenticidad de los remitentes y evitando hacer clic en enlaces sospechosos. La educación y la concientización de los usuarios son componentes clave en la lucha contra este tipo de amenaza cibernética.

[7] Fuente: Kaspersky (En línea) Latam Kaspersky (Consultado el 16 de mayo del 2022) Disponible en: https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

Además, existen diversas medidas preventivas para contrarrestar este tipo de ataques. Una de ellas es la verificación rigurosa de la fuente de información, asegurándose de que provenga de una fuente confiable antes de tomar cualquier acción. Asimismo, es fundamental abstenerse de acceder a cuentas bancarias u ofrecer información sensible a través de enlaces o hipervínculos presentes en correos electrónicos desconocidos.

Otra medida efectiva es el acceso seguro a correos electrónicos y cuentas bancarias a través de dispositivos que cuenten con medidas de seguridad adicionales, como antivirus y firewalls. Estas herramientas contribuyen a la protección contra posibles amenazas y a salvaguardar la información personal y financiera.

La prevención del Phishing implica una combinación de precaución, verificación y uso responsable de dispositivos. Al adoptar estas medidas, los usuarios pueden reducir significativamente su exposición a este tipo de ataques y preservar su seguridad digital.

El 18 de marzo de 2023, la Universidad Nacional de Colombia, Sede Bogotá, se enfrentó a un ataque cibernético que afectó su infraestructura tecnológica. Tras la intrusión, se llevaron a cabo acciones inmediatas para mitigar el riesgo y evitar la propagación del ataque. Para lograr este objetivo, se intensificaron las medidas de seguridad y se restringieron los permisos en los equipos perimetrales de las distintas sedes de la universidad.

La naturaleza del ataque lleva a especular que se pudo haber ejecutado a través de un correo electrónico malicioso, empleando la modalidad de Phishing. Esta táctica, ampliamente utilizada en la actualidad, involucra el engaño a los usuarios para que abran enlaces o archivos adjuntos peligrosos. En este caso, el ataque podría haberse originado a partir de un correo electrónico bajo esta modalidad, lo que permitió que se abriera y propagara a través de la red universitaria.

La rápida respuesta de la universidad y la implementación de medidas de seguridad adicionales demuestran la importancia de estar preparados para enfrentar amenazas cibernéticas. Estos eventos resaltan la necesidad constante de estar vigilantes, fortalecer las defensas de seguridad y educar a los usuarios sobre las mejores prácticas de seguridad cibernética.

4.1.2 Ransomware: El término "Ransomware" se origina a partir de la palabra "Ransom", que en inglés significa "rescate". Este tipo de software malicioso está diseñado con el propósito de secuestrar información y bloquear su acceso, hasta que se realice un pago de rescate. El ataque perpetrado mediante Ransomware implica la encriptación del sistema operativo completo o, en ocasiones, de rutas de archivos específicas.

La táctica detrás del Ransomware es extremadamente perjudicial. Una vez que los archivos o el sistema están cifrados, el usuario es forzado a tomar una decisión difícil: pagar el rescate exigido por los atacantes para recuperar el acceso a la información, o afrontar la pérdida de datos valiosos. Esta forma de ataque explota la urgencia y la necesidad de los usuarios de recuperar su información, lo que puede llevar a decisiones apresuradas y a menudo costosas.

El Ransomware ha demostrado ser un desafío importante en el campo de la ciberseguridad, ya que puede causar daños sustanciales a individuos, empresas e instituciones. La prevención y la preparación son cruciales en la lucha contra este tipo de ataque, involucrando medidas de seguridad sólidas, copias de seguridad regulares y la concientización de los usuarios para evitar caer en trampas cibernéticas que pueden resultar en un bloqueo de datos y la exigencia de rescates.

Para prevenir la propagación de este tipo de virus, se implementan análisis exhaustivos de vulnerabilidades para identificar posible software maliciosos que

puedan causar daños a los sistemas. Además, es esencial asegurarse de que las aplicaciones cuenten con las actualizaciones apropiadas, incluyendo parches de seguridad. Entre las medidas recomendadas para evitar la infección de este tipo de virus, se encuentra la precaución de no abrir enlaces sospechosos.

La realización de análisis de vulnerabilidades permite detectar y abordar posibles debilidades en los sistemas que podrían ser aprovechadas por los atacantes. La implementación de actualizaciones regulares y parches de seguridad es crucial para cerrar posibles brechas y mitigar la exposición a amenazas como el Ransomware.

Además, es fundamental que los usuarios se mantengan alerta y eviten abrir enlaces o archivos adjuntos provenientes de fuentes desconocidas o sospechosas. La conciencia y la educación en ciberseguridad son componentes esenciales en la prevención de este tipo de amenazas y en la preservación de la integridad de los sistemas y datos.

Es importante destacar que del Ransomware se derivan tres tipos principales, entre ellos el Scareware. Este tipo de Ransomware no busca ser tan intimidante en su ataque, y suele incluir publicidad engañosa, ofrecer supuesto soporte técnico gratuito e incluso enviar mensajes de alerta falsos indicando que el dispositivo ha sido infectado con malware. Estos mensajes buscan crear la sensación de urgencia y provocar que el usuario realice un pago para eliminar la supuesta amenaza.

Otro tipo de Ransomware son los bloqueadores de pantalla. Mediante este enfoque, se impide el uso de la pantalla del dispositivo y se muestra un distintivo, a menudo alegando ser del FBI u otra entidad oficial. Esta táctica tiene la intención de intimidar al usuario, sugiriendo que han incurrido en actividades ilegales y que deben pagar una multa para desbloquear su dispositivo.

Finalmente, encontramos el Ransomware de cifrado. En este tipo de ataque, los ciberdelincuentes toman control de los archivos y los encriptan, dejando al usuario sin acceso a su propia información. Para desbloquear los archivos, se exige un pago de rescate. Este enfoque es particularmente peligroso, ya que afecta directamente los datos personales y empresariales, y puede causar daños significativos si no se aborda adecuadamente, la comprensión de estos tipos de Ransomware es esencial para tomar medidas preventivas adecuadas y comprender cómo protegerse frente a estas amenazas cibernéticas cada vez más sofisticadas.

En el contexto del año 2021, marcado por la aparición de la pandemia de COVID-19, la Universidad del Bosque demostró tener un sistema de seguridad informática de última generación, meticulosamente concebido para resguardar la integridad de la valiosa información alojada en su entorno digital. Sin embargo, incluso ante estas salvaguardias, la institución se encontró inesperadamente en el epicentro de un acto delictivo perpetrado por individuos no identificados.

Dentro de este lamentable suceso, resultaron particularmente afectadas las plataformas digitales de mayor relevancia: la cuenta oficial de Twitter y las cuentas de correo institucionales. Estos pilares fundamentales de la comunicación y el intercambio académico fueron objeto de intrusión, desencadenando una serie de consecuencias que captaron la atención de la comunidad universitaria y más allá.

La magnitud de este incidente resalta la sofisticación y audacia de los perpetradores, quienes lograron burlar las avanzadas medidas de seguridad implementadas por la universidad. A pesar de contar con un sistema de protección robusto, la vulnerabilidad inherente a la interconexión digital se hizo evidente en este escenario, sirviendo como recordatorio de la constante necesidad de evolucionar y fortalecer las defensas cibernéticas.

En la búsqueda de respuestas y soluciones, la Universidad del Bosque emprendió una exhaustiva investigación en colaboración con expertos en seguridad informática y las autoridades pertinentes. Este incidente no solo puso de relieve la importancia de salvaguardar los activos digitales, sino también la necesidad de mantenerse alerta frente a las amenazas en constante evolución que el entorno digital puede presentar.

A medida que la institución trabaja incansablemente para restablecer la normalidad y reforzar sus medidas de seguridad, este episodio sirve como lección para todas las entidades educativas y organizaciones en el ámbito digital. La Universidad del Bosque reafirma su compromiso con la seguridad y la excelencia académica, perseverando en la adaptación y mejora continua de sus prácticas digitales en pos de un futuro más seguro y resiliente.

En respuesta a este desafío, la universidad desplegó un equipo de especialistas en seguridad cibernética con el objetivo de implementar un plan de acción integral. Este plan se orientó hacia la resolución de la situación en el menor tiempo posible, asegurando que el funcionamiento normal de los sistemas se restaurara de manera efectiva. La acción coordinada del personal especializado permitió superar este incidente, restaurar la seguridad de las cuentas afectadas y garantizar la continuidad operativa de los sistemas digitales.

Este incidente resalta la importancia de la preparación y respuesta eficiente ante amenazas cibernéticas, incluso para organizaciones con sólidos sistemas de seguridad. Además, demuestra que la ciberseguridad es un desafío en constante evolución que requiere vigilancia continua y adaptación a las tácticas cambiantes de los ciberdelincuentes. En este caso, la respuesta rápida y eficaz permitió minimizar los impactos y salvaguardar la integridad de los sistemas digitales de la universidad.

De manera paralela, en el mismo año, la Universidad Javeriana sufrió un incidente de seguridad que resultó en la interrupción de algunas de sus aplicaciones clave. Los efectos se concentraron en mayor medida en las sedes de Cali y Bogotá. Gracias a las medidas preventivas implementadas con prontitud, no se registró ningún indicio de fuga o pérdida de información. Además, se logró asegurar de manera inmediata los sistemas Core, evitando daños mayores.

En respuesta a esta situación, un equipo altamente especializado en ciberseguridad tomó la iniciativa. Su esfuerzo se centró en restablecer los sistemas de información de manera progresiva y cuidadosa, asegurando que el funcionamiento volviera a la normalidad con la máxima garantía de seguridad. A través de un enfoque gradual, se logró restablecer la operatividad de los sistemas, lo que permitió a la universidad retomar sus funciones con la menor interrupción posible.

Este episodio enfatiza la importancia de la acción inmediata ante incidentes cibernéticos y cómo la preparación y respuesta eficiente pueden minimizar el impacto de las amenazas. La rápida movilización de un equipo especializado permitió a la Universidad Javeriana preservar la integridad de sus sistemas y proteger sus activos digitales. Estos incidentes sirven como recordatorio de la constante necesidad de fortalecer las medidas de seguridad en el entorno digital en evolución.

