UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador

AUTOR:

Vélez Armijo, Efraín Alexander

Trabajo de Titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

Ing. Vallejo Samaniego, Luis Vicente, M.Sc.

Guayaquil, Ecuador

7 de marzo del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

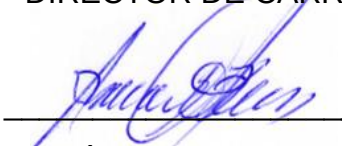
CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Vélez Armijo Efraín Alexander**, como requerimiento para la obtención del título de **Ingeniero en Telecomunicaciones**.

TUTOR

Ing. Vallejo Samaniego, Luis Vicente, M.Sc.

DIRECTOR DE CARRERA



Ing. Heras Sánchez, Miguel Armando, M.Sc.

Guayaquil, a los 7 días del mes de marzo del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Vélez Armijo, Efraín Alexander**

DECLARÓ QUE:

El Trabajo de Titulación, **"Análisis de la ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador"** previo a la obtención del título de Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 7 días del mes de marzo del año 2022

EL AUTOR

f._____

Vélez Armijo, Efraín Alexander

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Vélez Armijo, Efraín Alexander**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, **"Análisis de la ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 7 días del mes de marzo del año 2022

EL AUTOR

f._____

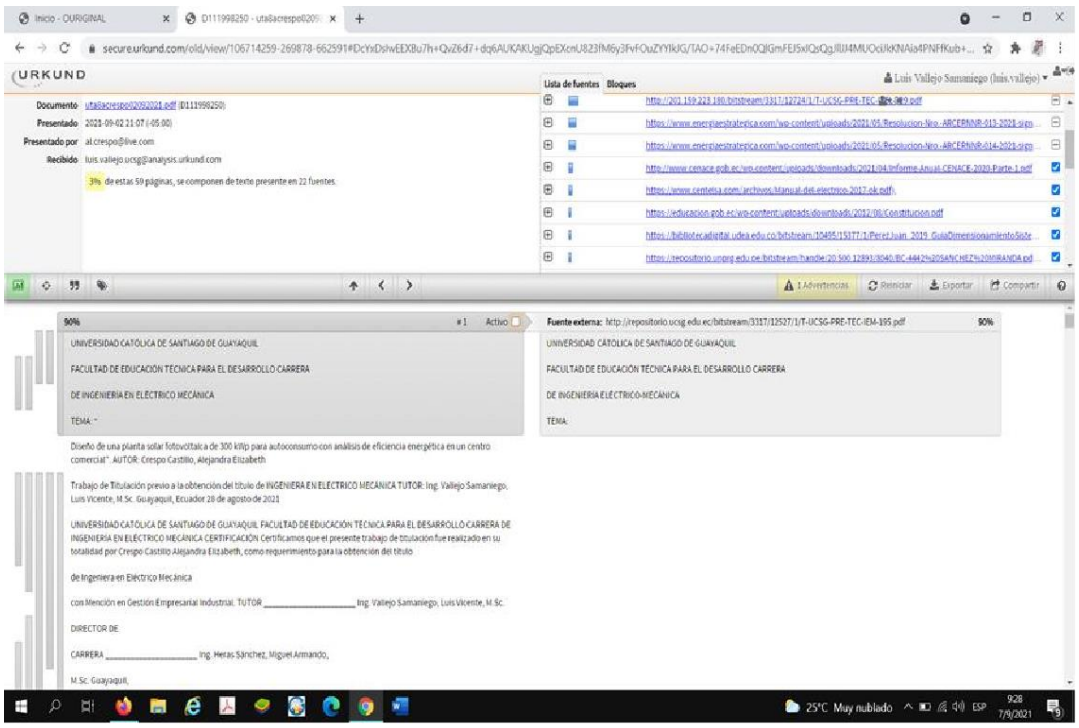
Vélez Armijo, Efraín Alexander

REPORTE DE URKUND

Datos

Documento:	Trabajo de Titulación
Título del Trabajo:	"**ANÁLISIS DE CIBERSEGURIDAD EN REDES DE TELECOMUNICACIONES Y SISTEMAS INFORMÁTICOS PARA EDUCACIÓN 4.0 COMO RESPUESTA A LA INDUSTRIA 4.0 EN EL ECUADOR"**
Carrera:	Ingeniería en Telecomunicaciones
Estudiante:	EFRAÍN ALEXANDER VÉLEZ ARMIJO
Semestre:	B-2021
Fecha:	FEB/2022

Reporte final URKUND



Conclusión: La revisión de coincidencias del resultado de la revisión, considera la desactivación de la información de texto de los formatos de presentación de trabajos de titulación en la UCSG. Se adjunta documento de Reporte URKUND de la Revisión Final en medio digital. Porcentaje de coincidencia final del 2%.

Firmado electrónicamente por:
LUIS VICENTE
VALLEJO SAMANIEGO

Ing. Luis Vallejo Samaniego, M.Sc.
DOCENTE-TUTOR

AGRADECIMIENTO

Expreso mi total gratitud a Dios Jehová por guiarme por el buen camino, darme fuerzas para seguir adelante y por siempre llenar mi vida y la de mi familia de bendiciones, sin su ayuda no podría haber alcanzado este logro en mi vida.

Mi profundo agradecimiento a mis pilares fundamentales en la vida, mi padre Efraín Vélez y mi madre Tanya Armijo, 2 piezas indispensables que siempre me mostraron amor, dedicación, paciencia, y que me acompañaron en cada paso que di en mi desarrollo personal y profesional. De la misma forma a toda mi familia que siempre estuvo pendiente en cada etapa de mi progreso.

A todos los docentes de la Prestigiosa Universidad Católica de Santiago de Guayaquil, que me guiaron en mi camino a convertirme en un profesional. Gracias a todos por su dedicación, paciencia, amistad y apoyo incondicional.

Especialmente a mi tutor encargado Ing. Luis Vallejo Samaniego, M. Sc. Y también al director de carrera Ing. Miguel Heras Sánchez, M.Sc. por la ayuda brindada, por la disponibilidad en cualquier horario y por compartir conmigo la sabiduría y conocimiento para poder completar a cabalidad este trabajo de titulación.

Vélez Armijo, Efraín Alexander

DEDICATORIA

Dedico con todo mi amor y cariño este trabajo de titulación a mi Dios Jehová quien siempre me ha guiado por buen camino y me ha dado la fortaleza necesaria para llegar hasta donde estoy y poder seguir adelante.

A mis padres que siempre creyeron en mí y en mis capacidades, por estar en los momentos más importantes de mi vida, quienes con su apoyo y palabras de aliento me hacían perseverar y seguir adelante con mis ideales.

A mi abuelita que siempre estuvo pendiente de cada paso que daba, por su preocupación, consejos y sabiduría que han sido de gran ayuda en mi vida y en mi crecimiento como persona.

Vélez Armijo, Efraín Alexander

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESÚS

DECANO

f. _____

M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DEL ÁREA

f. _____

M. Sc. HERAS SÁNCHEZ, MIGUEL ARMANDO

OPONENTE

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La ciberseguridad es uno de los aspectos más importantes tanto en los países desarrollados como en los que están en vías de desarrollo, ayuda a defender los datos de distintos ataques maliciosos. Estos ciberataques son uno de los mayores retos a nivel nacional y requieren de un análisis que examine los aspectos que han convertido a las acciones de estos en uno de los desafíos más grandes para las instituciones educativas tanto públicas como privadas del Ecuador. Para solucionar estas ciberamenzas, es preciso implementar diferentes políticas de ciberseguridad en los puntos clave donde se ejecutan los procesos de recepción, envío y almacenamiento de información de las instituciones que lo necesiten con el fin de proteger la confidencialidad de los datos. Los ciberataques no sólo se originan interceptando el tránsito de datos entre el emisor y el receptor, sino también ingresando desde servidores y estaciones de trabajo, donde los operadores facilitan el acceso y permiten a los atacantes ingresar a la red.

Palabras claves: CIBERSEGURIDAD, CIBERATAQUE, CIBERAMENAZA, E-LEARNING, MALWARE, RANSOMWARE, PHISHING.

ABSTRACT

Cybersecurity is one of the most important aspects in both developed and developing countries, helping to defend data from various malicious attacks. These cyber-attacks are one of the biggest challenges at the national level and require an analysis that examines the aspects that have turned their actions into one of the biggest challenges for both public and private educational institutions in Ecuador. To solve these cyber threats, it is necessary to implement different cybersecurity policies in the key points where the processes of receiving, sending, and storing information of the institutions that need it to protect the confidentiality of the data. Cyber-attacks are not only originated by intercepting the transit of data between the sender and the receiver, but also by entering from servers and workstations, where operators facilitate access and allow attackers to enter the network.

Keywords: CYBERSECURITY, CYBERATTACK, CYBERTHREAT, E-LEARNING, MALWARE, RANSOMWARE, PHISHING.

CAPÍTULO 1

INTRODUCCIÓN

1.1. Preámbulo

A lo largo de la historia, la forma de educar ha ido cambiando debido a los avances tecnológicos en el sector. En la actualidad, con la aparición del internet, la mayoría de los jóvenes conviven en entornos tecnológicos, en donde las tecnologías de la información y comunicación (TIC'S) forman parte de su diario vivir, lo cual incluye el uso de herramientas educacionales que los ayudan en su formación.

Sin embargo, la proliferación de estas nuevas tecnologías inteligentes trae consigo un aumento en los problemas de ciberseguridad. Un delincuente no debe tener necesariamente un recurso computacional demasiado grande para efectuar estos ataques y vulnerar los sistemas informáticos.

Por lo que se darán recomendaciones para reducir e incluso prevenir estos tipos de riesgos en las redes de telecomunicaciones y los sistemas informáticos en la educación 4.0.

La inseguridad virtual es algo que nunca va a dejar de existir, es un tema de suma preocupación y da lugar a la obligación de contar con herramientas o procesos para identificar a tiempo y de forma correcta los posibles riesgos que puedan surgir, y de esta manera proteger la información de las personas involucradas.

Con este análisis se logrará identificar y prevenir las distintas vulnerabilidades y posibles peligros de ciberseguridad que existan en el uso de las redes de telecomunicaciones y sistemas informáticos en la educación 4.0, y de esta forma brindar soluciones oportunas en el tiempo y lugar adecuado.

1.2. Antecedentes

Las instituciones centradas en la educación persiguen la adaptabilidad para brindar diversos servicios a los estudiantes, razón por la que su infraestructura y el manejo de la información debe conservar una ciberseguridad consistente, para que, a pesar de sufrir cualquier ataque cibernético, sigan cumpliendo normalmente con sus actividades.

Por ello, constantemente se están realizando estudios en los que se analizan los ataques que sufren, la forma de atacar y el impacto en las instituciones afectadas, con el fin de establecer políticas de seguridad más confiables, para evitar corrupción y pérdidas de información de valor para la institución.

1.3. Definición del Problema

Las redes de telecomunicaciones son usadas por la mayoría de los estudiantes hoy en día, lo que incrementa mucho más la preocupación de los ciberataques que puedan ocurrir.

Además, algunas Universidades se han visto afectadas por sufrir ataques en la seguridad de sus sistemas. Los ciberataques se han convertido en una amenaza real a nivel nacional no sólo por las pérdidas financieras sino también por las consecuencias que podrían generar al exponer información confidencial a la vista del público.

1.4. Justificación del Problema

Con esta investigación se logrará formar un plan de procedimiento para la gestión de la ciberseguridad en las redes de telecomunicaciones y en los sistemas informáticos usados en las instituciones académicas, para de esta manera proporcionar un plan de contingencia informática mediante políticas de ciberseguridad y reducir los riesgos o ataques cibernéticos a las instituciones.

1.5. Objetivos del Problema de Investigación.

1.5.1. Objetivo General

Analizar el impacto de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador.

1.5.2. Objetivos Específicos

- Identificar y determinar las diferentes vulnerabilidades que utilizaron los ciberdelincuentes en los sistemas informáticos educativos durante la pandemia del Covid-19.
- Establecer los distintos métodos y prácticas de ciberseguridad para tomar las medidas adecuadas de protección en las redes y sistemas informáticos enfocados a la educación.
- Diseñar planes para la futura implementación de medidas y acciones para protección y prevención de ataques cibernéticos a instituciones educativas.

1.6. Hipótesis

La hipótesis es que el uso de nuevas herramientas tecnológicas incrementa la probabilidad que las diferentes instituciones educativas tanto públicas como privadas, sean más propensas a los ciberataques presentados a corto, medio y largo plazo.

1.7. Metodología de Investigación

El tipo de investigación a utilizar en el presente trabajo de titulación es descriptivo y documental. Descriptivo porque permitirá que se describa al área de las telecomunicaciones con la seguridad informática y su influencia en las aplicaciones educativas.

Documental porque se recopilará datos de diferentes fuentes bibliográficas y se realizará el análisis respectivo para determinar los métodos más apropiados de protección y prevención.

En base al tipo de investigación a utilizarse, la metodología a emplear permitirá puntualizar al área de las telecomunicaciones con la ciberseguridad, su influencia en la educación y documentar los datos recopilados de las distintas fuentes bibliográficas.

Se realizará un análisis de la realidad actual donde las aplicaciones educativas se encuentran expuestos a un riesgo en la seguridad de sus sistemas. Se elegirá las técnicas apropiadas de recolección de los datos, utilizando diversas fuentes bibliográficas, documentos, artículos científicos.

Además, se basará en el método deductivo-cualitativo porque con el análisis respectivo se logrará encontrar los mecanismos adecuados para prevenir y proteger las aplicaciones educativas contra los ataques cibernéticos.

PARTE I MARCO TEÓRICO

CAPÍTULO 2

FUNDAMENTACIÓN TEÓRICA

2.1. Fundamentos de Revolución 4.0

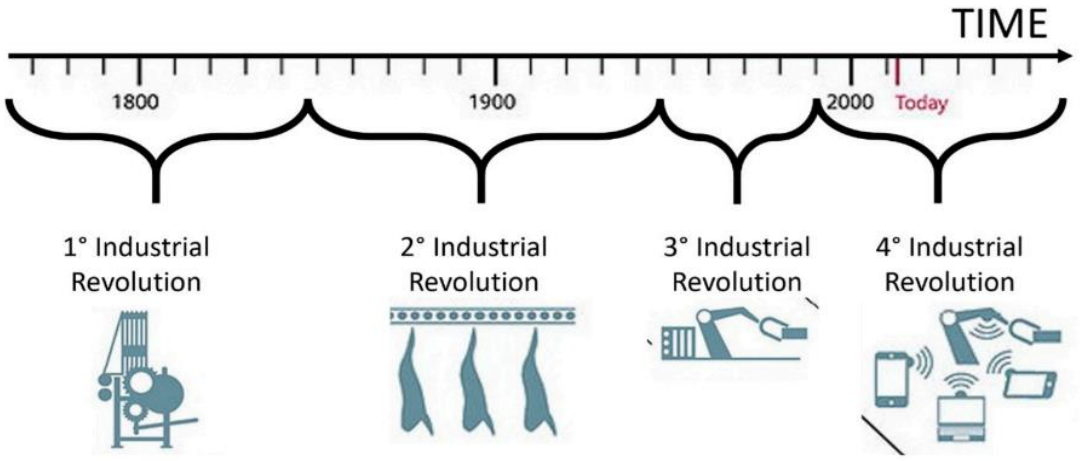
La tecnología digital ofrece ventajas innovadoras para la empresa económica. En la industria, la primera revolución comenzó alrededor de 1780 con la introducción de plantas de producción mecánicas impulsadas por agua líquida o vapor como se ve en la Figura 2.1.

La segunda revolución industrial nació 30 años después, cuando se construyó la primera cadena de montaje mecánica alimentada por electricidad.

La tercera revolución industrial comenzó a finales de los años 60, cuando se construyó el primer controlador lógico programable (PLC). A partir de ese momento, fue posible automatizar la producción utilizando la electrónica y la tecnología de la información (TI) (Zambon et al., 2019).

Figura 2. 1

Evolución de la Industria 1.0 a la 4.0.



Nota. Adaptado de *Revolution 4.0: Industry vs. Agriculture in a Future Development for SMEs,* de Zambon et al., 2019, Documento de investigación.

La cuarta revolución industrial comenzó en 2011 en Alemania con un proyecto del gobierno alemán para promover una profunda informatización e innovación conceptual de la producción. En estos pocos años, las empresas alemanas han transformado la teoría en aplicaciones de éxito.

La cuarta revolución industrial es la actual y hace uso de la cibernética. La eliminación de la separación entre el mundo físico y el virtual es un patrón esencial de la Industria 4.0.

Partiendo de estas premisas, la estructura de objetos virtuales está vinculada al concepto de Internet de las cosas (IoT). En la industria, como también en la educación, el IoT combina los conceptos de "Internet" y "cosa", lo que puede explicarse a través de algunas características clave del IoT, que son: la interconectividad, los servicios relacionados con los objetos, la heterogeneidad, los cambios dinámicos, y la alta escalabilidad como se muestra en la tabla 2.1.

Por lo tanto, la IoT puede definirse semánticamente como una red mundial (World Wide Network) de objetos con direcciones únicas interconectados a través de protocolos de comunicación estándar. En consecuencia, Internet sirve de infraestructura de almacenamiento y comunicación que contiene una de las cosas que conecta la información relevante con los objetos físicos.

Los objetos virtuales actúan como centros de información de objetos, que combinan y actualizan continuamente los datos procedentes de una amplia gama de fuentes. Los objetos virtuales pueden utilizarse para coordinar y controlar procesos empresariales a distancia a través de Internet.

La revolución 4.0 ofrece un nuevo contexto para estudiar la difusión de las fronteras económicas, lo que permitirá a los futuros investigadores ofrecer resultados generalizables sobre cómo las empresas transfieren o amplían sus modelos de negocio de la industria manufacturera a las TIC (Tecnologías de la Información y la Comunicación), y viceversa.

Tabla 2. 1

Características principales del IoT.

Interconectividad	Todo puede estar interconectado con la información global y las infraestructuras de la información y la comunicación.
Servicios relacionados con los objetos	La IoT puede proporcionar servicios relacionados con los objetos, dentro de los límites definidos por éstos como la protección de la privacidad y la coherencia semántica entre los objetos físicos y objetos virtuales asociados.
Heterogeneidad	Los dispositivos de la IoT son heterogéneos, ya que se basan en diferentes plataformas de hardware y redes. Pueden interactuar con otros dispositivos o plataformas de servicios a través de diferentes redes.
Cambios dinámicos	El estado del dispositivo puede cambiar dinámicamente, como la conexión y/o desconexión, así como el contexto en el que operan los dispositivos, incluyendo la ubicación, la velocidad, la cantidad de producto, etc. El número de dispositivos también puede cambiar dinámicamente.
Alta escalabilidad	El número de dispositivos que hay que gestionar y que se comunican entre sí puede ser muy grande.

Nota. Adaptado de *Revolution 4.0: Industry vs. Agriculture in a Future Development for SMEs,* de Zambon et al., 2019, Documento de investigación.

2.2. Fundamentos de Tecnología 4.0

Hace unos años, el elevado coste de la utilización de las tecnologías actuales, como los sensores sofisticados, las herramientas de conectividad, el almacenamiento de datos y la alta potencia informática, hacía que se evitara la implantación de dichas tecnologías. Hoy en día, estas tecnologías se han abaratado y por ello se están utilizando ampliamente.

Además, las empresas están estableciendo cada vez más su columna vertebral de TI (Tecnología de la Información) para un motor de calidad integrado en la producción que conecta, supervisa y analiza todos los datos relevantes para el operador, la máquina, el producto y las herramientas en tiempo real en términos de control de procesos.

Las tecnologías de calidad 4.0 se dividen en cuatro categorías: Big-Data, conectividad, colaboración y presentación de datos (Sader et al., 2021).

2.2.1. Big-data

Los nuevos sistemas de producción han aumentado exponencialmente la generación de datos en la cadena de valor digital. El uso de los datos generados de forma adecuada puede suponer una mejora en las prácticas de gestión de la calidad.

Por lo tanto, la regulación de la calidad basada en datos es vital para maximizar las recompensas de los métodos de análisis y corrección de errores. La recopilación de datos en tiempo real se hizo posible gracias a Big-Data.

Aquí llegan las nuevas herramientas de ciencia de datos como la Inteligencia Artificial, el Aprendizaje Automático y el Aprendizaje Profundo. El uso de estas herramientas permitirá a los expertos en calidad descubrir factores relacionados no vistos que afectan a la calidad (Sader et al., 2021).

2.2.2. Conectividad

Conecta todas las partes de la cadena de valor de la producción, incluidas las personas, los productos, los dispositivos y los procesos con otras soluciones de gestión empresarial, como el ERP, y el sistema de gestión de la calidad. Las personas pueden utilizar dispositivos inteligentes para transmitir y recibir información que pueda servir de apoyo a sus funciones en sus respectivas ubicaciones. Los productos pueden guardar los datos generados durante la producción. Las tecnologías pueden almacenar datos sobre los procesos o máquinas por los que ha pasado el producto.

La introducción de IPv6 y la mejora de la infraestructura de red amplían el espacio para conectar más dispositivos en línea, y los productos pueden proporcionar información sobre su rendimiento en el campo para mejorarlos.

Dicha información incluye defectos, entorno de funcionamiento, circunstancias de los fallos e incluso comentarios de los clientes. Además, puede compararse con otros datos de los dispositivos, los procesos y los sistemas ERP, lo que lleva a una explicación de los defectos (Sader et al., 2021).

2.2.3. Colaboración

Tecnologías como las plataformas de medios sociales pueden contribuir al desarrollo de la calidad mediante la creación de canales de colaboración con los clientes, entre los empleados y entre las empresas. Otra tecnología es el blockchain, que ahora utilizan muchas empresas industriales para rastrear el historial de los productos, especialmente cuando las cadenas de suministro son profundas y versátiles.

La colaboración en el contexto de la calidad 4.0 es una de múltiples vías en la que los clientes participan más en las actividades de calidad a través de las plataformas de los medios sociales.

Los clientes pueden contribuir al avance de los productos durante las etapas de desarrollo y producción. La retroalimentación es más avanzada utilizando tecnologías como el aprendizaje profundo, donde se recogen contenidos como comentarios y reacciones, se analizan y se dirigen automáticamente a la parte implicada pertinente (Sader et al., 2021).

2.2.4. Presentación de datos

No basta con analizar los datos y mostrar los resultados, sino que también es importante cómo se presentarán los resultados a las personas pertinentes. Los dispositivos inteligentes están ahora extendidos por todas partes, incluidos los móviles tabletas y pantallas inteligentes. Las herramientas de comunicación tradicionales, como el teléfono, el fax y los ordenadores se sustituyen ahora por un dispositivo de visión única llamado smartphone.

La tecnología de realidad aumentada se utiliza ahora para enriquecer las transmisiones de vídeo normales con información objetada sobre la misma. Las aplicaciones móviles están proporcionando una mejor experiencia de usuario y un mayor nivel de participación, colaboración y eficiencia.

Además, los sistemas de apoyo favorecen de forma proactiva y eficiente a los trabajadores en su trabajo, cambiando el papel de los empleados de operadores de máquinas a tomadores de decisiones. Se pueden ubicar más dispositivos y pantallas inteligentes en el taller que muestren información enriquecida a los operarios y a los superiores, mostrando ricas animaciones, alertas de colores e instrucciones (Sader et al., 2021).

2.3. Definición de calidad 4.0

La Calidad 4.0 es la mezcla de prácticas y técnicas tradicionales de gestión de la calidad con nuevas tecnologías como el aprendizaje automático, las tecnologías en la nube, Big-Data, dispositivos de conectividad, Internet de las Cosas e Inteligencia Artificial.

Dicha integración dio lugar a un entorno colaborativo avanzado en el que las actividades de gestión están impulsadas por una mayor conectividad entre la cadena de valor, desde el proveedor hasta el cliente final (Sader et al., 2021).

La diferencia entre la calidad 4.0 y la calidad tradicional es el cambio de la medición manual, el registro de los resultados en los gráficos de calidad, y reajustar el proceso de fabricación, a la actividad totalmente automatizada, donde los sensores miden, las aplicaciones de software analizan y controlan el proceso para el autoajuste. En la figura 2.2 se muestra la definición sugerida de la Industria 4.0 como incubadora de apoyo para mejorar y potenciar las prácticas de gestión de la calidad. El impacto se ilustra con la flecha descendente en la parte derecha de la figura 2.2. Por el contrario, la flecha ascendente del otro lado de la figura 2.2 subraya que el ámbito de la gestión de la calidad se desarrolla por etapas.

Además, la Calidad 4.0 proporcionó un alcance más amplio a la gestión de la calidad mediante la integración del poder del conocimiento, la conectividad y las herramientas de Big-Data para transformar las actividades de gestión de la calidad de reactivas o proactivas a predictivas.

Existen cinco aplicaciones para la Calidad 4.0: en la fabricación, la I+D, el servicio y la posventa, el aprovisionamiento, y la logística y las ventas.

Figura 2. 2

La industria 4.0 en las prácticas de gestión de la calidad.

Nota. Adaptado de *A review of quality 4.0: definitions, features, technologies, applications, and challenges,* de Sader et al., 2021, Artículo de revista académica.