4.1.3 Adware: Este tipo de software está diseñado con el propósito de mostrar anuncios en la pantalla de su dispositivo, principalmente a través del navegador, especialmente en navegadores como Google Chrome. Esta clase de software despliega anuncios de manera automática, a menudo en forma de ventanas emergentes, que promocionan programas dudosos o contenido potencialmente malicioso. El objetivo principal de estos anuncios es inducir al usuario a hacer clic en ellos, lo que puede llevar a redirecciones a sitios web no seguros o a la instalación involuntaria de programas no deseados.

Para evitar las posibles vulnerabilidades generadas por este tipo de publicidad intrusiva, se recomienda encarecidamente la instalación de extensiones en su navegador. Una de las extensiones más conocidas y efectivas para este propósito es Adblock. Esta extensión trabaja de manera activa para bloquear el flujo de información publicitaria no deseada, lo que resulta en una inmediata obstrucción de los anuncios molestos.

La instalación de Adblock, u otras extensiones similares, no solo ayuda a mejorar la experiencia de navegación, sino que también reduce significativamente los riesgos asociados con los anuncios maliciosos. Al bloquear la exhibición de anuncios sospechosos o potencialmente dañinos, se disminuye la probabilidad de redirecciones no deseadas o de la ejecución inadvertida de programas perjudiciales. En última instancia, estas extensiones contribuyen a salvaguardar la seguridad y privacidad del usuario mientras navega en línea.

4.1.4 Whaling: Es crucial reconocer que estos ataques explotan la psicología humana, aprovechando la confianza y la curiosidad natural de las personas. Al presentar información personalizada y redactar los correos en un lenguaje simple directo, los perpetradores buscan disminuir las sospechas y fomentar la interacción con el mensaje malicioso.

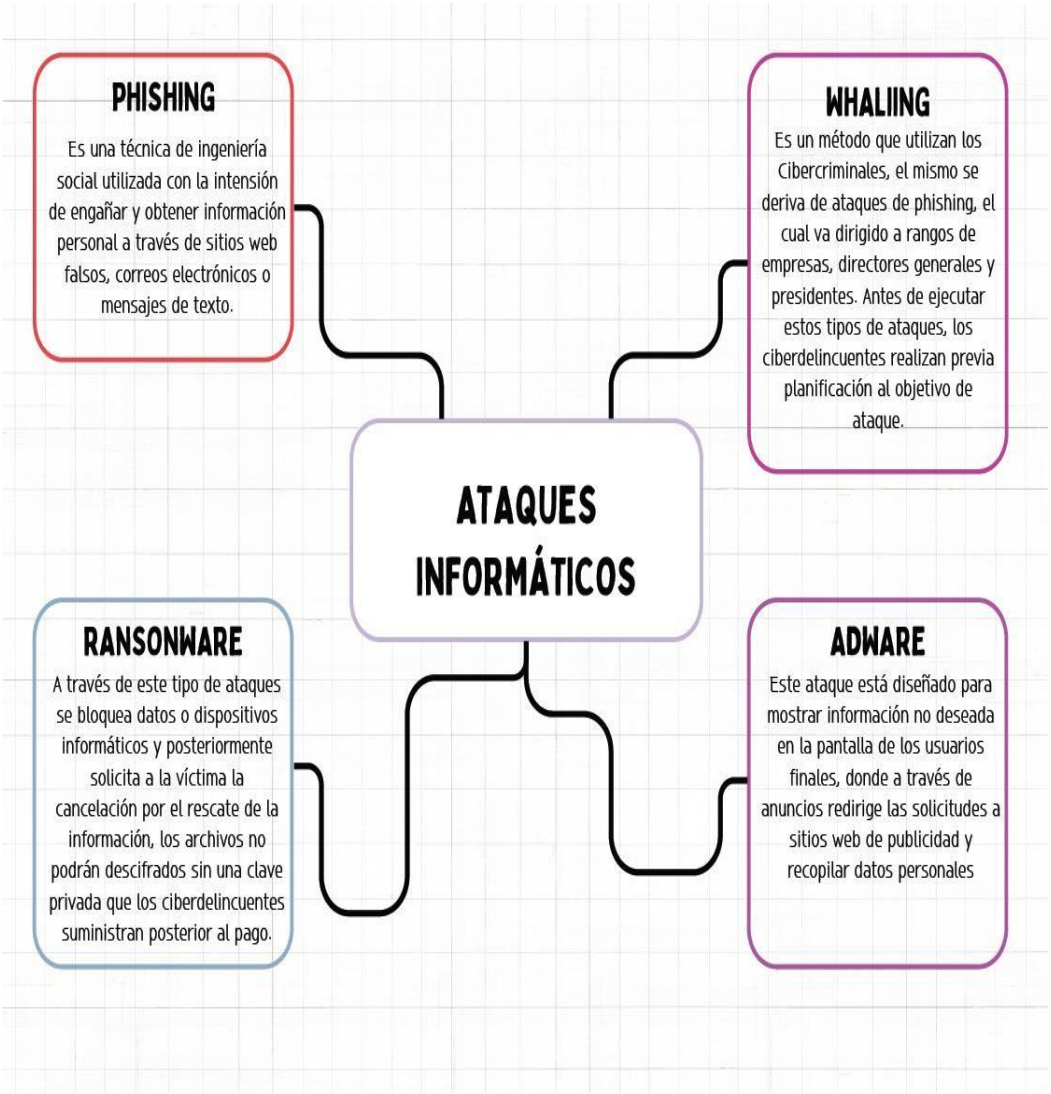
Ante esta creciente amenaza, es esencial que las organizaciones y los individuos estén al tanto de los métodos empleados en los ataques de "Whaling". La educación sobre seguridad cibernética y la implementación de medidas preventivas sólidas son fundamentales para contrarrestar esta forma avanzada de ciberdelito y proteger la integridad de la información y los activos digitales.

> *MEDINA ROJAS, Jonatán Deyvi; RIVAS MONTALVO, Yonathan Yajanovic[8]. Un ataque informático consiste en que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, ya sea el caso de un host, una red privada o un servidor, lo cual tendrá como consecuencia perdida de información y/o pérdidas económicas en alguna organización. Por ello la seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar enfocada a proteger la propiedad intelectual y la información relevante de las organizaciones y personas. Las redes inalámbricas 802.11 están en constante crecimiento actualmente, tienen la ventaja de ser flexibles y adaptarse a la infraestructura de las organizaciones, pero la desventaja que conlleva es que es vulnerable a cualquier tipo de ataque informático.*

De manera clara en el párrafo anteriormente citado se evidencia el daño que se pueden llegar a causar a los sistemas informáticos, cuando se está expuesto a un ataque informático, no solo se pierde la información si no que se puede llegar a tener una gran pedida económica, consecuente en lo anterior relaciono algunos de los ataques informáticos más comuniones en el mundo de las tecnologías.

[8] MEDINA ROJAS, Jonatán Deyvi; RIVAS MONTALVO, YONATHAN Yajanovic. Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos [En línea] 2020 Disponible en https://repositorio.unprg.edu.pe/handle/20.500.12893/8074

Figura 1 Grafica de ataques



Fuente: autor

4.1.5 Vectores de ataque en ciberseguridad: La ciberseguridad enfrenta diversos vectores de ataque, que representan las distintas vías utilizadas por los ciberdelincuentes para introducir códigos maliciosos con el fin de obtener ganancias económicas. El término "vector" se refiere generalmente a un punto débil o una falla en la seguridad establecida, a través del cual se puede infiltrar información. Es a través de estos vectores que los ataques cibernéticos explotan las vulnerabilidades en las redes, abarcando componentes como aplicaciones, computadoras, correos electrónicos y debilidades derivadas de la ingeniería social.

Estos vectores de ataque representan las puertas traseras que los atacantes utilizan para acceder a sistemas y datos valiosos. Entre los medios más comunes se encuentran los fallos en el software, las brechas en la seguridad de las redes, así como las vulnerabilidades en los sistemas operativos y las aplicaciones. Los ciberdelincuentes también pueden valerse de correos electrónicos maliciosos y tácticas de ingeniería social para engañar a los usuarios y obtener acceso no autorizado a información confidencial.

La importancia de abordar estos vectores de ataque radica en su potencial para causar daños significativos tanto a nivel financiero como en la reputación de individuos y organizaciones. La protección contra estas amenazas implica una combinación de soluciones tecnológicas avanzadas, políticas de seguridad sólidas y una educación continua en materia de seguridad cibernética. Al abordar de manera proactiva y efectiva los vectores de ataque en ciberseguridad, se puede reducir el riesgo y fortalecer la resiliencia ante las amenazas digitales en constante evolución.

Por esta razón, se sugiere encarecidamente implementar soluciones técnicas en seguridad informática que estén especialmente diseñadas para hacer frente a este tipo de ataques cibernéticos. Para proporcionar una comprensión más completa de los vectores de ataque en ciberseguridad y reconocer las aplicaciones más

comúnmente utilizadas como vías para perpetrar este tipo de ataques, a continuación, presento una lista de ejemplos:

4.1.6 Correo Electrónico: El correo electrónico es ampliamente reconocido como el principal vector de ataque, principalmente debido a su prominencia como uno de los canales de comunicación más utilizados en la actualidad. A lo largo de los años, el correo electrónico ha evolucionado de ser una herramienta de comunicación útil a ser un vehículo para diversas formas de ataques cibernéticos. Desde la proliferación del correo no deseado (Spam) hasta la ejecución de técnicas de suplantación de identidad (Phishing) y la distribución de archivos infectados con malware, este medio ha demostrado ser una superficie fértil para la actividad maliciosa en el mundo de la informática.

4.1.7 Navegación: Este tipo de vector se manifiesta mientras se navega por Internet, y a menudo surge a través de publicidad engañosa presente en anuncios. En estas situaciones, es posible descargar involuntariamente códigos maliciosos, como el Malware, Ransomware, Spyware u otras formas de virus capaces de causar daños tanto en la integridad como en el acceso a la información. Estos ataques, que se originan en la aparente seguridad del entorno en línea, pueden tener consecuencias perjudiciales y resaltar la necesidad de medidas de protección y precaución al interactuar en la web.

4.1.8 Endpoint: Dentro de este contexto de vector de ataque, nos referimos a las estaciones de trabajo empleadas por los empleados como una posible fuente de infección para los sistemas de la organización. Este virus puede propagarse a través de medios extraíbles, tales como memorias USB o discos duros portátiles. Por medio de esta estrategia, un atacante puede introducir código malicioso en los equipos de cómputo, causando daños considerables tanto a nivel de los dispositivos individuales como dentro de la red en su conjunto. Este enfoque subraya la importancia de implementar medidas de seguridad adecuadas y fomentar prácticas de uso seguro de dispositivos extraíbles dentro del entorno laboral.