2.4. Definición de Industria 4.0

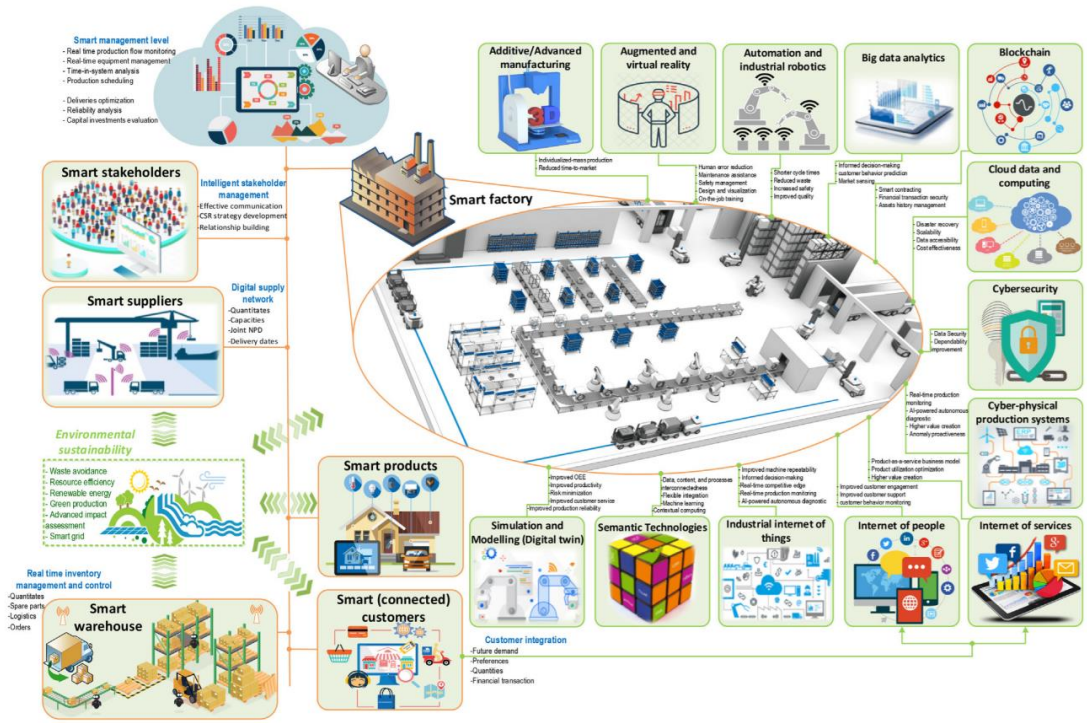
La Industria 4.0 es una nueva esfera de la industria, que apareció como resultado de la aparición y distribución de nuevas tecnologías que permiten desarrollar procesos de producción totalmente automatizados. La Industria 4.0 crea productos industriales tradicionales y nuevos productos industriales, que no pueden ser fabricados en otras esferas de la economía del sector real. Así, el empresario optimiza los procesos empresariales utilizando las posibilidades que ofrece Industria 4.0, el empleado domina las nuevas competencias que son necesarias, y el consumidor domina nuevos productos industriales.

Mientras que en la actualidad la Industria 4.0 es un nuevo vector de desarrollo de la industria, en el futuro la formación de la Industria 4.0 puede conducir a la modernización progresiva de otras esferas o ámbitos de la industria. Esto significa que la Industria 4.0, tratada como una esfera de la industria, tiene un potencial para cambiar el modo tecnológico existente (Popkova et al., 2019).

La Figura 2.3 describe el alcance de la Industria 4.0 y la funcionalidad de sus componentes. Como se explica claramente en la Figura 2.3, la transformación digital de la Industria 4.0 implica la digitalización e integración de toda la cadena de valor del ciclo de vida de los productos. La red de suministro digital (DSN) ofrece una red integrada dentro de la cual todas las funciones de valor, como proveedores inteligentes, clientes conectados, fábricas inteligentes, maquinaria de producción, productos y materiales inteligentes, interactúan y se comunican entre sí en tiempo real y a escala global (Ghobakhloo, 2020).

Figura 2. 3

El diseño arquitectónico de la Industria 4.0.



Nota. Adaptado de *Industry 4.0, digitization, and opportunities for sustainability*, de Ghobakhloo, 2020, Artículo de revista académica.

2.5. Definición de Educación 4.0.

En general, la Educación 4.0 es una entidad de creencias que fomenta el pensamiento inteligente en la educación. La Educación 4.0 promueve la enseñanza de forma diferente, principalmente mediante el consumo de herramientas y recursos basados en la tecnología. Esto significa que los estudiantes no aprenderán usando libros de texto físicos, bolígrafos y profesores en las aulas tradicionales. En su lugar, la Educación 4.0 permite a los estudiantes acceder remotamente a Internet e inscribirse en cursos a través de una variedad de programas abiertos en línea, videollamadas o llamadas de voz. La educación 4.0 fue reconocida como una respuesta a la Industria 4.0, aumentando considerablemente el uso de las tecnologías de Internet y las herramientas de comunicación cruzada.

La Educación 4.0 responde a las necesidades de la sociedad en la "era de la innovación". Esta gestión del aprendizaje debe ayudar a desarrollar la capacidad del estudiante para aplicar la nueva tecnología, lo que los ayudará a desarrollarse de acuerdo con los cambios en la sociedad. Para poder vivir en la sociedad y dar lo mejor de su capacidad (Puncreobutr, 2016).

La Educación 4.0 es un método de aprendizaje más realista y práctico, de hecho, utiliza sistemas inteligentes de gestión escolar, software de gestión del aprendizaje, herramientas de comunicación y otras herramientas de enseñanza y aprendizaje.

El aprendizaje personalizado con la Educación 4.0 favorece la comprensión y permite a los estudiantes llegar a convertirse en profesionales realmente memorables e interesados en lo que aprenden.

Para los profesores La Educación 4.0 es una revolución inteligente, virtual y digital en beneficio de muchas partes interesadas. Es beneficiosa para los educadores de los centros educativos porque pueden reducir la carga administrativa mediante la automatización de muchos procesos mientras se modernizan procesos específicos y métodos de enseñanza (Sharma, 2019).

La Educación 4.0 también se aplica a los administradores y las personas que no se dedican a la enseñanza, como los directivos. Esto se debe en gran medida a que la Educación 4.0 se basa en el uso óptimo de herramientas y recursos tecnológicos, como los sistemas de gestión escolar que se desarrollan con frecuencia para aumentar la eficiencia de las instituciones educativas y superar la responsabilidad financiera del trabajo y la gestión.

El objetivo más importante de la Educación 4.0 para todas las instituciones educativas es animar a los estudiantes y mejorar los resultados de su aprendizaje.

También estiliza el aprendizaje con ejercicios más dinámicos y accesibles, como fotos y vídeos que hacen que los estudiantes se interesen más y aprendan a través de herramientas y plataformas. Esta es realmente revolucionaria y mejora enormemente los resultados de aprendizaje de los estudiantes (Hussin, 2018).

2.5.1. Características de Educación 4.0

Las herramientas de e-Learning ofrecen grandes oportunidades para el aprendizaje a distancia y a ritmo propio. El enfoque de aula invertida también desempeña un gran papel, ya que permite que el aprendizaje interactivo se realice en clase, mientras que las partes teóricas se aprenden fuera del tiempo de clase.

Los refuerzos positivos se utilizan para promover una experiencia de aprendizaje positiva y aumentar la confianza de los estudiantes en sus propias capacidades académicas.

Aunque los resultados de aprendizaje de un curso están preestablecidos por las instituciones u organismos encargados del plan de estudios, los estudiantes son libres de elegir las herramientas o técnicas de aprendizaje que prefieran. Los estudiantes deben aplicar sus conocimientos y habilidades en la realización de un par de proyectos de corta duración.

Al participar en los proyectos, están practicando sus habilidades de organización, colaboración y gestión del tiempo, que son útiles en sus futuras carreras académicas.

También estarán expuestos a un aprendizaje más práctico a través de la experiencia de campo, como las prácticas, las tutorías y proyectos de colaboración.

Serán evaluados de forma diferente y las plataformas convencionales para evaluar a los estudiantes pueden resultar irrelevantes o insuficientes.

Sus aportaciones ayudarán a los diseñadores del plan de estudios a mantener la contemporaneidad, la actualización y la utilidad de este.

Serán más independientes en su propio aprendizaje, lo que obligará a los profesores a asumir un nuevo papel de facilitadores que guiarán a los estudiantes en su proceso de aprendizaje.

Estas características de la Educación 4.0 desplazan las principales responsabilidades de aprendizaje de los instructores a los estudiantes.

Los instructores deben desempeñar su papel para apoyar la transición y nunca deben considerarla una amenaza para la profesión docente convencional (Hussin, 2018).

2.6. Fundamentos de Ciberseguridad.

La ciberseguridad se refiere a la comprensión de los problemas que rodean a los diversos ciberataques y a la elaboración de estrategias de defensa que preservan la integridad y la confidencialidad de la información.

Muchos expertos en ciberseguridad creen que el malware es el arma clave para llevar a cabo las intenciones maliciosas de violar los esfuerzos de ciberseguridad en el ciberespacio.

El malware se refiere a una amplia clase de ataques que se cargan en un sistema, normalmente sin el conocimiento del propietario legítimo, para comprometer el sistema en beneficio de un adversario.

Los programas maliciosos infectan los sistemas de diversas maneras, por ejemplo, propagándose desde máquinas infectadas, engañando al usuario para que abra archivos contaminados o incitándolo a visitar sitios web que propagan programas maliciosos.

El malware puede propagarse desde dispositivos y equipos que contienen sistemas integrados y lógica computacional. Las víctimas de los programas maliciosos pueden ser desde sistemas de usuario final, servidores, dispositivos de red y sistemas de control de procesos como los de control y adquisición de datos (SCADA).

El malware se utiliza a menudo para atacar sitios web gubernamentales o corporativos con el fin de recopilar información protegida o interrumpir sus operaciones.

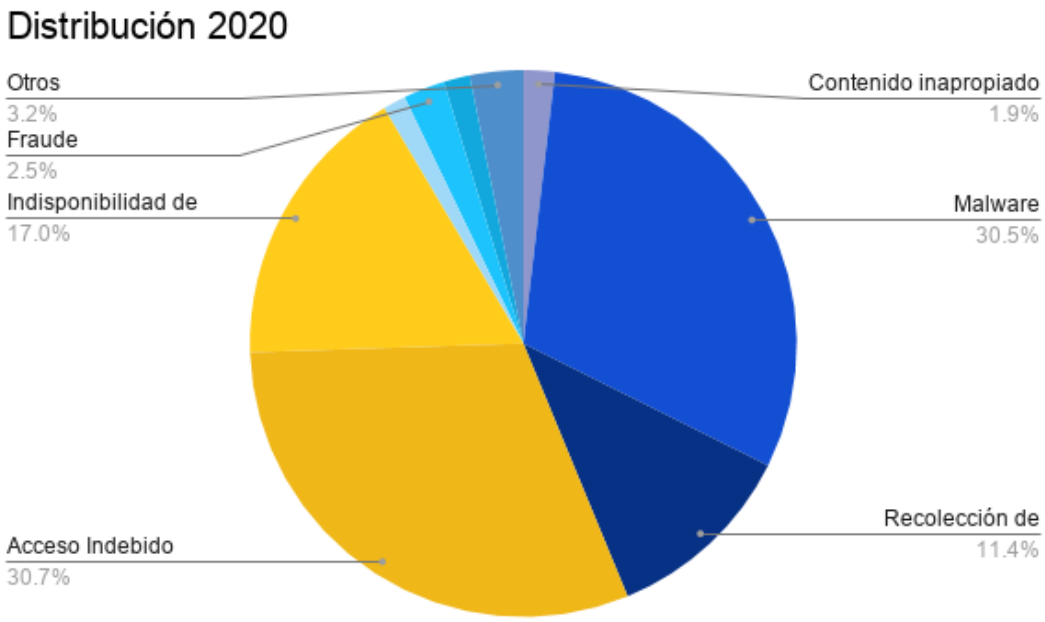
En otros casos, el malware también se utiliza contra individuos para obtener información personal, como números de la seguridad social o de tarjetas de crédito.

Desde el auge del acceso generalizado a Internet de banda ancha, más barato y rápido, el malware se ha diseñado cada vez más no sólo para ocultar información, sino también con fines estrictamente lucrativos. Durante el año 2020 se produjeron 2.798 vulnerabilidades de ciberseguridad, 38 de estos fueron catalogados como de gravedad "Alta", lo que supone un aumento del 26% respecto al año anterior.

Se mantuvo un crecimiento porcentual del "Malware" y aumentaron las vulnerabilidades del tipo "Acceso indebido" y "Recolección de información". La figura 2.4 describe las proporciones relativas de los incidentes de seguridad (Gub, 2020).

Figura 2. 4

Tipos de malware.



Nota. Adaptado de *Estadística de incidentes de Seguridad Informática 2020*, de Gub, 2020, Página web de investigación.

2.7. Clasificación de ciberseguridad

La ciberseguridad protege la integridad de los sistemas conectados a Internet, el hardware, el software y los datos de un ordenador frente a los ciberataques.

Sin un plan de seguridad, los piratas informáticos pueden acceder a un sistema informático y hacer un uso indebido de la información personal, la información de los clientes, la información comercial y mucho más.

Con una dependencia tan grande de los ordenadores, descuidar la posibilidad de la ciberdelincuencia en las empresas es extremadamente arriesgado y potencialmente perjudicial para la empresa, los empleados y los clientes.

Sin un sentido de la seguridad, las empresas funcionan con un alto riesgo de ciberataques. Existen diferentes tipos de ciberseguridad (Rosenthal, 2018).