4.1.9 Aplicación web: Cuando se mencionan las aplicaciones web, nos referimos a todos aquellos portales y páginas web de una organización que pueden ser utilizados a través de Internet. Estos recursos pueden convertirse en vectores de ataque, ya que ofrecen oportunidades para extraer cierta información que se encuentra en su interior de manera relativamente sencilla.

4.1.10 Red: La estructura de la red es de mucha importancia ya que al estar expuesta a ciertas vulnerabilidades se van a perpetuar ataques cibernéticos que coloque en riesgo la información, las grandes entiendes del gobierno, centro educativos y bancarios poseen conexión a través del Data Center y mediante este tomar soluciones de seguridad con la capacidad de fortalecer la red con la finalidad de evitar grandes pérdidas.

En síntesis, de lo anteriormente expuesto se puede evidenciar que son muchos los aspectos que influyen a la vulnerabilidad que están expuestos los sistemas de información, ya que se ven inmersos en el uso de las tecnologías, si bien se puede apreciar en la presente investigación los ataques cibernéticos más recurrentes se realizan mediante las herramientas que habitualmente utilizamos entre ellas el correo como medio de comunicación más frecuente dentro de las organizaciones, claro ejemplo.

La universidad del bosque, que atacaron el correo electrónico ya que fue el primer medio de comunicación que pudieron suplantar para extraer la información.

La universidad Javiera en sus sedes de Bogotá y Cali, afectando sus sistemas de informáticos, al evidenciar él lo sucedido de manera casi que inmediata un esquipo especializado en temas de ciberseguridad dio inicio a las labores informáticas que permitieran restablecer nuevamente el servicio, ya que si bien lo que se vio afectado en la operabilidad fueron los sistemas informáticos, se pretendía prevenir posibles robos de información o daños más severos, a pesar de este ataque informático las directivas de la universidad se pronunciaron que luego de verificar a profundidad el tema, no se evidencio fuga de información o perdida de información así mismo indico que los sistemas Core, están debidamente protegidos y que los sistemas fueron habilitados de manera gradual con la finalidad de que se garantizara la seguridad y el uso de sus sistemas informáticos.

4.2 MARCO CONCEPTUAL

4.2.1 Ataque Informático: se refiere al intento deliberado de acceder a sistemas informáticos o servidores mediante la introducción de virus o programas maliciosos con el propósito de alterar su funcionamiento, causar daños o extraer información sensible.

4.2.2 Amenaza Informática: toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático.

4.2.3 Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.

4.2.4 Ciberdelincuentes: No necesariamente tiene conocimientos técnicos. Usa el crimen como servicio como servicio.

4.2.5 Copia De Seguridad: Proceso mediante el cual se duplica la información existente de un soporte a otro, con el finde poder recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento.

4.2.6 DBA: (Database Administrator) Administrador de base de datos.

4.2.7 Denegación De Servicios: Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.

4.2.8 Dmz: Acrónimo en ingles de Desmilitarized Zone; en español, zona desmilitarizada, Consiste en una red aislada que se encuentran dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servicio web o de correo. Por lo general, un DMZ permite las conexiones procedentes tanto de internet como de la rede local de la empresa, donde están los equipos de los trabajadores, pero las conexiones que van desde DMZ a la red local están permitidas.

4.2.8 Escaneo De Vulnerabilidades: Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.

4.2.9 Fuga De Datos: La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

4.2.10 Fuga De Información: Proceso por el cual se produce una fuga de la información almacenada en una red interna o en dispositivos físicos provocada por un atacante malintencionado y que es volcada o publicada en internet para su libre consulta por parte de terceros sin autorización.

4.2.11 Filtrado De Paquetes: Mecanismo de un cortafuegos que permite controlar el acceso a una red interna a través del análisis de tráfico de paquetes tanto entrantes como salientes, teniendo en cuenta una serie de parámetros (dirección IP de origen y de destino, protocolo, etc.) así como su inclusión en una lista negra de IPs.

4.2.12 Hacking Ético: Actividades encaminadas a encontrar vulnerabilidades con el fin de remediarlas y mitigarlas. Estas actividades son autorizadas de manera formal.

4.2.13 Spyware:[9] Este es un programa espía, cuya finalidad principal es la obtención de información, a través de este se presenta un trabajo silencioso, sin dar rastro de su ejecución y de esta forma recolectar información sobre nuestra computadora personal.

[9] MALWAREBYTES ¿Cómo puede el spyware infectar mi equipo? [En línea] El spyware es una forma de malware que se oculta en su dispositivos Disponible en: https://es.malwarebytes.com/spyware/#:~:text=es%20el%20spyware%3F,Spyware.,Internet%2C%20as%C3%AD%20como%20otros%20datos.

4.2.14 Ataques informáticos: MIERES, Jorge.[10] Un ataque informático consiste en aprovechar alguna debilidad o falla (Vulnerabilidad) en el software, en el hardware, e incluso, en las personas que conforman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

DEFINO, Steven[11]. En la actualidad existen cinco (5) fases comunes de un ataque informático y de las cuales se pueden apreciar los siguientes: **Fase 1**. *Reconnaissance (Reconocimiento)*, A través de esta etapa se involucra la obtención de información (Information Gathering) con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing. **Fase 2**: Scanning (Exploración). En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners. **Fase3**. Gaining Access (Obtener acceso). En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración.

[10] MIERES, Jorge Ataques informáticos Debilidades de seguridad comúnmente explotadas [En línea] 2009 https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

[11] DEFINO, Steven Official Certified Ethical Hacker Review Guide [En línea] 978-1435488533 Delmar Cengage Learning; 1er edición (9 noviembre 2009) https://www.amazon.com/-/es/Steven-DeFino/dp/1435488539

Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking. **Fase 4** Maintaining Access (Mantener el acceso). Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos. **Fase 5:** Covering Tracks (Borrar huellas). Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

4.2.15 **Sistemas de información:** A la hora de definir sistemas de información quizás no se puede obtener un consenso sobre la definición de este, dentro de las definiciones más acertadas podemos encontrar sea propuesta por ***HERNANDEZ TRASOBARES, Alejandro.*** [12] *Quien lo defina como un "conjunto formal de procesos que, operando sobre una colección de datos estructurada de acuerdo a las necesidades de la empresa, recopila, elabora y distribuyen selectivamente la información necesaria para la operación de dicha empresa y para las actividades de dirección y control correspondientes, apoyando, al menos en parte, los procesos de toma de decisiones necesarios para desempeñar funciones de negocio de la empresa de acuerdo con su estrategia".*

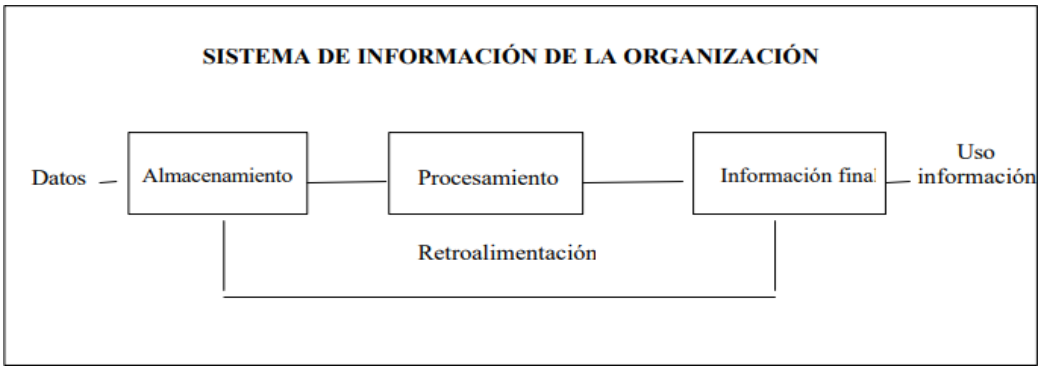
Todo sistema de información utiliza como materia prima los datos, los cuales almacena, procesa y transforma para obtener como resultado final información, la cual será suministrada a los diferentes usuarios del sistema, existiendo además un

[12] HERNANDEZ TRASOBARES, Alejandro. Los Sistemas De Información: Evolución Y Desarrollo [En línea] 2017 Disponible en www.Dialnet-LosSistemasDeInformacion-793097%20.pdf

proceso de retroalimentación o “feedback”, en la cual se ha de valorar si la información obtenida se adecua a lo esperado.

Consecuente con la anterior es importante ilustrar el anterior párrafo mediante la siguiente grafica que claramente se puede evidenciar el sistema de información de la organización y donde mediante esta, se almacena, procesa y se trasforma la información un resultado éxitos que permite a los usuarios del sistema obteniendo un rendimiento óptimo de sus recursos tanto de software como de hardware.

Figura 2 Sistemas de información de la Organización empresarial: funciones



Fuente: HERNANDEZ TRASOBARES, Alejandro. Los Sistemas De Información: Evolución Y Desarrollo [En línea] 2017 Disponible en www.Dialnet-LosSistemasDeInformacion-793097%20.pdf

4.2.16 Universidades: El concepto universidad, que en su acepción etimológica se remonta a la cultura clásica romana, aparece en la lengua latina como universitas, el cual significa “el conjunto de todas las cosas para Cicerón es el mundo, el universo. Columela escribe sobre las universitas rustications, la agricultura en general. Plinio se refiere al todo del discurso, con universitas orationis

Pablo de Ballester explica que la idea griega de universidad fue: Panepistimion. Pan: todo, por completo, integrado; epi: encima; istimi: estar (de donde viene

estatua, stabat mater, etc.) El universitario es aquel que está encima de su tema, es decir, el que está dominando su materia, el que se ha enseñoreado perfectamente de un conocimiento. No el que se informó y lo transmite, sino que lo posee, que está encima de eso, que es suyo[13]

4.3 MARCO LEGAL

El congreso de la república en uso de sus facultades legales y aquellas que le confiere la ley y en especial el Articulo 150 numeral 1 de la Constitución Política de Colombia, realiza una modificación del código penal, donde se crea un bien jurídico tutelado a través de la ***Ley 1273*** *del 2009* ***(enero 5 del 2009)***[14] denominado "de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". **CAPITULO PRIMERO.** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

A través de la presente ley cuenta con una regulación legal en el caso que se pueda llegar algún perpetuar ataque de acuerdo con las disposiciones que se presentan en la mencionada ley, dentro del estudio del presente trabajo esta aplicaría cuando mediante un ataque informático se vulneran los sistemas de una organización.

El congreso de la república en uso de sus facultades legales y aquellas que le confiere la ley y en especial el Articulo 150 numeral 1 de la Constitución Política de Colombia crea la **LEY ESTATUTARIA 1581 DE 2012[15],** La cual tiene como objeto, La presente ley tiene por objeto desarrollar el derecho constitucional que tienen

[13] DE BALLESTER Pablo, El fantástico Mundo Griego, México, Publicaciones Cruz O., 1991, p. 187
[14] Ley 1273 del 2009 Congreso de la República, "de la protección de la información y de los datos"- Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[15] Ley Estatutaria 1581 De 2012 Congreso de la República. Por la cual se dictan disposiciones generales para la protección de datos personales

todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

que la popularización del término SI (Seguridad de la Información) fue motivada por la elevación en el número de incidentes de seguridad, ocurridos a nivel mundial. Los trastornos generados por esos incidentes son variados, generando daños a la imagen del negocio o fuga de informaciones críticas, lo que puede resultar en pérdidas financieras sustanciales.

Las presentes normas se adhieren al presente trabajo en el sentido que a través de ellas se puede evidenciar las diversas acciones que se pueden llevar a cabalidad cuando se pueda llegar a faltar a los establecido en ellas, es decir aquella persona que realice ataques frente a los sistemas informáticos.

4.3.1 Ley 599 del 2000[16] Por la cual se expide el Código Penal. se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa"

16 Ley 599 del 2000 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Ley 1341 del 2009[17] "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"

[17] Ley 599 del 2000 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

5 DESARROLLO OBJETIVOS

5.1 FUENTES DE INFORMACIÓN RELACIONADAS CON ATAQUES INFORMÁTICOS:

Comencemos por definir que es un ataque informático; los ataques informáticos son una serie de intentos que se realizan desde cualquier lugar del mundo a un determinado equipo informático o servidor, mediante le penetración de virus informático el cual conlleva la alteración de los sistemas, cuando se hace referencia a un ataque informático, se habla del intento de ingreso de manera abrupta a la seguridad informática la cual coloca en riesgo determinado conjunto de hardware y/o software que contiene información privilegiada.

Asimismo, El mundo está experimentando la cuarta revolución industrial de la tecnología, el imparable avance de los medios tecnológicos y la inmersión de las Tecnologías de la Información y las Comunicaciones (TIC) sin lugar a duda han aportado a la humanidad cambios significativos, no solo en lo personal si no en los ámbitos económicos, sociales y políticos. Por otra parte, es importante mencionar que de manera simultánea esta evolución tecnológica ha provocado una avalancha de ataques informáticos, donde los ciberdelincuentes a través de herramientas experimentadas aprovechando las debilidades y vulnerabilidades de las infraestructuras tecnológicas, haciendo uso de sus habilidades atacan de manera abrupta los sistemas informáticos colocando en riesgo el activo más importante de las organizaciones como lo es la información, afectando los tres elementos fundamentales de los sistemas de información como lo son la confidencialidad, integridad y disponibilidad de los sistemas.

5.2 Ataque informático Universidad del Bosque: Es así, como a continuación y de acuerdo con las fuertes de información consultadas y analizadas referente a ataques informáticos se coloca en contexto el ataque perpetuado el 28 de junio del 2021 a la Universidad del Bosque, donde ciberdelincuentes accedieron a datos personales de la comunidad estudiantil y administrativa, tomando el control de correos institucionales, aulas virtuales, Cuentas de Google Drive, Redes sociales y de más plataforma, donde se vio involucrando tanto infraestructura interna como externa de la universidad.

El tipo de ataque mediante esta técnica de engaño que se llevó a cabo en la Universidad del Bosque, es el denominado **spear phishing,** mediante esta práctica de ataque se puede obtener credenciales de acceso de los usuarios que comprometer la infraestructura de una organización, la ejecución del este ataque se efectúa mediante correo electrónico, que mediante una URL contenida en el cuerpo de correo contiene direccionamiento a otras fuertes que extraen información personal entre ellas contraseñas de cuentas bancarias, correo electrónicos y redes sociales.

5.1.2 Formas de contrarrestar y prevenir el ataque spear phishing: Existen diferentes prácticas que permiten prevenir el ataque informático a través del Spear Phishing de las cuales encontramos las siguientes:

Veracidad del remitente: Es decir, se debe verificar que el dominio de correo electrónico remitente sea un dominio de confianza de remitentes que normalmente recibe el usuario.

Verificación del lenguaje: Comúnmente los ciberdelincuentes cometen errores de ortografía, concordancia y relación a la hora de redactar los correos electrónicos que tiene como objetivo perpetuar el ataque.

Verificación de la URL: El usuario al observar un URL dentro del contexto del correo lo primero que debe realizar es cruzar el mouse sobre esta, con la finalidad de verificar el contenido de esta.

Así las cosas, se puede observar que los sistemas de información e infraestructura de la Universidad del Bosque estuvieron expuestos bajo la vulnerabilidad y ataque que conllevo realizar acciones tempranas para impedir acciones incontrolables sobre el secuestro de sus plataformas.

5.1.3 Ataque informático Universidad Nacional de Colombia: La Universidad Nacional de Colombia a inicios del año 2023 sufrió un ataque informático en sus nueve (9) sedes de las cuales se vio comprometida la infraestructura tecnológica, generando la indisponibilidad de los servicios, entre ellos, servidores sin acceso, portales y pagina web. [18]

El tipo de ataque que se efectuó en la infraestructura de la Universidad Nacional de Colombia fue a través de un **Ransomware,** este tipo de ataques es una forma de virus malicioso impidiendo a los usuarios acceder a los archivos, posterior a realizar la encriptación de la información advierte al usuario que para acceder nuevamente a la misma, se debe realizar el pago por el rescate, este tipo de virus cuenta con diferentes formas con las cuales puede infectar los dispositivos, uno de los métodos más recurrentes en la actualidad, es mediante mensajes de correos electrónicos no deseados donde dentro del contexto del mensaje contiene archivos adjuntos como PDF o documentos en Word.

Las acciones adoptadas por el personal de infraestructura y Gestión de Servicios TI, Seguridad de la Información, Identidades Profesionales Digitales permitieron que

[18] Los detalles secretos del grave hackeo que sufrió la Universidad Nacional [En línea] 2023. Disponible en: https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335/

el ataque no se perpetuara en su totalidad tanto en los demás servidores como que se apoderara de la totalidad de la información que ya se encontraba afectada.

Referente a la prevención de este tipo de ataques como lo es el Ransomware primeramente contar con buena infraestructura de seguridad informática, antivirus, firewall, protección en tiempo real diseñado para frustrar ataques avanzados, y contar con protección especial de los programas o software más vulnerable que exista dentro de la organización.

5.1.4 Ataque informático Pontificia Universidad Javeriana: Para el año 2021 la universidad javeriana fue blanco de ataque informático el cual derivo el secuestro de datos por parte de hacker informáticos afectando sus sedes en Bogotá y Cali, el cual conllevo a la suspensión de algunos servicios que brinda la institución mediante servicios web, ya que su infraestructura informática quedo en riesgo. El tipo de ataque perpetuado aún se desconoce. [19]

En relación con la investigación sobre fuentes de información, se puede apreciar diferentes formas de ataques las cuales son utilizadas con recurrencia por intrusos informáticos para efectuar el cibercrimen de una manera más efectiva, es así como se relacionan las siguientes técnicas de ataques.

5.1.5 Técnicas de ataques DOS árboles de ataques: Esta es una de las técnicas más recurrentes por los ciberdelincuentes para realizar ataques a los sistemas de información, pero primeramente para contextualizar el termino DoS, Se es necesario realizar una ilustración de este.

5.1.6 DoS (50ELACIONA Service) traducido al español "Denegación de Servicio" Consiste en generar una serie de peticiones de manera masiva al

[19] Universidad Javeriana confirmó que fue víctima de un ataque cibernético [En línea] 2021. Disponible en: https://www.infobae.com/america/colombia/2021/11/23/universidad-javeriana-confirmo-que-fue-victima-de-un-ataque-cibernetico/

servidor, con la finalidad de provocar una sobre carga de este y por consiguiente la alteración o denegación del servicio al que recurren los usuarios finales, para realizar la detención de este tipo de ataque basta con identificar la dirección IP de donde se está realizando y bloquear el acceso de manera inmediata, de esta forma la sobrecarga desaparece y se restablece el servicio.

Ahora bien, definido lo que es un DoS, podemos encontrar lo que se denomina un ataque DdoS (Distributed 51ELACIONA Service) traducido al español (Denegación Distribuida de Servicio) Este a diferencia del DoS, es un poco más complejo de detener ya que la metodología utilizada por los ciberdelincuentes es diferente, ya que se realiza desde diferentes ordenadores diferentes realizando llamadas masivas y de forma constante al servidor, cada uno con una dirección IP distinta y ubicados en diferentes lugares.

Usualmente los computadores empleados para realizar los Ataques DdoS, son computadores personales que contienen un virus informático, que permite al atacante realizar uso eficiente de los recursos del hardware del equipo atacante perpetuar los ataque DdoS, Es decir mediante esta técnica lo que permite es crear una red de computadores que se tiene un control des de un punto central y de esta forma desestabilidades de una manera más rápida y efectiva sobre los servicios.

Consecuente con lo anterior me permito relacionar y definir los diferentes ataques que se presenta mediante el uso de las dos técnicas anteriormente presentadas.

5.1.7 DoS y DoS Inundación SYN (SYN flooding): El presente método consiste, donde un usuario a través de un programa cliente, hace uso para llevar acabo un ataque usando paquetes regulares y paquetes grandes, con tamaño superior de 250 bytes de manera simultánea él envió de paquetes agotan los recursos del servidor y los paquetes grandes saturan la red.

5.1.8 Cortina de Humo: a través del de este ataque desvía la atención ataque en la camada OSI, y este se ejecuta mediante otro vector de la red con la finalidad de ocasionar conflicto en las reglas de seguridad de la red automatizadas.

5.1.9 Ataques de fragmentación: A través de la presente técnica se realiza un ataque a la red mediante a saturación el cual ocasiona la negación del servicio, Fragmentado los paquetes remontados de una manera deliberada y de esta manera saturando el servicio, cuando finalmente el paquete es remontado, se impide el funcionamiento del Host. También se puede enviar fragmentos incompletos con o en cantidades mínimas para obtener el mismo efecto, para los especialistas en seguridad informática la diferencia que se evidencia está en el comportamiento del usuario con el sistema de contraseña bajo el ataque constante de ciberdelincuentes.