2.7.1. Seguridad de las infraestructuras críticas:

La seguridad de las infraestructuras críticas consiste en los sistemas ciberfísicos de los que dependen las sociedades modernas. Tener la infraestructura de una red la hace vulnerable a los ciberataques.

Las organizaciones con responsabilidad sobre cualquier infraestructura crítica deben actuar con la debida diligencia para conocer las vulnerabilidades y proteger su negocio contra ellas.

La seguridad y resistencia de estas infraestructuras críticas es vital para la seguridad y el bienestar de nuestra sociedad.

Las organizaciones que no son responsables de las infraestructuras críticas, pero que aún dependen de ellas para una parte de su negocio, deberían desarrollar un plan de contingencia evaluando cómo podría afectarles un ataque a las infraestructuras críticas de las que dependen (Rosenthal, 2018).

2.7.2. Seguridad de las aplicaciones:

La seguridad de las aplicaciones debe ser una de las varias medidas de seguridad imprescindibles adoptadas para proteger sus sistemas. La seguridad de las aplicaciones utiliza métodos de software y hardware para hacer frente a las amenazas externas que pueden surgir en la fase de desarrollo de una aplicación.

Las aplicaciones son mucho más accesibles a través de las redes, lo que hace que la adopción de medidas de seguridad durante la fase de desarrollo sea una fase imperativa del proyecto.

Las empresas también pueden detectar los activos de datos sensibles y protegerlos mediante procesos específicos de seguridad de las aplicaciones que se adjuntan a estos conjuntos de datos (Rosenthal, 2018).

2.7.3. Seguridad de la red:

Mientras que la ciberseguridad se ocupa de las amenazas externas, la seguridad de la red protege contra la intrusión no autorizada de sus redes internas debido a intenciones maliciosas.

La seguridad de la red garantiza la seguridad de las redes internas protegiendo la infraestructura e impidiendo el acceso a la misma.

Para ayudar a gestionar mejor la supervisión de la seguridad de la red, los equipos de seguridad están utilizando ahora el aprendizaje automático para señalar el tráfico anormal y alertar de las amenazas en tiempo real.

Los administradores de red siguen aplicando políticas y procedimientos para evitar el acceso, la modificación y la explotación no autorizados de la red (Rosenthal, 2018).

2.7.4. Seguridad en la nube:

La mejora de la ciberseguridad es una de las principales razones por las que la nube se está imponiendo. La seguridad en la nube es una herramienta de seguridad basada en software que protege y supervisa los datos de sus recursos en la nube.

Los proveedores de la nube están creando e implementando constantemente nuevas herramientas de seguridad para ayudar a los usuarios de las empresas a proteger mejor sus datos. El mito que rodea a la computación en nube es que es menos segura que los enfoques tradicionales.

La gente tiende a creer que sus datos son más seguros cuando se almacenan en servidores físicos y sistemas que usted posee y controla. Sin embargo, la seguridad en la nube ha demostrado que el control no significa seguridad y que la accesibilidad importa más que la ubicación física de sus datos (Rosenthal, 2018).

2.7.5. Seguridad del Internet de las cosas (IoT)

IoT se refiere a una amplia variedad de sistemas físicos cibernéticos críticos y no críticos, como electrodomésticos, sensores, televisores, routers wifi, impresoras y cámaras de seguridad.

El centro de datos de IoT, la analítica, los dispositivos de consumo, las redes, los sistemas integrados heredados y los conectores son la tecnología principal del mercado de IoT. Los dispositivos IoT se envían con frecuencia en un estado vulnerable y ofrecen pocos o ningún parche de seguridad.

La seguridad es uno de los mayores obstáculos para la adopción de la IoT, las empresas comprarían más dispositivos IoT por término medio si se resolvieran los problemas de seguridad, estas son optimistas sobre el valor comercial y el crecimiento de IoT.

En general, la ciberseguridad es esencial para gobernar las conductas y maneras de interactuar con los sistemas informáticos frente a comportamientos sospechosos.

En un mundo en el que hasta los electrodomésticos de la cocina y los coches están conectados a Internet, los ciberdelincuentes tienen infinitas oportunidades de provocar el caos.

A medida que los piratas informáticos sigan adaptándose al progreso de la tecnología, también lo harán los expertos en seguridad informática, cuyo principal objetivo es mantener los datos seguros (Rosenthal, 2018).

2.8. Servicios de ciberseguridad

2.8.1. Seguridad de los datos

La seguridad de los datos es un conjunto de procesos y prácticas de ciberseguridad diseñadas para proteger su ecosistema crítico de tecnología de la información (TI).

Una seguridad de datos eficaz adopta un conjunto de controles, aplicaciones y técnicas que identifican la importancia de varios conjuntos de datos y aplican los controles de seguridad más adecuados. La seguridad de los datos es uno de los muchos métodos críticos para evaluar las amenazas y reducir el riesgo asociado al almacenamiento y manejo de los datos. Es fundamental para las organizaciones del sector público y privado por varias razones. En primer lugar, está la obligación legal y moral que tienen las empresas de proteger los datos de sus usuarios y clientes para que no caigan en manos equivocadas.

Además, está el riesgo para la reputación que supone una violación de datos o un hackeo. Si no se toma en serio la seguridad de los datos, su reputación puede verse dañada de forma permanente en caso de que se produzca una filtración o un pirateo informático de gran repercusión. Tendrá que dedicar tiempo y dinero a evaluar y reparar los daños, así como a determinar qué procesos empresariales han fallado y qué hay que mejorar (Harrington, 2018).

Los tipos de seguridad de los datos son:

- **Controles de acceso**

Este tipo de medidas de seguridad de datos incluye la limitación del acceso tanto físico como digital a los sistemas y datos críticos. Esto incluye asegurarse de que todos los ordenadores y dispositivos están protegidos con una entrada de acceso obligatoria, y que en los espacios físicos sólo puede entrar el personal autorizado.

- **Autenticación**

Al igual que los controles de acceso, la autenticación se refiere específicamente a la identificación precisa de los usuarios antes de que tengan acceso a los datos. Esto suele incluir elementos como contraseñas, números PIN, fichas de seguridad, tarjetas magnéticas o datos biométricos.

- **Copias de seguridad y recuperación**

Una buena seguridad de los datos significa que tienes un plan para acceder de forma segura a los datos en caso de fallo del sistema, desastre, corrupción de datos o violación.

Necesitará una copia de seguridad de los datos, almacenada en un formato distinto, como un disco físico, una red local o la nube, para recuperarlos en caso necesario.

- **Borrado de datos**

Querrá eliminar los datos adecuadamente y de forma regular. El borrado de datos emplea un software para sobrescribir completamente los datos en cualquier dispositivo de almacenamiento y es más seguro que el borrado de datos estándar.

El borrado de datos verifica que los datos son irrecuperables y, por lo tanto, no caerán en manos equivocadas.

- **Enmascaramiento de datos**

Mediante el uso de software de enmascaramiento de datos, la información se oculta mediante el uso de letras y números con caracteres proxy. Esto enmascara eficazmente la información clave incluso si una parte no autorizada accede a ella. Los datos vuelven a su forma original sólo cuando un usuario autorizado los recibe.

- **Resistencia de los datos**

La seguridad integral de los datos significa que sus sistemas pueden soportar o recuperarse de los fallos. Incorporar la resistencia a su hardware y software significa que eventos como cortes de energía o desastres naturales no comprometerán la seguridad.

- **Cifrado**

Un algoritmo informático transforma los caracteres de texto en un formato ilegible mediante claves de cifrado. Sólo los usuarios autorizados con las claves correspondientes pueden desbloquear y acceder a la información. Todo, desde los archivos y la base de datos hasta las comunicaciones por correo electrónico, puede estar cifrado en cierta medida.

2.8.2. Integridad del mensaje

La integridad de los mensajes significa que los datos deben llegar al receptor exactamente como fueron enviados. No debe haber cambios durante la transmisión, ni de forma accidental ni maliciosa.

La integridad del mensaje debe preservarse en una comunicación segura. La integridad de los mensajes significa que un mensaje no ha sido manipulado o alterado.

El enfoque más común es utilizar una función hash que combina todos los bytes del mensaje con una clave secreta y produce un compendio del mensaje que es difícil de revertir. La comprobación de la integridad es uno de los componentes de un programa de seguridad de la información.

2.8.3. Autenticación

El proceso de autentificación en el contexto de los sistemas informáticos significa la garantía y la confirmación de la identidad de un usuario. Antes de que un usuario intente acceder a la información almacenada en una red, debe demostrar su identidad y su permiso para acceder a los datos.

Cuando se conecta a una red, el usuario debe proporcionar una información de acceso única, incluyendo un nombre de usuario y una contraseña, una práctica que fue diseñada para proteger una red de la infiltración de los hackers.

La autenticación emplea diferentes combinaciones de datos, códigos de acceso, códigos QR, contraseñas, tarjetas de acceso, firmas digitales, escáneres de huellas dactilares, retina, rostro y voz para verificar la identidad de los usuarios antes de que puedan acceder a una red (Sangfor, 2021).

2.8.4. Control de acceso

El control de acceso es un componente fundamental de la seguridad de los datos que dicta quién puede acceder y utilizar la información y los recursos de la empresa.

Mediante la autenticación y la autorización, las políticas de control de acceso garantizan que los usuarios son quienes dicen ser y que tienen un acceso adecuado a los datos de la empresa.

El control de acceso también puede aplicarse para limitar el acceso físico a los campus, edificios, salas y centros de datos. Minimiza el riesgo de acceso autorizado a los sistemas físicos e informáticos, formando una parte fundamental de la seguridad de la información, la seguridad de los datos y la seguridad de la red.

2.9. Mecanismos de ciberseguridad

2.9.1. Intercambio de autenticación

El término autenticación suele referirse a la autenticación de usuarios, pero también puede referirse a la autenticación de dispositivos o procesos de software. Por ejemplo, algunos protocolos de enrutamiento soportan la autenticación de rutas, por lo que un router debe pasar algunos criterios antes de que otro router acepte sus actualizaciones de enrutamiento.

Mecanismo destinado a garantizar la identidad de una entidad mediante el intercambio de información. Este mecanismo de seguridad se ocupa de la identidad que debe conocerse en la comunicación (Cisco, 2010).

2.9.2. Criptografía

La criptografía es el proceso de conversión entre un texto legible, llamado texto plano, y una forma ilegible, llamada texto cifrado.

Esto ocurre de la siguiente manera:

- El emisor convierte el mensaje de texto plano en texto cifrado. Esta parte del proceso se llama encriptación (a veces cifrado).
- El texto cifrado se transmite al receptor.
- El receptor convierte el mensaje de texto cifrado de nuevo en su forma de texto plano. Esta parte del proceso se denomina desencriptación (a veces descifrado).

La conversión implica una secuencia de operaciones matemáticas que cambian la apariencia del mensaje durante la transmisión, pero no afectan al contenido.

Las técnicas criptográficas pueden garantizar la confidencialidad y proteger los mensajes contra la visualización no autorizada, ya que un mensaje cifrado no es comprensible. Las técnicas criptográficas involucran un algoritmo general, concretado por el uso de claves.

Hay dos clases de algoritmos:

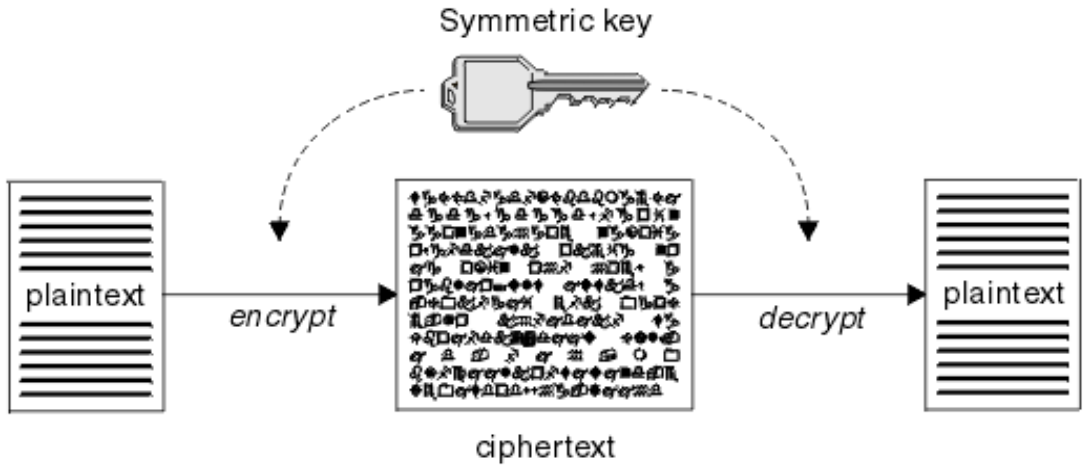
- Requieren que ambas partes utilicen la misma clave secreta, utilizan una clave compartida y se conocen como algoritmos simétricos. La figura 2.5 ilustra la criptografía de clave simétrica.
- Utilizan una clave para el cifrado y otra diferente para el descifrado, una de ellas debe mantenerse en secreto, pero la otra puede ser pública. Los algoritmos que utilizan pares de claves públicas y privadas se los conocen como algoritmos asimétricos.

La figura 2.6 ilustra la criptografía de clave asimétrica, la cual también se conoce como criptografía de clave pública.

Los algoritmos de cifrado y descifrado utilizados pueden ser públicos, pero la clave secreta compartida y la clave privada deben mantenerse en secreto (IBM, 2021).

Figura 2. 5

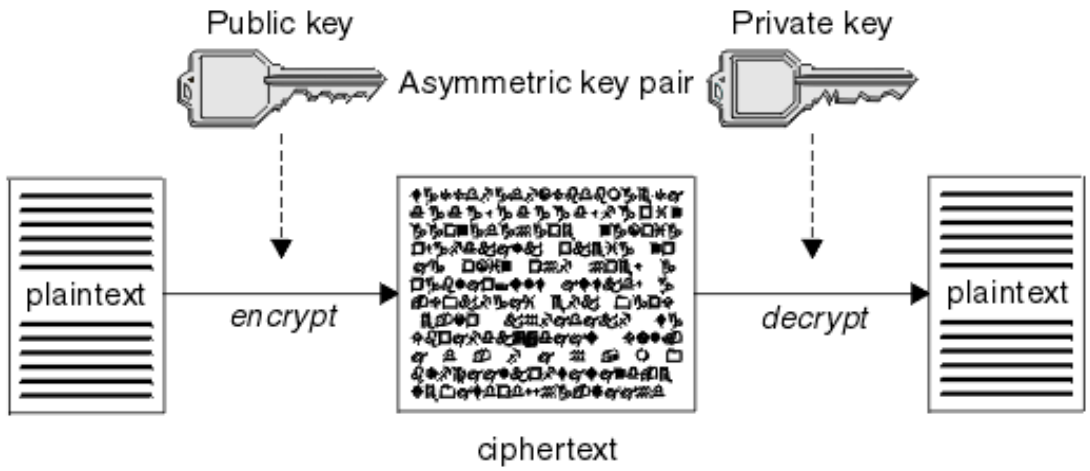
Criptografía de clave simétrica.



Nota. Adaptado de *Cryptography is the process of converting between readable text, called plaintext, and an unreadable form, called ciphertext*, de IBM, 2021, Página web de investigación.

Figura 2. 6

Criptografía de clave asimétrica.



Nota. Adaptado de *Cryptography is the process of converting between readable text, called plaintext, and an unreadable form, called ciphertext*, de IBM, 2021, Página web de investigación.

La figura 2.6 muestra el texto plano cifrado con la clave pública del receptor y descifrado con la clave privada del mismo. Sólo el receptor previsto tiene la clave privada para descifrar el texto cifrado.

Con los algoritmos asimétricos, los mensajes se cifran con la clave pública o con la privada, pero sólo pueden descifrarse con la otra clave.

Sólo la clave privada es secreta, la pública puede ser conocida por cualquiera. Los algoritmos asimétricos son más lentos, pero tienen la ventaja de que no existe el problema de la distribución de claves (IBM, 2021).

2.9.3. Cortafuegos

Un cortafuegos es un programa de hardware o software diseñado para mejorar la seguridad de la red. Su objetivo es bloquear todo el tráfico entrante no deseado y permitir que las comunicaciones autorizadas fluyan libremente.

Un cortafuegos de seguridad de red tradicional sólo puede proteger la red interna contra el tráfico entrante.

A pesar de ello, los cortafuegos han desempeñado un papel importante durante las últimas tres décadas.

Los tipos de cortafuegos son:

- **Cortafuegos proxy**

Un cortafuegos proxy protege los recursos de una red privada filtrando los mensajes marcados en la capa de aplicación.

- **Cortafuegos de inspección de estado**

Este tipo de cortafuegos bloquea el tráfico entrante basándose en el estado, el puerto y el protocolo.

- **Cortafuegos de nueva generación (NGFW)**

Los cortafuegos de nueva generación pueden bloquear las ciberamenazas actuales, como el malware avanzado y los ataques a la capa de aplicación.

- **Cortafuegos de gestión unificada de amenazas (UTM)**

Los cortafuegos UTM ofrecen una única solución de seguridad que proporciona múltiples funciones de seguridad.

- **NGFW centrado en las amenazas**

Los NGFW centrados en las amenazas ofrecen detección y corrección de amenazas avanzadas.

2.9.4. Firma digital

La firma digital es una técnica que valida la autenticidad e integridad de un mensaje, un programa informático o unos documentos digitales.

Permite verificar el nombre del autor, la fecha y la hora de las firmas, y autentificar el contenido del mensaje.

La firma digital ofrece una seguridad mucho más inherente y pretende resolver el problema de la suplantación en las comunicaciones digitales.

La autentificación de la información empresarial basada en la informática interrelaciona tanto la tecnología como la ley.

También exige la cooperación entre personas de diferentes ámbitos profesionales y áreas de conocimiento. Se diferencian de otras firmas electrónicas no sólo en cuanto al proceso y al resultado, sino que también hace que las firmas digitales sean más útiles a efectos legales.

2.9.5. Funciones HASH

La función Hash tiene un gran papel en la seguridad de un sistema, ya que convierte los datos normales que se le dan, en un valor irregular de longitud fija. Cuando se introducen datos en esta función, se obtiene un valor irregular.

El valor irregular que emite se conoce como "Valor Hash". Los valores Hash son simplemente números, pero a menudo se escriben en hexadecimal. Los ordenadores gestionan los valores como binarios. El valor hash también es un dato y suele gestionarse en Binario.

Hashing es un algoritmo que se aplica a datos como un archivo o un mensaje para producir un número llamado hash. Hash se utiliza para verificar que los datos no han sido modificados, manipulados o corrompidos.

Un punto clave sobre el hash es que no importa cuántas veces se ejecute el algoritmo de hash contra los datos, este siempre será el mismo si los datos son los iguales (GeeksforGeeks, 2018).

2.9.6. Terceras partes de confianza (TTP)

Entidad distinta del propietario y del verificador en la que el propietario, el verificador o ambos confían para prestar determinados servicios. Es una entidad que facilita las interacciones entre dos partes que confían en el tercero. En los modelos TTP, las partes que confían utilizan esta confianza para asegurar sus propias interacciones.

Los TTP son comunes en cualquier número de transacciones comerciales y en las transacciones digitales criptográficas, así como en los protocolos criptográficos.

Del mismo modo, las transacciones que necesitan un registro de terceros también necesitarían un servicio de depósito de terceros de algún tipo.

2.10. Ciberseguridad en centros de datos

La ciberseguridad en los centros de datos son los sistemas y medidas de apoyo físico y digital que mantienen las operaciones, las aplicaciones y los datos de los centros de datos a salvo de las amenazas.

Los centros de datos son instalaciones que proporcionan acceso compartido a aplicaciones y datos críticos utilizando una compleja infraestructura de red, computación y almacenamiento.

Existen normas de la industria para ayudar en el diseño, la construcción y el mantenimiento de los centros de datos, con el fin de garantizar la seguridad y la alta disponibilidad de los datos.

- **Seguridad física de los centros de datos**

Los centros de datos deben estar protegidos contra las amenazas físicas a sus componentes. Los controles de seguridad física incluyen una ubicación segura, los controles de acceso físico del edificio y los sistemas de supervisión que mantienen seguras las instalaciones de un centro de datos.

Además de los sistemas de seguridad física desplegados dentro de un centro de datos, las infraestructuras de TI de los centros de datos requieren un análisis exhaustivo de confianza incorporado en cualquier diseño de centro de datos.

- **Seguridad digital de los centros de datos**

Además de las protecciones físicas, los centros de datos también requieren una seguridad centrada en las amenazas digitales.

Esto incluye la implementación de controles de acceso a la seguridad informática del centro de datos y la selección de soluciones de seguridad adaptadas a las necesidades de los centros de datos (Checkpoint, 2021).

2.10.1. Herramientas de seguridad digitales en las redes de centros de datos

El hacking, el malware y el spyware son las amenazas obvias para los datos almacenados en un centro de datos. Una herramienta de gestión de eventos e información de seguridad (SIEM) ofrece una visión en tiempo real de la postura de seguridad de un centro de datos. La creación de zonas seguras en la red es una forma de incorporar la seguridad al centro de datos. Los administradores pueden dividir las redes en tres zonas: una zona de pruebas con gran flexibilidad, una zona de desarrollo con un entorno algo más estricto y una zona de producción con sólo equipos de producción aprobados.

Antes de desplegar las aplicaciones y el código, se pueden utilizar ciertas herramientas para escanearlas en busca de vulnerabilidades que puedan ser fácilmente explotadas, y luego proporcionar métricas y capacidades de remediación.

El código puede pasarse por un escáner para comprobar si hay desbordamientos de búfer u otras vulnerabilidades. Con el aumento de la computación en la nube, la visibilidad de los flujos de datos es una necesidad, ya que podría haber malware escondido dentro de un tráfico por lo demás legítimo.

- **Nmap**

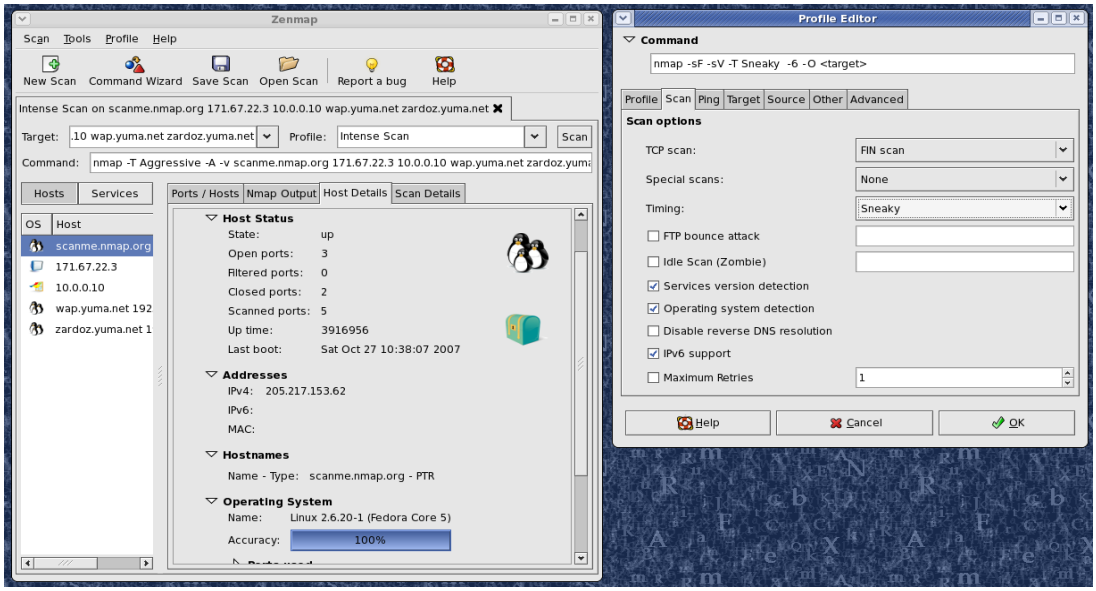
Nmap, abreviatura de Network Mapper, es una herramienta gratuita y de código abierto para el escaneo de vulnerabilidades y el descubrimiento de redes. Los administradores de red utilizan Nmap para identificar qué dispositivos se ejecutan en sus sistemas, descubrir los hosts que están disponibles y los servicios que ofrecen, encontrar puertos abiertos y detectar riesgos de seguridad.

Aunque Nmap ha evolucionado a lo largo de los años y es extremadamente flexible, en el fondo es una herramienta de escaneo de

puertos, que recopila información enviando paquetes en bruto a los puertos del sistema, escucha las respuestas y determina si los puertos están abiertos, cerrados o filtrados de alguna manera como se ve en la figura 2.7. Otros términos utilizados para el escaneo de puertos incluyen el descubrimiento de puertos o la enumeración.

Figura 2. 7

Escaneo de puertos en Nmap.



Nota. Adaptado de *Nmap: the Network Mapper - Security Scanner*, de Nmap, 2021, Página web de investigación.

- **SAINT**

SAINT (Security Administrator's Integrated Network Tool) es un programa informático utilizado para escanear las redes informáticas en busca de vulnerabilidades de seguridad y explotar las vulnerabilidades encontradas. El escáner SAINT examina todos los sistemas vivos de una red en busca de servicios TCP y UDP.

Describe cada una de las vulnerabilidades que localiza y describe las formas de corregir las vulnerabilidades. Proporciona enlaces a parches o nuevas versiones de software que eliminarán las vulnerabilidades detectadas.

- **NESSUS**

Nessus es una herramienta de escaneo de seguridad remota, que analiza un ordenador y emite una alerta si descubre alguna vulnerabilidad que los hackers malintencionados podrían utilizar para acceder a cualquier ordenador conectado a una red.

Para ello, ejecuta más de 1.200 comprobaciones en un ordenador determinado, comprobando si alguno de estos ataques podría utilizarse para entrar en el ordenador o dañarlo de alguna manera.