5.1.10 Árboles de Ataque[20]: El objetivo de un árbol de ataque es estudiar y analizar cómo se puede llevar a cabo un ataque y por tanto permite identificar de qué forma se puede evitar que este suceda mediante despliegue de técnicas de seguridad informática, el árbol de ataques también permite estudiar actividades que tendría que estudiar el atacante.

[20] GUÍAS GENERALES GLOSARIO ABREVIATURAS, Arboles de ataques [En línea] 2019. Disponible en https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=72.html

5.1.11 Fases de ciberataque : El principal y más acertado objetivo de un ataque es el de raptar información o cifrar contenidos para posteriormente s pedir un rescate por la misma, pero para ellos se requiere de plena observación del objetivo al que se va atacar, es por eso que dentro del estudio de investigación presentado para el caso que nos convoca, se puede evidenciar que los ciberataques cuentan con unas fases que le permite a los ciberdelincuentes obtener de una forma más inteligente su objetivo principal que es el de obtener la información o como se indicó anteriormente cifrarla, es por eso que a continuación me permito mencionar algunas de las fases más comunes que se pueden llegar a presentar.

5.1.12 Reconocimiento: en esta fase el atacante busca documentar con información sobre la empresa, normalmente inicia explorando la información que esta sobre la página web de la organización, posteriormente realizan un riguroso estudio sobre los sistemas de información, es decir que tecnologías utilizan e interactuar con el correo electrónico y demás redes sociales donde se esté publicando información de la organización.

5.1.13 Preparación: Sobre esta etapa el delincuente prepara el ataque al objetivo propuesto, un claro ejemplo es suplantar el correo de alguno de los empleados de la organización e iniciar a enviar conversaciones para obtener más información de una forma fraudulenta, normalmente dentro de estos correos se envía enlaces alternos que al abrirlos raptan información confidencial.

5.1.14 Distribución: En el trascurso de esta fase se genera la trasmisión del ciberataque, que normalmente se realiza por un documento comprimido que se envía a través de correo electrónico o de phishing, es decir mediante mensaje de texto.

5.1.15 Explotación: En este justo momento es donde el atacante compromete el equipo infectado y la red, esto se pueden conseguir a través de la explotación de vulnerabilidades, por medio de puertos que se encuentren abiertos o no se haya instalado parches de seguridad, es por eso la importancia de las actualizaciones o antivirus activo.

5.1.16 Instalación: En el trascurso de esta fase realiza la instalación del malware o rapta las credenciales de la víctima.

Para contextualizar lo anteriormente expuesto frente a los ataques que se presentan a los sistemas de información y los métodos que los ciberdelincuentes utilizan aprovechando las vulnerabilidades que existen, traeré a colación el caso que se presente en la universidad del bosque en el año 2021 y que fue considerado por expertos como un campanazo a las demás instituciones de educación superior

Figura 3 Fases de Ciberataque

Fuente: autor

Según lo anteriormente expuesto, se puede observar que uno de los ataques más frecuentes contra las instituciones de educación superior se lleva a cabo a través de la manipulación de sus bases de datos, mediante técnicas como el Ransomware, el Spear Phishing y la Denegación de Servicio Distribuido (DDoS). Mediante estas modalidades, los ciberdelincuentes aprovechan para enviar información engañosa a los usuarios dentro de las organizaciones, con el objetivo de que estos abran o ejecuten archivos adjuntos. Una vez ejecutados, el virus se propaga por la red de la organización, logrando su objetivo de secuestrar información de manera ilegal para luego exigir un rescate por la misma.

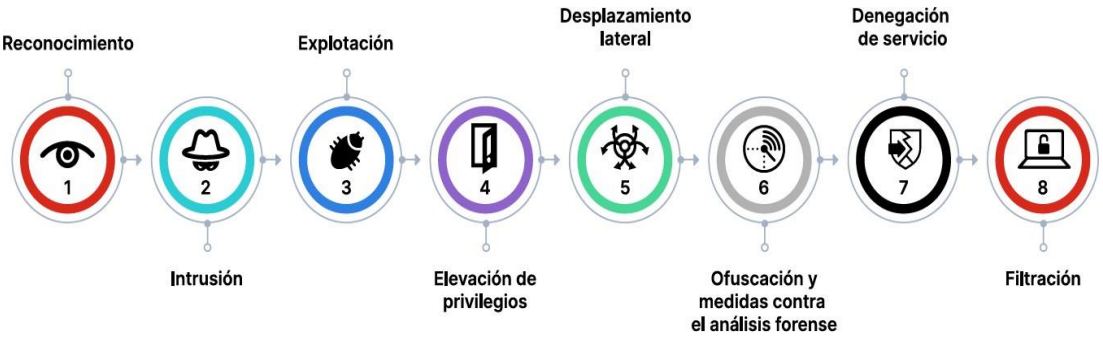
Además, es importante destacar que existen diversas estrategias para hacer frente a estas situaciones mediante medidas preventivas. Entre estas se encuentran la verificación de la autenticidad del remitente y del dominio del correo electrónico, mantener actualizado el antivirus, y contar con sistemas de infraestructura tecnológica actualizados, entre otras medidas.

5.2 ANALIZAR FUENTES DE INFORMACIÓN RELACIONADA FRENTE ATAQUES INFORMÁTICOS

El objetivo del presente estudio consiste en llevar a cabo una exhaustiva revisión de fuentes de información académica, tales como libros, artículos y revistas, con el fin de identificar una amplia gama de ataques informáticos. Ataques que son perpetuados comúnmente por ciberdelincuentes en su intento de cometer actos ilícitos contra sistemas de información. Así las cosas, es importante resaltar que mediante el presente ejercicio de revisión nos permita identificar los diferentes tipos de ataques con mayor recurrencia y que se han vuelto muy comunes en el panorama actual y aún más en el auge de la tecnología.

5.2.1 Taxonomía de un ataque informático: la presente imagen ilustra la taxonomía de incidentes que se pueden presentar en las redes o equipos de cómputo de las organizaciones.

Figura 4 Taxonomía de un ataque informático



Fuente: https://www.ucr.ac.cr/noticias/2022/5/05/voz-experta-taxonomia-del-malware-el-caso-ransomware-conti.html

Para comprender un poco más al detalle la taxonomía de un ataque informático es esencial explorar sus características fundamentales representadas mediante una estructura básica. Esta estructura tiene como objetivo principal identificar el tipo de ataque que se está llevando a cabo. En primer lugar, se busca realizar un reconocimiento del objetivo del ataque, como, por ejemplo, el robo de información confidencial, un acto de gran relevancia para cualquier organización. Además, se puede identificar un segundo tipo de objetivo, que implica la interrupción de los servicios web o cliente-servidor. Estos reconocimientos iniciales son cruciales para entender la naturaleza y las motivaciones detrás de un ataque informático. Mediante la taxonomía de ataque podemos encontrar diferentes tipos de ataque y su clasificación, es así como posterior al reconocimiento por parte de los ciberdelincuentes, se procede por los mismos a perpetuar la intrusión del ataque a través de diferentes métodos de ejecución como lo son:

5.2.2 Ataques de inyección (SQL injección, XSS): Es importante conocer cómo podemos prevenir los atauques informáticos de inyección de SQL como factor principal consiste en la capacitación del personal responsable de las diferentes aplicaciones de la organización Los ataques dirigidos a servidores SQL representan una grave amenaza para la seguridad de los datos almacenados. En estos escenarios, los atacantes buscan comprometer la integridad y confidencialidad de la información, poniendo en riesgo datos sensibles de los usuarios, como números telefónicos o detalles de tarjetas de crédito. Este tipo de ataque implica la manipulación o eliminación de datos, exponiendo la información confidencial a accesos no autorizados. La situación se agrava aún más cuando los atacantes logran obtener privilegios de administrador mediante la inserción de código malicioso. Este nivel de acceso les permite realizar acciones destructivas con mayor libertad y potencialmente causar un daño considerable tanto a nivel de seguridad como de confianza en el sistema afectado.

Es imperativo adoptar medidas de seguridad robustas y establecer protocolos de protección efectivos para contrarrestar los riesgos derivados de posibles ataques, garantizando así la preservación de la integridad de los datos almacenados en servidores SQL.

5.2.3 Ataques de interceptación de datos (man-in-the-middle). Este tipo de ataques informáticos se caracteriza por su naturaleza sigilosa, donde el ciberdelincuente busca interceptar y alterar la comunicación entre diferentes partes, como un emisor y un receptor. El objetivo primordial de estos ataques es obtener acceso no autorizado a la información transmitida y, en muchos casos, modificar el contenido de las conversaciones entre las partes involucradas. Esta capacidad de manipulación de la comunicación representa un peligro significativo, ya que los ciberdelincuentes pueden acceder y modificar datos sensibles, como contraseñas, números de tarjetas de crédito y detalles de cuentas bancarias. Además, estos ataques pueden dirigir a los usuarios a sitios web maliciosos con el fin de robar aún más información confidencial. La amenaza planteada por estos ataques subraya la importancia de implementar medidas de seguridad robustas para proteger la integridad y la confidencialidad de la información durante la transmisión en línea.

5.2.4 Phishing : El termino Phishing se deriva de Fish, que tiene como significado *“Pesca”* en inglés, siendo hoy en día es uno de los ataques informáticos más frecuentes, ataque malicioso, el sector de vulnerabilidad que se presenta es a través del correo electrónico que consiste en recibir información que a simple vista parecieran de fuentes confiables, pero que, en realidad estos contienen un enlace o hipervínculo que a la hora de abrirlo coloca en riesgo la información y datos personales, otra forma de recibir este tipo de virus es mediante mensajes de texto, (SMS) a través del diseño es así como a través de esta técnica los ciberdelincuentes engañan a los usuarios para robarles información confidencial de estos como lo son los datos personales en especial contraseñas o en su defecto realizar suplantación de identidad.

El contexto de los mensajes enviados a través de esta técnica de ataque, los ciberdelincuentes suelen utilizar el mismo lenguaje a la hora de realizar el envío masivo de esta técnica, es por eso por lo que, hoy en día es un poco más practico identificar que ese tipo de correos se trata de una forma de engaño para raptar de forma inapropiada datos, a manera de ilustrar lo anteriormente mencionado, observemos la siguiente imagen.