Nessus trabaja probando cada puerto de un ordenador, determinando qué servicio está ejecutando y, a continuación, probando este servicio para asegurarse de que no hay vulnerabilidades en él que puedan ser utilizadas por un hacker para llevar a cabo un ataque malicioso como se muestra en la figura 2.8.

2.10.2. Registro de eventos en la red

En las redes, un registro de eventos es un recurso básico que ayuda a proporcionar información sobre el tráfico de la red, el uso de esta y otras condiciones.

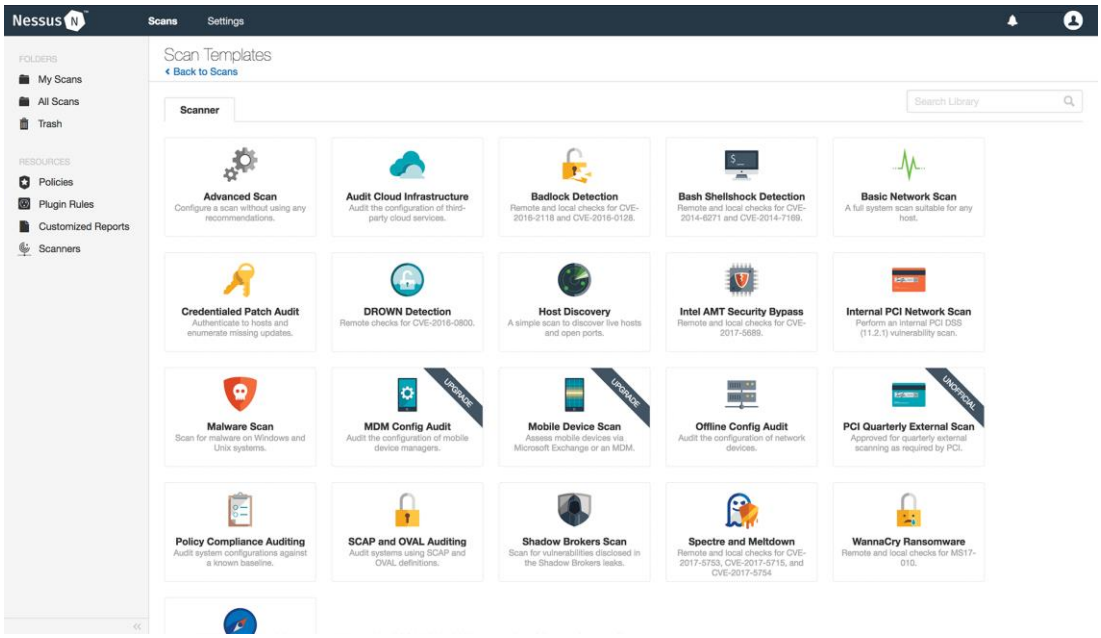
Un registro de eventos almacena estos datos para que los profesionales de la seguridad o los sistemas de seguridad automatizados puedan recuperarlos y ayudar a los administradores de la red a gestionar diversos aspectos como la seguridad, el rendimiento y la transparencia.

Un registro de eventos suele ser utilizado por una herramienta llamada información de seguridad y herramienta de gestión de eventos.

Esta herramienta proporciona un mayor nivel de análisis del contenido de un registro de eventos para ayudar a los administradores de la red a determinar lo que está sucediendo dentro de una red (Techopedia, 2021a).

Figura 2. 8

Software Nessus.



Nota. Adaptado de *Tenable® - The Cyber Exposure Company*, de Tenable, 2021, Página web de investigación.

2.10.3. Organismos de respuesta

- **CSIRT**

Los equipos de respuesta a incidentes de seguridad o CSIRT, restablecen las tareas con el mínimo impacto. El CSIRT debe cumplir con distintos objetivos, uno de ellos es mermar cualquier afectación.

También se debe coordinar la recuperación de las actividades que se han visto afectadas, para que la empresa vuelva a funcionar normalmente lo antes posible (WeLiveSecurity, 2015).

- **EcuCERT**

Este centro de respuesta tiene la responsabilidad de velar por el buen manejo de las redes de telecomunicaciones del país; para ello, brindará bienes, respuestas ágiles y servicios de calidad a la sociedad. Además, coopera con otros CSIRT dentro y fuera de Ecuador (Almeida, 2019).

2.10.4. Sanciones legales por infracción de políticas de ciberseguridad en Ecuador

- **Artículo 229 - Revelación ilegal de base de datos**

La persona que, en provecho propio o de un tercero, revele información registrada, contenida en archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (Ecuador. Leyes y Reglamentos, 2014).

- **Artículo 230 - Interceptación ilegal de datos**

Será sancionado con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (Ecuador. Leyes y Reglamentos, 2014).

- **Artículo 231 - Transferencia electrónica de activo patrimonial**

La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (Ecuador. Leyes y Reglamentos, 2014).

- **Artículo 232 - Ataque a la integridad de sistemas informáticos**

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo

rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (Ecuador. Leyes y Reglamentos, 2014).

- **Artículo 233 - Delitos contra la información pública reservada legalmente**

La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses,

siempre que no se configure otra infracción de mayor gravedad (Ecuador. Leyes y Reglamentos, 2014).

- **Artículo 234 - Acceso no consentido a un sistema informático, telemático o de Telecomunicaciones**

La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Ecuador. Leyes y Reglamentos, 2014).

2.11. Programas maliciosos habituales en ciberataques

Un ciberataque es un intento malicioso y deliberado por parte de un individuo u organización de violar el sistema de información de otro individuo u organización. Normalmente, el atacante busca algún tipo de beneficio al interrumpir la red de la víctima (Cisco, 2021).

Es un intento de inutilizar ordenadores, robar datos o utilizar un sistema informático violado para lanzar otros ataques. Utilizan diferentes métodos para lanzar un ciberataque que incluye el malware, el phishing, el ransomware, el ataque del hombre en el medio u otros métodos. Los ciberataques son cada vez más frecuentes en los últimos años.

Malware es un término utilizado para describir el software malicioso, incluyendo spyware, ransomware, virus y gusanos. El malware penetra en una red a través de una vulnerabilidad, normalmente cuando un usuario hace clic en un enlace peligroso o en un archivo adjunto de correo electrónico que luego instala un software arriesgado.

Una vez dentro del sistema, el malware puede hacer lo siguiente:

- Bloquea el acceso a componentes clave de la red (ransomware).
- Instala malware o software dañino adicional.
- Obtiene información de forma encubierta transmitiendo datos del disco duro (spyware).
- Interrumpe ciertos componentes y deja el sistema inoperativo.

2.11.1. Virus

Un virus informático, al igual que un virus de la gripe, está diseñado para propagarse de un huésped a otro y tiene la capacidad de replicarse. Del mismo modo, al igual que los virus de la gripe no pueden reproducirse sin una célula huésped, los virus informáticos no pueden reproducirse y propagarse sin una programación como la de un archivo o documento.

Un virus informático es un tipo de código o programa malicioso diseñado para propagarse de un ordenador a otro. Funciona insertando o adhiriéndose a un programa o documento legítimo que admita macros para ejecutar su código.

En el proceso, un virus tiene el potencial de causar efectos inesperados o perjudiciales, como dañar el software del sistema corrompiendo o destruyendo datos. Una vez que un virus se ha unido con éxito a un programa, archivo o documento, el virus permanecerá latente hasta que las circunstancias hagan que el ordenador o dispositivo ejecute su código.

Para que un virus infecte el ordenador, el operador tiene que ejecutar el programa infectado, lo que a su vez hace que se ejecute el código del virus. Una vez que el virus infecta el ordenador, puede infectar otros ordenadores de la misma red, robar contraseñas o datos, registrar las pulsaciones del teclado, corromper archivos, enviar spam a los contactos de correo electrónico e incluso tomar el control de la máquina son algunas de las cosas devastadoras e irritantes que puede hacer un virus.

2.11.2. Gusanos de red

Un gusano de red es un tipo de malware que se autorreplica en la red. Estos virus virtuales independientes se propagan por Internet, se introducen en los ordenadores y se replican sin la intervención de los usuarios y sin que éstos lo sepan.

Los gusanos de red pueden estar incluidos en cualquier tipo de virus, script o programa. Suelen infectar los sistemas aprovechando fallos o vulnerabilidades que suelen encontrarse en el software legítimo. Pueden propagarse por sí solos, esto los hace extremadamente peligrosos, también se conocen como gusanos informáticos.

Los gusanos de red están incrustados en el software y penetran la mayoría de los cortafuegos y otras formas de seguridad de la red. Las aplicaciones de software antivirus combaten los gusanos junto con otras formas de malware, como los virus.

2.11.3. Caballos de Troya

Un "troyano" es un tipo de malware que normalmente se oculta como un archivo adjunto en un correo electrónico o un archivo de descarga gratuita, y luego se transfiere al dispositivo del usuario.

Una vez descargado, el código malicioso ejecutará la tarea para la que lo diseñó el atacante, como obtener un acceso de puerta trasera a los sistemas corporativos, espiar la actividad en línea de los usuarios o robar datos sensibles. A diferencia de los virus informáticos, un troyano no puede manifestarse por sí mismo, por lo que necesita que un usuario descargue la parte del servidor de la aplicación para que funcione.

Los dispositivos pueden ser infectados por un troyano mediante tácticas de ingeniería social, que los ciberdelincuentes utilizan para coaccionar a los usuarios para que descarguen una aplicación maliciosa.

El archivo malicioso puede estar oculto en banners publicitarios, anuncios emergentes o enlaces en sitios web.

Los troyanos también pueden atacar e infectar los smartphones y las tabletas mediante una cadena de malware móvil.

Esto podría ocurrir a través del atacante que redirige el tráfico a un dispositivo conectado a una red Wi-Fi y luego lo utiliza para lanzar ciberataques (Fortinet, 2021).

2.11.4. Keyloggers

Un keylogger es un tipo de software o hardware que se utiliza para rastrear y registrar lo que alguien escribe en el teclado.

Los actores maliciosos pueden utilizarlos para capturar su información personal y financiera, códigos PIN y números de cuenta, números de tarjetas de crédito, nombres de usuario, contraseñas y otros datos sensibles, todo lo cual puede utilizarse para cometer fraudes o robos de identidad.

Registran todas las interacciones del teclado de un usuario, lo que permite a un tercero ver un registro completo de cada correo electrónico, mensaje instantáneo, consulta de búsqueda, contraseña, nombre de usuario u otras secuencias de teclas que el usuario escriba.

Los keyloggers pueden infectar al ordenador a través de muchos de los mismos mecanismos que otros virus comunes, pero también pueden ser adquiridos y descargados intencionadamente.

2.11.5. Spyware

El spyware se define en términos generales como un software malicioso diseñado para entrar en un dispositivo informático, recopilar datos y enviarlos a un tercero sin consentimiento.

El software espía malicioso se utiliza explícitamente para sacar provecho de los datos robados. La actividad de vigilancia del spyware le deja expuesto a violaciones de datos y al uso indebido de los datos privados.

El spyware puede entrar en un ordenador por todas las vías que toma otro malware, como cuando el usuario visita un sitio web comprometido o abre un archivo adjunto malicioso en un correo electrónico (Kaspersky, 2021b).

2.11.6. Adware

El adware, también conocido como software respaldado por publicidad, genera ingresos para sus desarrolladores al generar automáticamente anuncios en la pantalla, normalmente dentro de un navegador web.

Suele crearse para ordenadores, pero también puede encontrarse en dispositivos móviles. El adware es un software que muestra anuncios emergentes no deseados que pueden aparecer en el ordenador o en el dispositivo móvil.

El adware suele acabar en el dispositivo de un usuario de dos maneras:

- El usuario puede instalar un programa informático o una aplicación gratuita sin darse cuenta necesariamente de que contiene software adicional que contiene adware.
- Otra posibilidad es que haya una vulnerabilidad en el software o en el sistema operativo que los hackers aprovechen para introducir programas maliciosos, incluidos algunos tipos de adware, en el sistema.

2.11.7. Riskware

Riskware es un concepto general que se refiere a los programas legítimos que son potencialmente peligrosos debido a la incompatibilidad del software, la vulnerabilidad de la seguridad o las violaciones legales.

El software de riesgo suele dejar los sistemas vulnerables en lo que respecta a la explotación de datos y programas, y a los riesgos legales (Georgescu, 2020).

2.11.8. Ransomware

El ransomware es un tipo de malware que amenaza con publicar o bloquear el acceso a los datos o a un sistema informático, normalmente cifrándolo, hasta que la víctima pague un rescate al atacante.

En muchos casos, la petición de rescate viene acompañada de una fecha límite. Si la víctima no paga a tiempo, los datos desaparecen para siempre o el rescate aumenta.

Varias agencias gubernamentales, entre ellas el FBI, desaconsejan pagar el rescate para no fomentar el ciclo del ransomware, al igual que el Proyecto No More Ransom.

Además, la mitad de las víctimas que pagan el rescate son propensas a sufrir nuevos ataques de ransomware, especialmente si no se limpia del sistema (Proofpoint, 2020).

2.12. Fases de ciberataques

Los ciberataques a infraestructuras críticas son cada vez más comunes, complejos y creativos. Esto supone un reto permanente para los equipos de ciberseguridad, que necesitan saber dónde están expuestas sus operaciones a las amenazas antes de que los hackers puedan encontrarlas.

Los ataques tienen como objetivo la interrupción de los servicios en lugar de buscar el robo de datos para obtener beneficios económicos. En lugar de atacar directamente a sus objetivos principales, se dirigen a proveedores menos seguros que esos objetivos utilizan. Aunque los detalles de los ataques individuales pueden variar, es posible definir siete fases de un ciberataque.

Esto proporciona una base común para entender cómo y cuándo surgen las amenazas, de modo que se pueda optimizar la vigilancia, la prevención y las respuestas eficaces.

2.12.1. Primera fase: Reconocimiento de un objetivo para el hackeo

En la fase de reconocimiento, los hackers identifican un objetivo vulnerable y averiguan cómo explotarlo. El objetivo inicial puede ser cualquier persona de la empresa. Los atacantes sólo necesitan un punto de entrada para empezar. Los correos electrónicos de phishing dirigidos son habituales como método eficaz de distribución de malware en esta fase.

En esta fase, los hackers se preguntan quiénes son las personas importantes de la empresa, con quienes hacen negocios y qué datos públicos están disponibles sobre la organización objetivo. Cuanto más tiempo dediquen los hackers a obtener información sobre las personas y los sistemas de la empresa, más éxito tendrá el intento de pirateo.

2.12.2. Segunda fase: Arma de la información sobre una empresa

En la fase de armamento, el hacker utiliza la información previamente recopilada para crear formas de entrar en la red del objetivo. Esto podría implicar la creación de mensajes de correo electrónico de phishing selectivo que parezcan correos electrónicos que el objetivo podría recibir de un proveedor conocido u otro contacto comercial.

La acción final del atacante en esta fase es recoger las herramientas para explotar con éxito cualquier vulnerabilidad que pueda encontrar cuando más tarde obtenga acceso a la red del objetivo.

2.12.3. Tercera fase: "Entrega" del ataque

El ataque comienza en la fase de entrega. Se envían los correos electrónicos de phishing, se publican en Internet las páginas web y el atacante

espera la llegada de todos los datos que necesita. Si el correo electrónico de phishing contiene un archivo adjunto con un arma, el atacante espera a que alguien abra el archivo adjunto y que el malware que contiene "llame" al hacker.

2.12.4. Cuarta fase: Explotación de la brecha de seguridad

En la fase de explotación, el pirata informático comienza a cosechar los frutos de la preparación y ejecución del ataque. A medida que llegan los nombres de usuario y las contraseñas, el atacante los prueba contra los sistemas de correo electrónico basados en la web o las conexiones de red privada virtual (VPN) a la red de la empresa.

Si se han enviado archivos adjuntos infectados con malware, el atacante accede de forma remota a los ordenadores afectados. El hacker explora la red objetivo y se hace una idea del flujo de tráfico en ella, qué sistemas están conectados a ella y cómo pueden ser explotados.

2.12.5. Quinta fase: Instalación de una puerta trasera persistente

En la fase de instalación, el atacante se asegura el acceso continuo a la red. Para conseguirlo, el hacker instalará una puerta trasera persistente, creará cuentas de administrador en la red y desactivará las reglas del cortafuegos.

Incluso puede activar el acceso al escritorio remoto en los servidores y otros sistemas de la red. La intención del hacker en este punto es estar seguro de permanecer en el sistema el tiempo necesario para lograr sus objetivos.

2.12.6. Sexta fase: Ejercer el mando y el control

Ahora tienen acceso irrestricto a toda la red y a las cuentas de administrador, todas las herramientas necesarias están listas para la fase de comando y control.

El atacante puede mirar cualquier cosa, hacerse pasar por cualquier usuario de la red e incluso enviar correos electrónicos del director general a todos los empleados.

Ahora que tiene el control, el hacker puede bloquear a los usuarios de TI de una empresa de toda la red de la organización si lo desea, tal vez exigiendo un rescate para restaurar el acceso.

2.12.7. Séptima fase: Lograr los objetivos del hacker

Ahora comienza la fase de acción sobre los objetivos. Esto podría implicar el robo de información sobre empleados, clientes, diseños de productos, etc. O un atacante podría empezar a interrumpir las operaciones de la empresa objetivo.

Si una empresa recibe pedidos en línea, un hacker podría cerrar el sistema de pedidos o borrarlos, por ejemplo. Incluso podría crear pedidos y hacerlos llegar a los clientes de la empresa.

Si un hacker accede a un sistema de control industrial, podría apagar los equipos, introducir nuevos puntos de ajuste y desactivar las alarmas.

2.13. Tipos de ciberataques según autoría

2.13.1. Por Estados

Los Estados pueden emplear directamente a los hackers a través de sus ejércitos y autoridades gubernamentales, pueden financiarlos indirectamente. Esto hace que sea más fácil negar la implicación del Estado si se detecta el ataque. Esto, a su vez, puede disminuir las repercusiones diplomáticas que pueden tener estos ataques. También difumina la línea entre las organizaciones criminales y los grupos gubernamentales. Las unidades patrocinadas por el Estado se dirigen entonces a los adversarios de sus financiadores por diferentes razones.

Los ciberataques patrocinados por el Estado pueden, por ejemplo, implicar:

- Espionaje: Descubrimiento de secretos empresariales, tecnologías, información política secreta, etc.
- Atacar infraestructuras críticas y empresas: Esto puede dañar al defensor y disminuir en gran medida sus capacidades defensivas.
- Difusión de desinformación: Esta acción puede ser muy eficaz para perturbar la opinión política dentro de un Estado, afectar a las elecciones, difundir el resentimiento contra gobiernos o personas, o mejorar la opinión pública sobre determinados partidos.
- Probar las capacidades y la preparación de los adversarios: A veces, el único objetivo es poner a prueba las capacidades del atacante o ver lo bien preparado que está el adversario.

2.13.2. Por Organizaciones privadas

Estas llevan a cabo ataques para conseguir información confidencial de otras instituciones o gobiernos con el fin de obtener una ventaja en el mercado o un beneficio fraudulento. Suele llevarse a cabo junto a entidades gubernamentales.

2.13.3. Por Terrorismo, extremismo político e ideológico

El ciberterrorismo es cualquier ataque premeditado, con motivación política, contra los sistemas de información, programas y datos, que tiene como resultado la violencia.

El FBI distingue un ataque ciberterrorista como un tipo de ciberdelito explícitamente diseñado para causar daños físicos. Otras organizaciones y expertos sugieren que los ataques menos dañinos también pueden considerarse actos de ciberterrorismo, siempre que los ataques tengan la intención de ser perturbadores o de promover la postura política de los atacantes.

En algunos casos, la diferenciación entre los ataques ciberterroristas y la actividad cibercriminal más ordinaria radica en la intención: La motivación principal de los ataques ciberterroristas es perturbar o perjudicar a las víctimas, aunque los ataques no produzcan daños físicos o causen un daño financiero extremo.

2.13.4. Por Ataques de crimen organizado

La ciberdelincuencia es tan popular que redes bien organizadas de ciberdelincuentes trabajan en colaboración para llevar a cabo atracos masivos a través de Internet.

Estas organizaciones de ciberdelincuentes son grupos de hackers, programadores y otros bandidos tecnológicos que combinan sus habilidades y recursos para cometer grandes delitos que de otro modo no serían posibles.

Los grupos organizados de ciberdelincuencia pueden ser pequeños o grandes, estar poco afiliados o bien definidos; algunos grupos son casi de naturaleza corporativa, con un liderazgo establecido y varios miembros que desempeñan funciones específicas.

2.13.5. Por Hacktivismo

El hacktivismo es el acto de utilizar indebidamente un sistema informático o una red por una razón social o política.

El objetivo del hacktivismo es llamar la atención del público sobre algo que el hacktivista cree que es una cuestión o causa importante, como la libertad de información, los derechos humanos o un punto de vista religioso.

Los hacktivistas expresan su apoyo a una causa social o su oposición a una organización mostrando mensajes o imágenes en el sitio web de la organización que creen que está haciendo algo mal o a cuyo mensaje o actividades se oponen.

2.14. Tipos de ciberataques según impacto

2.14.1. Spear-phishing

El spear phishing es una estafa por correo electrónico o por comunicaciones electrónicas dirigida a una persona, organización o empresa específica. Aunque a menudo pretende robar datos con fines maliciosos, los ciberdelincuentes también pueden tener la intención de instalar malware en el ordenador del usuario objetivo.

Muchas veces, hackers y hacktivistas patrocinados por el gobierno están detrás de estos ataques. Los ciberdelincuentes hacen lo mismo con la intención de revender datos confidenciales a gobiernos y empresas privadas. Como resultado, incluso los objetivos de alto rango dentro de las organizaciones, como los altos ejecutivos, pueden encontrarse abriendo correos electrónicos que pensaban que eran seguros (Kaspersky, 2021a).

2.14.2. Watering-hole

Un ataque de watering hole es un exploit de seguridad en el que el atacante busca comprometer a un grupo específico de usuarios finales infectando sitios web que los miembros del grupo son conocidos por visitar. El objetivo es infectar el ordenador de un usuario objetivo y obtener acceso a la red en el lugar de trabajo del objetivo.

El término "watering hole attack" proviene de "hunting". En lugar de rastrear a su presa a lo largo de una gran distancia, el cazador determina dónde es probable que vaya la presa. Cuando la presa se acerca por su propia voluntad, a menudo con la guardia baja, el cazador ataca. La víctima objetivo puede ser un individuo, una organización o un grupo de personas.

El atacante hace un perfil de sus objetivos para determinar el tipo de sitios web que frecuentan. A menudo se trata de tablones de anuncios o sitios de interés general populares entre el objetivo previsto.

2.14.3. Man in the middle

Un ataque de Man in the middle (MITM) es un término general para referirse a cuando un perpetrador se posiciona en una conversación entre un usuario y una aplicación, ya sea para espiar o para hacerse pasar por una de las partes, haciendo parecer que se está produciendo un intercambio normal de información.

El objetivo de un ataque es robar información personal, como credenciales de acceso, detalles de cuentas y números de tarjetas de crédito. La información obtenida durante un ataque puede utilizarse para muchos fines, como el robo de identidad, las transferencias de fondos no aprobadas o el cambio ilícito de contraseñas.

2.14.4. Masquerade

Un ataque de enmascaramiento es un ataque que utiliza una identidad falsa, como una identidad de red, para obtener acceso no autorizado a la información de un ordenador personal a través de una identificación de acceso legítima.

Los ataques de enmascaramiento se pueden perpetrar utilizando contraseñas e inicios de sesión robados, localizando lagunas en los programas o encontrando una forma de eludir el proceso de autenticación.

El grado de acceso que obtienen los atacantes de la mascarada depende del nivel de autorización que hayan logrado obtener. Los ataques personales, aunque menos comunes, también pueden ser perjudiciales (Techopedia, 2021b).

2.14.5. Modification

La modificación es un ataque contra la integridad de la información. Básicamente hay tres tipos de modificaciones:

- **Modificación**: Cambiar la información existente. La información ya existe, pero es incorrecta. Los ataques de modificación pueden dirigirse a la información sensible o a la información pública.
- **Inserción**: Cuando se realiza un ataque de inserción, se añade información que no existía previamente. Este ataque puede ir dirigido a la información histórica o a la que aún no se ha actuado.
- **Borrado**: Eliminación de información existente.

2.14.6. Negación de servicios

Un ataque de denegación de servicio (DoS) es un ataque destinado a apagar una máquina o red, haciéndola inaccesible a sus usuarios.

Estos lo consiguen inundando el objetivo con tráfico, o enviando información que desencadena una caída. En ambos casos, el ataque DoS priva a los usuarios legítimos del servicio o recurso que esperaban.

Aunque los ataques DoS no suelen provocar el robo o la pérdida de información significativa u otros activos, pueden costar a la víctima una gran cantidad de tiempo y dinero.

2.14.7. Trapdoor

Una trapdoor es un punto de entrada en un sistema de tratamiento de la información que elude las medidas normales de seguridad. Por lo general, se trata de un programa oculto o de un componente electrónico que hace ineficaz el sistema de protección si se le dan ciertas órdenes no documentadas.

Además, la trapdoor suele activarse mediante un evento o una acción normal. Otra definición de trapdoor es que se trata de un método para eludir los métodos normales de autentificación.

La mejor garantía contra las trapdoors es utilizar software cuyos códigos fuente sean públicos y sean analizados por un máximo de personas.