Figura 5 Pasos ejecución Phishing

Fuente: autor

Este tipo de ataque informático de acuerdo con lo establecido en las tres universidades citadas, Universidad Nacional de Colombia, Universidad del Bosque y Universidad Pontificia Javeriana, se generó mediante este ataque, no obstante, no produjo mayo efecto ya que se tomaron las acciones tempranas de control.

El sector de vulnerabilidad que se ejerce con este lo hace a través de los sistemas en especial los servidores donde reposa la información, para el caso de las universidades citas en la búsqueda de la información, en la Universidad Nacional y la Universidad Pontificia Javeriana, se logró el secuestro de servidores de correos electrónicos y pagina web, pero estas instituciones no pagaron por su rescate ya que, de manera oportuna detuvieron el ataque.

En la siguiente imagen se puede observar los pasos de ejecución del ataque Ransomware que se ejecuta comúnmente:

Figura 6 Pasos ejecución de un Ransomware

Fuente: autor

5.2.5 Adware: Este tipo de software que se encuentra diseñado con el fin de mostrar publicada en la pantalla del dispositivo a través del explorador en especial Google Chrome donde se despliegan anuncios de forma automática, don dudosos programas que induce a dar clic sobre publicidad.

Este tipo de software que se encuentra diseñado con el fin de mostrar publicada en la pantalla del dispositivo a través del explorador en especial Google Chrome donde se despliegan anuncios de forma automática, don dudosos programas que induce a dar clic sobre publicidad.

La forma que permite evitar que mediante este tipo de publicidad se genere vulnerabilidad, lo más recomendable es realizar la instalación de extensiones a través del explorador, la extensión más común es Adblock esta extensión impide el tráfico de información publicitaria de contenidos no deseados y lo que genera es un bloqueo inmediato.

Mediante este tipo de ataques con respecto a las 3 tres universidades citadas, no se perpetuo en ninguna de las instituciones, pero es de recalcar que es una técnica muy usual utilizada por los ciberdelincuentes para raptar información de forma indebida.

Asimismo, en la siguiente imagen tenemos un ejemplo de un ataque informático de Adware.

Figura 7 Pasos ejecución de un Adware

Fuente: autor

Según lo expuesto anteriormente, se pueden observar los versos ataques informáticos, los cuales se caracterizan por iniciar con una toxemia de ataque. Este proceso comienza con un reconocimiento especial de la víctima y progresa hacia una intrusión por parte del atacante, quien emplea métodos como inyecciones (SQL, XSS), interceptación de datos, phishing, ransomware, entre otros.

Además, es evidente que contrarrestar este tipo de ataques requiere la adopción de medidas necesarias para prevenir la intrusión de los mismos.

5.3 IDENTIFICAR ESTRATEGIAS DE MITIGACIÓN DEL RIESGO

Antes de comenzar a contextualizar e identificar las estrategias de riesgo, comencemos por comprender **¿Qué es un riesgo?**

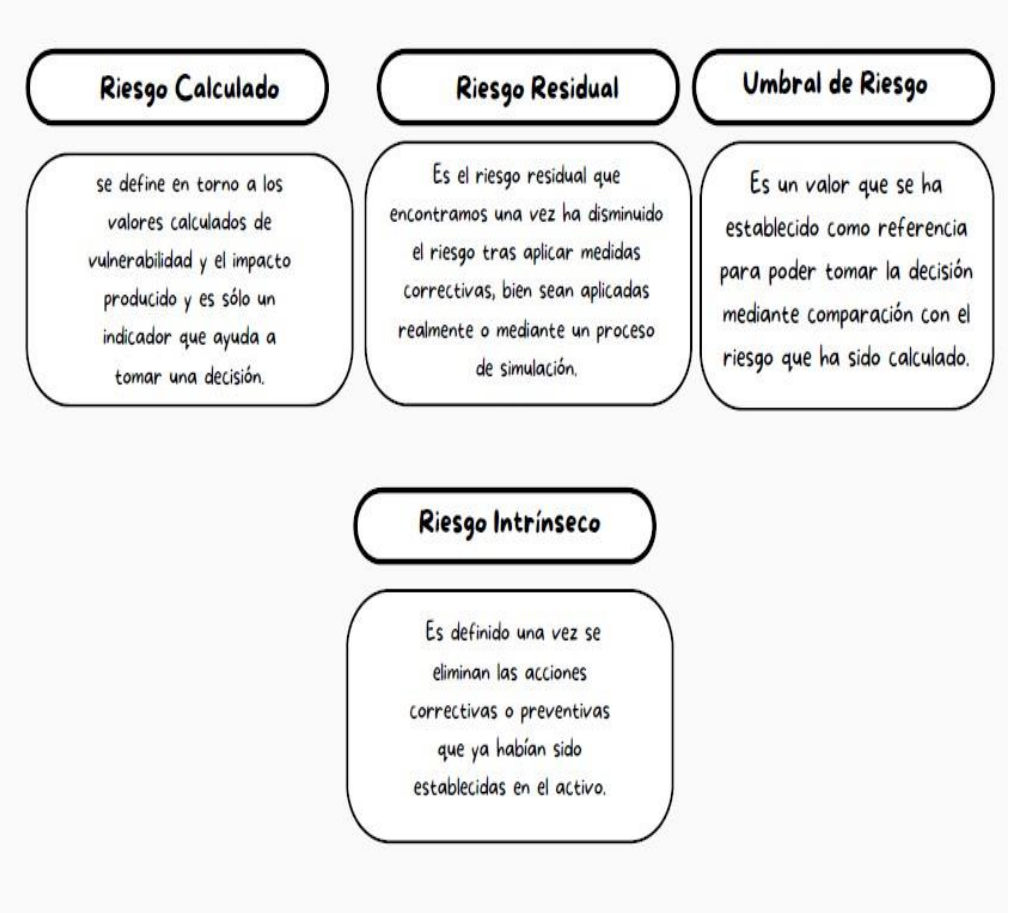
Entiéndase como riesgo, una alta probabilidad que se produzca un impacto en uno de los activos de seguridad, donde a través de este se ven comprometidos los activos de seguridad, donde se pueden ver comprometidos diferentes sistemas de información e incluso estar en riesgo toda la organización, es de anotar que el nivel de riesgo se determina de acuerdo al impacto de la vulnerabilidad.

5.3.1 Características del riesgo: Según lo establecido en la **ISO27001** es considerado el riesgo el resultado que se refleja mediante el análisis de riesgo, este análisis de riesgo, se considera la ejecución de un proceso complejo que permite identificar las debilidades, para posteriormente decidir si se toman las acciones sobre las mismas.

5.3.2 Tipos de riesgo: Los tipos de riesgo se identifican dependiendo el objetivo específico que se requiera, es a través de este que se la acción, los tipos de riesgo más comunes que se encuentran, se puede identificar el riesgo calculado, riesgo residual, umbral de riesgo y riesgo intrínseco.

A través de la presente imagen se observa el objetivo principal de cada uno de los riesgos anteriormente citados.

Figura 8 Tipo de Riesgos

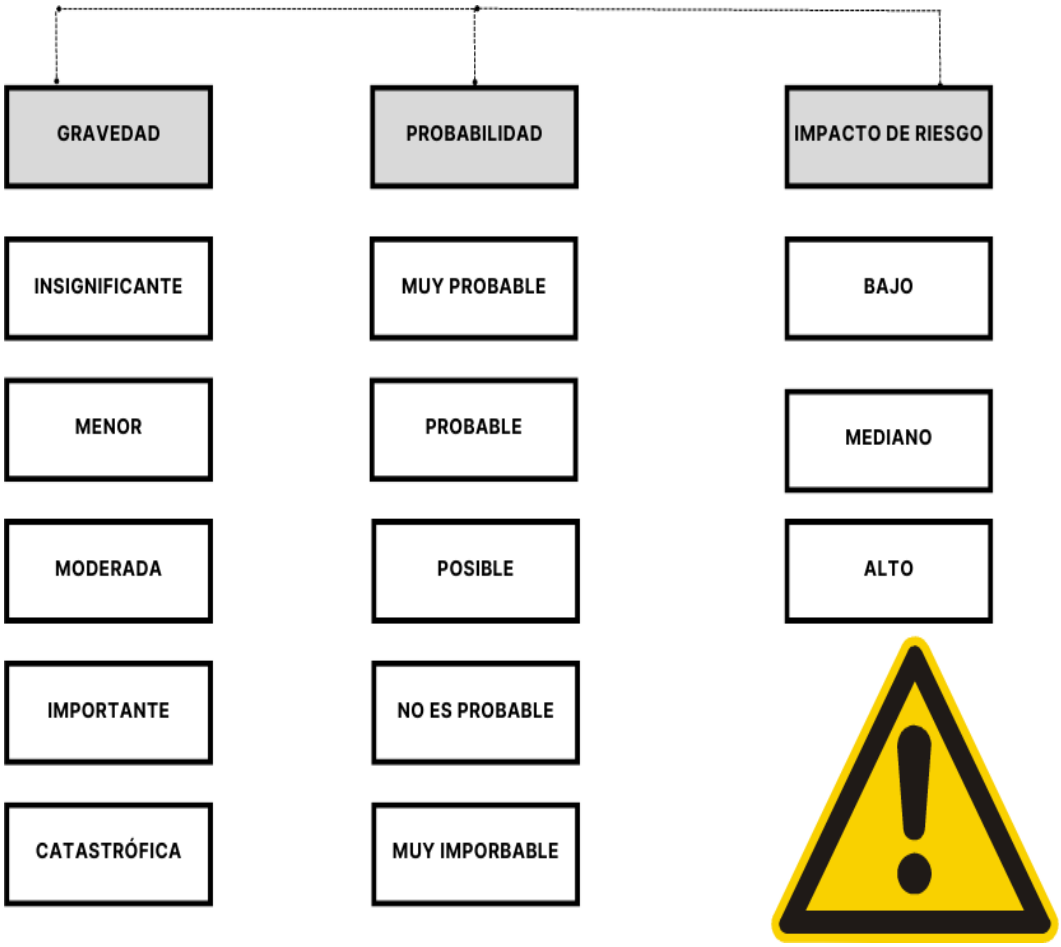


Fuente: autor

5.3.3 Estrategias de mitigación de riesgo: Las estrategias de mitigación de riesgos representan un proceso fundamental que se lleva a cabo a través del desarrollo de diversas opciones y acciones. Estas medidas se implementan con el propósito de reducir al mínimo el impacto negativo o la probabilidad de que ocurra una acción o evento específico que podría ocasionar daños irreversibles en los sistemas de información.

Con el fin de poner en contexto, a través de la siguiente imagen, podemos observar los criterios que se deben tener en cuenta al adoptar estrategias de mitigación del riesgo.

Figura 9 Criterios de la matriz de riesgo



Fuente: autor

5.3.4 Riesgos asociados a procesos, personas y tecnologías: los riesgos que pueden existir en relación a procesos persona y tecnología son aquellas actividades que pueden ser ocasionales de manera intencional que surgen mediante de procedimientos inapropiados o defectuosos o que pueden surgir por desastres naturales.

5.3.5: Plan para mitigar de riesgo que permitan brindar protección adecuada a los sistemas de información frente a los ataques informáticos: La seguridad de la información es un proceso fundamental en el cual se detectan y promueven el uso de sistemas autorizados, de acuerdo con las políticas implementadas dentro de las organizaciones. Esto implica el cumplimiento riguroso a través de diversos mecanismos para garantizar el correcto funcionamiento de los activos de la organización frente a las posibles amenazas que puedan surgir de forma inesperada por parte de terceros. Es esencial implementar acciones preventivas para mitigar el riesgo en los sistemas de información. Esto va más allá de contar simplemente con infraestructuras que aseguren el buen funcionamiento de los sistemas; implica realizar análisis de riesgos exhaustivos sobre los sistemas de información e implementar normas y estándares internacionales que orienten y faciliten la adopción de medidas preventivas y correctivas en las arquitecturas de los sistemas tecnológicos.

Por lo tanto, a través de la presente investigación, se pudo evidenciar una serie de medidas preventivas y correctivas que deben ser implementadas para adoptar buenas prácticas que minimicen el riesgo al que están expuestos los sistemas informáticos.

Es crucial enfatizar que los planes de mitigación de riesgos representan una medida preventiva altamente eficaz ante las distintas eventualidades que puedan surgir. Estos planes desempeñan un papel fundamental en la reducción de pérdidas, al mismo tiempo que simplifican la planificación, el diseño y la colaboración en la gestión del riesgo al evaluar la probabilidad de ocurrencia de dichos riesgos.

De esta manera, al examinar la imagen proporcionada, podemos visualizar las etapas iniciales y de planificación del proyecto, donde se identifican los activos involucrados, se determina el tipo de amenaza más relevante, se realiza la

identificación del riesgo, se evalúa su criticidad y se establece el tratamiento necesario para contrarrestar los posibles efectos que este riesgo podría generar.

Figura 10 Plan de mitigación de riesgo

PLAN DE MITIGACIÓN DEL RIESGO								
ACTIVO	AMANAZA	DEFINICIÓN DE AMENAZA	RIESGO	NIVEL DE CRITICIDAD	VULNERABILIDAD	SALVAGUARDAR	TRATABMIENDO DEL RESIGO	ISO 27002
INFRAESTRUCTURA TI	amenazas persistentes avanzadas (APTs)	Ataques informáticos por ciberdelincuentes	5.5	Alto	Falta de Gestión ubicación de infraestructura fuera de las instalaciones	Contratar servicios en la nube para evitar pérdida de información	Mitigar	8.1.3 Uso aceptable de los activos - Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
RED	intrusos con privilegios, robo de contraseñas, espionaje	Ataques e intrusión de red por ciberdelincuentes	6.5	Alto	Falta de administración mediante firewalls u Checkpoint	Restringir acceso mediante permisos elevados	Mitigar	6.1.2 Segregación de tareas - Control Las funciones y áreas de responsabilidad deberían segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
SISTEMAS DE INFORMACIÓN	Ataques informáticos, mediante malware, troyanos	Ataques a las aplicaciones empresariales	6.7	Alto	Falta de centro de datos para almacenar la información	Servidor dedicado para la información mediante cintas de respaldo	Mitigar	0.2 Requisitos de seguridad de la información Es esencial que una organización identifique sus requisitos de seguridad. Existen tres fuentes principales para los requisitos de seguridad: i. Evaluar los riesgos para la organización; ii. requisitos legales, reguladores, estatutarios y contractuales; iii. conjunto particular de principios, objetivos y requisitos comerciales

Fuente: autor

Como se mencionó previamente, el correo electrónico se identifica como el vector más vulnerable para llevar a cabo ataques informáticos. Por esta razón, a continuación, presentaré las medidas que deben ser consideradas para prevenir este tipo de ataques.

5.3.6 Protección del vector de ataque común correo electrónico[21]: Como regla general en lo que respecta a la protección que debemos implementar, consiste en la monitorización de cualquier actividad de mensajería que pueda considerarse sospechosa, especialmente los correos que incluyan documentos adjuntos que no hayan sido previamente analizados por un antivirus web.

5.3.7 Detección temprana de código o archivos maliciosos: La mejor práctica para garantizar el correcto funcionamiento de los equipos de cómputo dentro de las organizaciones consiste en realizar un inventario completo del hardware disponible, junto con las correspondientes licencias de uso. Posteriormente, es fundamental asegurarse de que todos los equipos cuenten con un antivirus con licencia. Además, se recomienda que todos los programas y software utilizados en la empresa estén debidamente licenciados. Esto facilita la actualización efectiva del software, permitiendo la descarga de parches de seguridad necesarios para evitar vulnerabilidades, ya que los equipos de cómputo son especialmente susceptibles a amenazas debido a su función operativa.

5.3.8 Protección de contraseñas: El uso y la gestión de contraseñas deben ser objeto de una protección rigurosa. Con frecuencia, caemos en la mala costumbre de recordar nuestras contraseñas en los navegadores o incluso de anotarlas en notas adhesivas y ubicarlas en lugares visibles, como el escritorio o documentos personales. Para abordar esta situación, se recomienda el uso de software seguro de gestión de contraseñas, donde estas se almacenan de forma encriptada y segura, garantizando así una protección efectiva de la información sensible.

[21] EMPRSARIA & LABOR ¿Cómo evitar y proteger la información de ataques informáticos? [En línea] 2020 Disponible en https://revistaempresarial.com/tecnologia/como-evitar-y-proteger-la-informacion-de-ataques-informaticos/

5.3.9 Identificación de activos: Dentro de los activos de información en las organizaciones podemos encontrar dos tipos de activos los cuales generan valor, claramente debemos identificarlos y como se encuentran divididos estos (tangibles e intangibles) a maneral de ejemplo relaciono los siguientes: Información, Reputación, Marca, Instalaciones, Equipos, Dinero en efectivo e Inversión, Lista de clientes, Investigaciones, Personas y Servicios / Procesos de negocio.

La identificación de amenazas es primordial ya que dentro de estas son múltiples las amenazas que se pueden llegar a presentar en las diferentes plataformas o sistemas de información es así donde me permito relacionar las más relevantes como lo son: Físicas, Eventos naturales, Perdida de servicios esenciales, Perturbación debido a la radicación, Compromisos de información, Fallas técnicas, Acciones no autorizadas, Compromisos de funciones.

5.3.10 Identificación de Vulnerabilidades: En estos espacios de vulnerabilidades es donde se encuentra expuesta la infraestructura y de más aplicaciones funciones de los sistemas de información por consiguiente me permito relacionar los siguientes: Red, Físicas, Aplicaciones y Servicios, Utilidades, Cadena de suministros, Procesos, Equipos, Computación en la nube. Biga Data y Evolución de vulnerabilidades.

5.3.10 Medias preventivas: Si bien en Colombia no se tiene extremas medidas para penalizar los delitos informáticos mediante la LEY 1273 DE 2009 se modifica el código penal y se crea un nuevo bien jurídico tutelado, denominado “ De la protección de la información y de los datos personales” donde se adiciona al título VII del mencionado código, es en esta ley que quienes encuentre responsables frente los atentados en contra de la confidencialidad, integridad y disponibilidad de la información de los datos y los sistemas informáticos pueden acarrear con problemas penales por violentar el acceso no autorizado de los sistemas de información.

Es así como, para evitar el desconocimiento por algunos de los empleados frente al delito informático, es necesario plasmas una serie de recomendaciones entro de la entidad que contribuyan con el buen desarrollo y privacidad de la información.

- Solicitud de aceptación de la política de seguridad
- Cláusulas contractuales con los empleados en relación con la custodia conservación y buenas prácticas en la utilización de la seguridad.
- Establecimiento de una política de uso de los medios tecnológicos, que determine alcance y uso de los diferentes dispositivos que se utilicen en la organización.

5.3.11 Medidas de prevención organizativa: Estructurar protocolos mediante el SGSI donde se documenten los incidentes presentados durante el trascurso de la semana, mes o año, documentar estos incidentes y generar planes de acción y prevención que permitan tomar medidas temprano y así evitar la fuga de **información.**

Así las cosas, se destaca la importancia de la identificación y la elaboración de estrategias para mitigar los riesgos, lo que nos permite comprender mejor el concepto de riesgo y sus características según la norma ISO 27001. Esta identificación incluye diversos tipos de riesgos, como el riesgo calculado, el riesgo residual, el umbral de riesgo y el riesgo intrínseco. Estos aspectos nos facilitan la detección temprana y la implementación de acciones preventivas ante posibles riesgos que puedan surgir.

Además, es fundamental para las organizaciones definir criterios claros para elaborar matrices de riesgo que orienten las acciones a largo y mediano plazo. Asimismo, resulta crucial determinar el nivel de riesgo al que se enfrenta la organización, lo que proporciona una base sólida para la toma de decisiones y la retribución de recursos destinados a la gestión de riesgos.

6. CONCLUSIONES

Dentro del riguroso proceso de investigación frente a los ataques informáticos se logra concluir que los sistemas de información siempre estarán sujetos a los ataques cibernéticos y que por más robustas que pueda ser la implementación de las infraestructuras tecnologías, siempre van a estar sujetas algún tipo de vulnerabilidad, aún más cuando no se toman las medidas necesarias para que permitan la identificación de brechas de seguridad en los sistemas.

Los usuarios internos de las organizaciones, siempre se van a considerarse el punto vulnerable para realizar cualquier ataque, si bien se relacionó en el apartado de la parte superior de este escrito, hoy en día es inevitable el uso de correo electrónico y se pudo evidenciar que es uno de los vectores principales por donde los ciberdelincuentes realizan los ataques informáticos.

La actualización constante de los sistemas operativos y demás plataformas que lo requieran es de suma importancia, ya que a través de estas se descargan parches de seguridad que corrigen las brechas de vulnerabilidad dentro de los sistemas de información, evitando que los ciberdelincuentes pueden sacar ventaja de las condiciones de la red.

La mayoría de los ataques informáticos que se ejecutan en los sistemas de información, son provenientes de los usuarios finales que, por desconocimiento de la funcionalidad de los virus, permiten que mediante los virus enviados por correos electrónicos se presente el robo de datos personales.

La mala práctica en la implementación de los sistemas de información y la no ejecución de auditorías de control permiten que se presenten brechas de vulnerabilidad y amenazas a los sistemas informáticos, por eso es importante realizar uso de las guías de implementación como lo son las normas técnicas ISO 27001 y normas subsiguientes de la familia de las ISO.

Es importante resaltar que, dentro de la implementación o distribución de la infraestructura tecnológica, se cuente con una zona DMZ o comúnmente denominada zona de desmilitarización, con la finalidad de que los sistemas de información no estén expuestos a los diferentes ataques cibernéticos y dentro de la organización se crea manual de políticas de usuario y designación de roles, para prevenir mal manejo de las plataformas informáticas.

7. RECOMENDACIONES

Teniendo en cuenta los resultados obtenidos frente a la investigación realizada se generan una seria de recomendación que mediante estas contribuyan para mitigar los riesgos de ataques informáticos que se pueden llegar a presentar dentro de las organizaciones.

Se debe de manera permanente mantener medidas de acción y prevención en lo que refiere a los sistemas de información de la organización, con dichas dentro de estas medidas es fundamental la revisión periódica de actualizaciones y sistemas de detección de vulnerabilidades, como lo son el firewall, Check Point y parches de seguridad de los sistemas operativos de los equipos de cómputo y servidores donde repose información, implementación de antivirus licenciado, entre otros.

Capacitación al personal que tenga injerencia directa con la operabilidad de los sistemas, como lo son servidores, bases de datos, copias de seguridad y acceso al Data center.

Recurrir a la adquisición de nuevas tecnologías, preferiblemente que sea mediante servicios de aplicación, que se maneja a través de la nube, ya que actualmente estos son sistemas hiperconvergentes y permiten a las organizaciones llevar un mejor control sobre los sistemas y adicionalmente optimizar recursos en infraestructuras.

Crear políticas de seguridad que permitan llevar un mejor control sobre los activos de la organización, a través esta policita permitirá que las personas se apropien aun más de su responsabilidad en cuanto el buen uso de los sistemas, la toma de prevención frente a unidades extraíbles, ya que a través de estas es que también se puede perpetuar un ataque informático.

Realizar auditorías mediante pruebas de intrusión y penetración que permitan evidenciar cual es el estado actual de la red, ya que mediante estas técnicas se pueden tomar acciones tempranas para evitar ataques perpetuados por los ciberdelincuentes.

Establecer que información debe ser protegida en las universidades, la cual se consideren o puedan ser motivo de crisis a la hora de un ataque y que datos deberían protegerse entre los niveles más altos de seguridad con la finalidad de que no trascienda y se encuentren expuestos a la competencia o al público en general, es decir clasificarlos de tal manera que no todos se han públicos.

Identificar que vulnerabilidades de la seguridad informática son las más recurrentes a nivel mundial y de este modo tomar rápidas acciones frente a este tipo de ataques.

BIBLIOGRAFÍA

ALEMAN NOVOA, Helena. Metodologías Para el Análisis de Riesgos en los SGSI [En línea] **2019** Journal specializingin engineering, 9, 1 Fundación Universitaria Juan de Castellanos, Facultad de Ingeniería, T unja, Boyacá, Disponible en https://hemeroteca.unad.edu.co/index.php/publicaciones-e investigacion/article/view/1435/1874

ANCHUNDIA-BETANCOURT, Carlos E. Ciberseguridad en los sistemas de información de las universidades [En línea] **2017** Vol. 3, No 3 https://dominiodelasciencias.com/ojs/index.php/es/article/view/636

ARÉVALO CORDOVILLA, Felipe Emiliano; ORDOÑEZ-SIGCHO, Ingrid Beatriz; PEÑAHERRERA LARENAS; Milton Fabiá; SUÁREZ MATAMOROS; Verónica Janeth. Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información [En línea] **2020** Dialnet-ImportanciaDeLaSeguridadDeLosSistemasDeInformacion-7425694.pdf

BACA URBINA, Gabriel. Introducción a la seguridad informática [En línea].**2016** Editorial Grupo Editorial Patria eLibro E- ISBN 9786077444718 p. 361 Disponible https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/40458?page=46

BUXARRAIS ESTRADA, María Rosa; OVIDE, Evaristo. El impacto de las nuevas tecnologías en la educación en valores del siglo XXI [En línea] no.37 Tlaquepaque julio. **2011** ISSN 2007-7033versión impresa ISSN 1665-109X Disponible http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-109X2011000200002

CAÑÓN PARADA, Lady Johana. Ataques informáticos, ethical hacking y conciencia de seguridad informática en niños [En línea] Universidad Piloto de Colombia. **2012**. Disponible en http://polux.unipiloto.edu.co:8080/00002427.pdf

CORDOBA RODRIGUEZ, Norma Edith. Evolución de riesgos, amenazas y vulnerabilidades. Plan de seguridad informática para la entidad financiera [En línea] **2017** p.2-20 Disponible en http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap5.PDF

FIGUEROA SUÁREZ, Juan A; RODRÍGUEZ-ANDRADE, Richard F; BONE OBANDO; Cristóbal C; SALTOS GÓMEZ; Jazmín A La seguridad informática y la seguridad de la información [En línea] **2017** pp. 145-155 ISSN: 2550 - 682X Disponible file:///C:/Users/ESOLORZANOR/Downloads/420-1655-2-PB.pdf

GIL VERA, Víctor Daniel; GIL VERA, Juan Carlos. Seguridad informática organizacional: un modelo de simulación basado en dinámica de Sistemas [En línea] **2017** vol. 22, núm. 2, junio, , pp. 193-197 ISSN: 0122-1701 Disponible en https://www.redalyc.org/pdf/849/84953103011.pdf

GOMÉZ VIEITES, Álvaro Gestión de incidentes de seguridad Informática [En línea] **2016** Editorial RA – MA Editorial eLibro E- ISBN 9788499643311 p. 124 Disponible en https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62467?page=13

HERNANDEZ, Ronald. Impacto de las TIC en la educación: Retos y Perspectivas, [En línea] V5N1.149 Universidad San Ignacio de Loyola, Lima, Perú **2017**. ISSN 2310-4635 Disponible en https://revistas.usil.edu.pe/index.php/pyr/article/view/149

ILLA GAY, Ramon. Seguridad en servidores empresariales. Control y análisis de configuraciones de seguridad y de vulnerabilidades [En línea] Universitat Oberta de

Catalunya **2019** Disponible en http://openaccess.uoc.edu/webapps/o2/handle/10609/95326

NUÑEZ CHOCCLLO, Yeny Actitud hacia las tecnologías de la información y la comunicación y la gestión pedagógica en los profesores de la institución educativa de Aplicación Fortunato Luciano Herrera [En línea] **2021** 253T20210156 Disponible en http://repositorio.unsaac.edu.pe/handle/20.500.12918/5842

OSPINA DÍAZ, Milton Ricardo; SANABRIA RANGEL, Pedro Emilio. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia [En línea] **2020** Rev. Crim. vol.62 no.2 Bogotá ISSN 1794-3108. Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199.

PALACIO PUERTA, Marcela; CABRERA PEÑA, Karen Isabel. La gobernanza de internet como plataforma para impulsar políticas en la educación con TIC. El caso de Colombia [En línea] Revista Opera, ISSN-e 1657-8651, Nº. 21**, 2017**, págs. 5-23 Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6187514

PARRA MOSQUERA, Carlos Andrés. TIC, conocimiento, educación y competencias tecnológicas en la formación [En línea] ISSN 0121-7550, ISSN-e 2539-4762, N.º. 36, **2012**, págs. 145-159 Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=3964185

PEÑA RODRÍGUEZ, Faustino; OTÁLORA PORRAS, Nelson. Educación y tecnología: problemas y relaciones Pedagogía y Saberes No. 48 Universidad Pedagógica Nacional Facultad de Educación. **2018**, pp. 59-70 Disponible http://www.scielo.org.co/pdf/pys/n48/0121-2494-pys-48-00059.pdf

RUBINOS CARVAJAL, Alejandro Manuel; NUEVO LEÓN, Heidy Alina. Seguridad en bases de datos Revista Cubana de Ciencias Informáticas [En línea] **2011** (RCCI) ISSN: 1994-1536 Disponible https://www.redalyc.org/pdf/3783/378343671005.pdf

SANDOVAL CASTELLANOS, Edgar Jair. Ingeniería social: corrompiendo la mente humana. Seguridad cultura de prevención para TI [En línea]**2019** Disponible en https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

SAN MARTIN GONZALEZ, Enrique. Salvaguarda de los Datos: Administración de bases de datos [En línea] **2018**. Editorial IC Editorial eLibro E- ISBN: 9788416433315 Disponible en https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44140?page=135

SIERRA LLORENTE, jose; BUENO GUIRALDO, Isidro; MONROY TORO Stella. Análisis del uso de las tecnologías TIC por parte de los docentes de las Instituciones educativas de la ciudad de Riohacha, [En línea] **2016** Universidad del Zulia pp. 50 – 64. ISSN: 1315-8856 Disponible en https://www.redalyc.org/pdf/737/73749821005.pdf

SUNKEL, Guillermo; TRUCCO, Daniela La integración de las tecnologías digitales en las escuelas de América Latina y el Caribe: una mirada multidimensional [En línea] **2013** LC/L.3601 https://repositorio.cepal.org/handle/11362/21681

MARQUEZ DÍAS, Jairo Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas Bioética y Derecho no.46 Barcelona ISSN 1886-5887 [En línea] octubre del **2019** Disponible en https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006

MARTINEZ LOZANO, Jeferson Eleazar; ATENCIO ORTIZ, Pedro Sandino. Creación de un ataque DDOS utilizando HTTP-GET FLOOD a partir de la metodología CYBER KILL CHAIN [En línea] vol.16 no.1 Bucaramanga Jan/June **2019** Disponible http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-17982019000100041

NAVA MUÑOZ, Rixio Socialización del conocimiento académico con el uso de tecnologías de información y comunicación [En línea] **2007**, vol.4, n.3, pp.41-56. ISSN 1690-7515 Disponible en http://ve.scielo.org/scielo.php?pid=S1690-75152007000300004&script=sci_abstract