2.14.8. Ingeniería Social

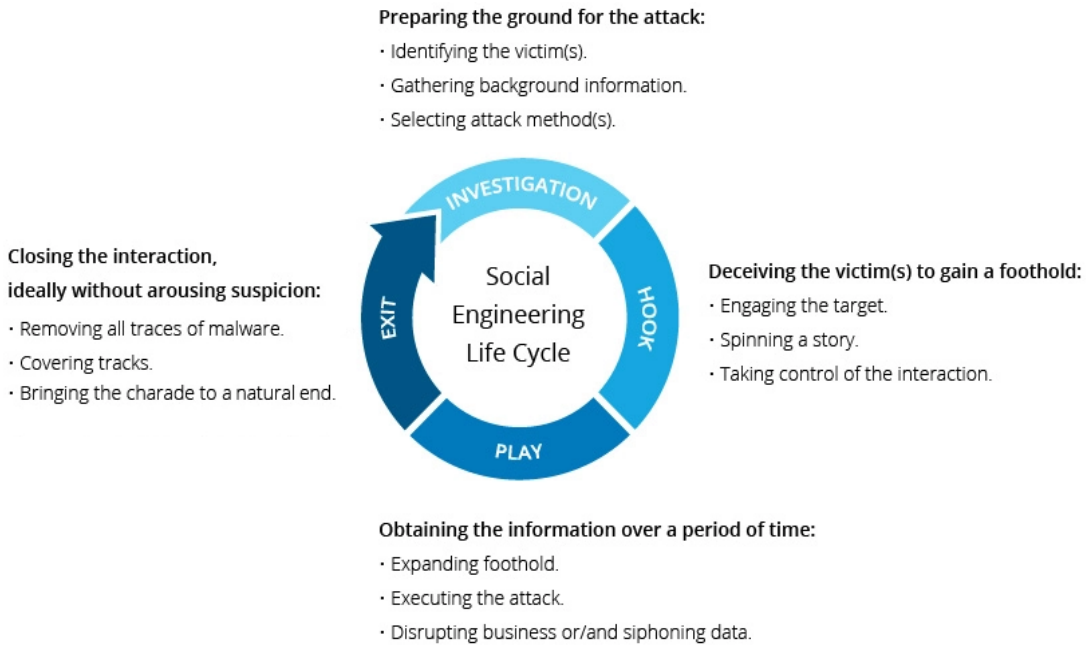
La ingeniería social es el término utilizado para una amplia gama de actividades maliciosas realizadas a través de las interacciones humanas. Utiliza la manipulación psicológica para engañar a los usuarios para que cometan errores de seguridad o faciliten información sensible. Los ataques de ingeniería social se producen en uno o varios pasos.

En primer lugar, el agresor investiga a la víctima prevista para recopilar la información de fondo necesaria, como los posibles puntos de entrada y los protocolos de seguridad débiles, necesarios para llevar a cabo el ataque.

Después, el atacante se mueve para ganarse la confianza de la víctima y proporcionar estímulos para las acciones posteriores que rompen las prácticas de seguridad, como revelar información sensible o conceder acceso a recursos críticos. Estos ataques tienen un ciclo de vida el cual se muestra en la figura 2.9. (Imperva, 2021).

Figura 2. 9

Ciclo de vida de los ataques de ingeniería social.



Nota. Adaptado de *Social Engineering, Attack Techniques & Prevention Methods*, de Imperva, 2021, Página web de investigación.

PARTE II APORTACIONES

CAPÍTULO 3

ESTUDIO Y APORTACIONES

3.1. Análisis de vulnerabilidades de ciberseguridad ocurridos en la última década

A lo largo de la última década, se ha visto de todo. Ha habido monstruosas violaciones de datos, años de prolífico hacktivismo, multitud de operaciones de ciberespionaje, ciberdelincuencia de motivación financiera y malware destructivo que ha dejado los sistemas inutilizables.

3.1.1. Stuxnet

Stuxnet es un gusano informático desarrollado conjuntamente por los servicios de inteligencia estadounidenses e israelíes con el fin de sabotear el programa de armas nucleares de Irán, que se estaba poniendo en marcha a finales de la década de 2000. El gusano fue diseñado específicamente para destruir los equipos SCADA utilizados por el gobierno iraní en sus procesos de enriquecimiento de combustible nuclear. El ataque tuvo éxito, destruyendo equipos en varios lugares.

3.1.2. Operación Aurora

Formaba parte de una serie de ataques que más tarde se conocieron como Operación Aurora, una campaña coordinada de piratería informática llevada a cabo por los hackers militares del gobierno chino contra algunas de las mayores empresas del mundo de la época, como Adobe, Rackspace, Juniper, Yahoo, Symantec, Northrop Grumman y Morgan Stanley, entre otras.

La operación Aurora supuso un punto de inflexión en la historia de Google. Después de que Google descubriera y revelara públicamente los

ataques, la empresa decidió dejar de colaborar con el gobierno chino en la censura de los resultados de búsqueda de Google.cn, y Google acabó cerrando sus operaciones en China poco después. El ciberataque de la Operación Aurora se mencionó específicamente como una de las razones de la decisión de Google.

3.1.3. Press Release

Entre 2010 y 2015, un grupo de cinco hombres de Europa del Este hackearon varios servicios de noticias desde los que robaban comunicados de prensa que se anunciaban pronto. Fue uno de los hackeos más inteligentes de la década, el grupo utilizó la información privilegiada que obtuvo para anticiparse a los cambios en el mercado de valores y realizar operaciones que les reportaron más de 100 millones de dólares de beneficios.

3.1.4. LulzSec

Al grupo le gustaba hackear empresas de renombre y luego exhibirse por todo Internet. Su campaña "50 días de lulz" y todos los demás hackeos importantes que llevaron a cabo marcaron la tendencia de lo que se vio durante el resto de la década por parte de una serie de grupos de hackers imitadores en busca de atención, como Lizard Squad, New World Hackers, TeaMp0isoN, CWA y otros.

Sin embargo, LulzSec se mantiene por encima de todos los demás principalmente debido a su impresionante lista de objetivos hackeados, que incluye a Fox, HBGary, PBS, la CIA y Sony.

3.1.5. Shamoon

Creado en Irán, Shamoon (también conocido como DistTrack) es un malware diseñado para borrar datos, Shamoon destruyó más de 35.000 estaciones de trabajo en la red de Saudi Aramco, la compañía petrolera

nacional de Arabia Saudí, poniendo a la empresa de rodillas durante semanas.

En su momento se informó que Saudi Aramco compró la mayoría de los discos duros en su esfuerzo por reemplazar su flota de PCs destruidos, lo que hizo que los precios de los discos duros subieran durante meses, mientras los vendedores luchaban por satisfacer la demanda.

3.1.6. Flame

Descubierto por Kaspersky y vinculado al Equation Group, Flame fue descrito como la cepa de malware más avanzada y sofisticada jamás creada. Acabó perdiendo este título cuando Kaspersky encontró Regin dos años después, en 2014, pero el descubrimiento de Flame reveló la brecha técnica y de capacidades entre el ciber arsenal de Estados Unidos y el resto de las herramientas empleadas por otros grupos de estados-nación.

Un informe posterior del Washington Times afirmaba que Flame formaba parte del mismo arsenal de herramientas de hacking que Stuxnet, y que se desplegó principalmente contra Irán. El malware no se ha vuelto a ver desde entonces, pero su descubrimiento sigue considerándose hoy como un punto importante en la escalada de las operaciones de ciberespionaje en todo el mundo.

3.1.7. Snowden

Las filtraciones de Snowden son probablemente el acontecimiento de ciberseguridad más importante de la década. Dejaron al descubierto una red de vigilancia global que Estados Unidos y sus socios de los Cinco Ojos habían creado tras los atentados del 11-S.

Las revelaciones de Snowden llevaron a países como China, Rusia e Irán a crear sus propias operaciones de vigilancia y a ampliar los esfuerzos

de recopilación de inteligencia en el extranjero, lo que llevó a un aumento del ciberespionaje en su conjunto.

3.1.8. Silk Road

Silk Road fue el primer gran desmantelamiento de un mercado de la web oscura alojado en Tor para vender productos ilegales. Su desmantelamiento en 2013 mostró al mundo por primera vez que la web oscura y Tor no eran perfectos, y que el brazo de la ley podía llegar incluso a este rincón de internet, que hasta entonces se creía impenetrable. Tras el desmantelamiento de Silk Road surgieron otros mercados como setas, pero ninguno sobrevivió mucho tiempo. La mayoría de ellos salieron estafados o también acabaron siendo desmantelados por las fuerzas del orden.

3.1.9. Carbanak

Los informes sobre Carbanak (también conocido como Anunak o FIN7) mostraron por primera vez la existencia de un grupo de hackers altamente cualificados que era capaz de robar dinero directamente de la fuente, es decir, los bancos.

Los informes de Kaspersky Lab, Fox-IT y Group-IB mostraron que el grupo Carbanak era tan avanzado que podía penetrar en la red interna de los bancos, permanecer oculto durante semanas o meses y, a continuación, robar enormes cantidades de dinero, ya sea a través de transacciones bancarias SWIFT o cobros coordinados en cajeros automáticos. En total, se cree que el grupo ha robado más de 1.000 millones de dólares de los bancos hackeados, una cifra que aún no ha sido igualada por ningún otro grupo.

3.1.10. Heartbleed

La vulnerabilidad Heartbleed en OpenSSL permitía a los atacantes recuperar claves criptográficas de servidores públicos, claves que podían utilizar para descifrar el tráfico o autenticarse en sistemas vulnerables.

Fue explotado a los pocos días de ser revelado públicamente, y condujo a una larga cadena de hackeos en 2014 y más allá, ya que algunos operadores de servidores no parchearon sus instancias de OpenSSL, a pesar de las repetidas advertencias. En el momento en que se hizo público, se creía que alrededor de medio millón de servidores de Internet eran vulnerables, un número que tardó años en ser derribado.

3.1.11. Ashley Madison

La filtración tuvo lugar en julio de 2015, cuando un grupo de hackers que se autodenomina Impact Team divulgó la base de datos interna de Ashley Madison, un sitio web de citas que se promociona como un lugar para tener una aventura.

La brecha de Ashley Madison, que expuso los trapos sucios de muchas personas como ninguna otra brecha lo había hecho. Los usuarios registrados en el sitio se enfrentaron a intentos de extorsión, y algunos se suicidaron después de que se descubriera públicamente que tenían una cuenta en el sitio. Se trata de uno de los pocos incidentes de ciberseguridad que han conducido directamente a la muerte de alguien.

3.1.12. Anthem y OPM

Ambos hackeos fueron revelados en 2015 (Anthem en febrero y la Oficina de Administración de Personal de Estados Unidos OPM en junio) y fueron llevados a cabo por hackers chinos respaldados por el gobierno de Pekín. Robaron 78,8 millones de registros médicos de Anthem y 21,5 millones de registros de trabajadores del gobierno estadounidense.

Los dos son los principales de una serie de hackeos que el gobierno chino perpetró contra los Estados Unidos, con el propósito de reunir información de inteligencia. Los hackeos señalaron el ascenso de China como actor de amenazas en el escenario global, tan sofisticado y avanzado como Estados Unidos y Rusia.

3.1.13. SIM swapping

El SIM swapping es una táctica en la que los hackers llaman a una compañía de telefonía móvil y engañan a los operadores de telefonía móvil para que transfieran el número de teléfono de la víctima a una tarjeta SIM controlada por el atacante. La popularidad de los ataques de intercambio de tarjetas SIM aumentó cuando los hackers se dieron cuenta de que también podían utilizar esta técnica para acceder a cuentas bancarias o de criptomonedas, desde las que podían robar grandes sumas de dinero.

La técnica se ha vuelto cada vez más frecuente, siendo las empresas de telecomunicaciones estadounidenses las más susceptibles de sufrir ataques debido a su falta de voluntad para impedir que los usuarios puedan migrar los números de teléfono sin tener que acudir en persona a una de sus tiendas, como se hace en la mayor parte del mundo.

3.1.14. DD4BC

En 2015 las demandas de extorsión DDoS aparecieron. La técnica fue iniciada y popularizada por un grupo llamado DD4BC que enviaba correos electrónicos a las empresas exigiendo el pago en Bitcoin, o bien atacaban la infraestructura de la empresa con ataques DDoS y dejaban caer servicios cruciales.

Europol detuvo a los miembros de este grupo original a principios de 2016, pero el modus operandi de DD4BC fue copiado por un grupo que se hacía llamar Armada Collective, que popularizó aún más esta práctica.

3.1.15. DNC

En la primavera de 2016, el Comité Nacional Demócrata admitió que había sufrido una brecha de seguridad después de que un hacker conocido como Guccifer 2.0 empezara a publicar correos electrónicos y documentos de los servidores de la organización. A través de pruebas forenses, se descubrió

que el DNC había sido hackeado por dos grupos rusos de ciberespionaje, conocidos como Fancy Bear (APT28) y Cozy Bear (APT29). Los datos robados durante el hackeo se utilizaron en una operación de inteligencia cuidadosamente montada con el objetivo de influir en las próximas elecciones presidenciales de Estados Unidos.

3.1.16. Shadow Brokers

Entre agosto de 2016 y abril de 2017, un grupo de hackers que se autodenomina The Shadow Brokers se burló, subastó y luego filtró herramientas de hacking desarrolladas por el Equation Group, un nombre en clave de la Agencia de Seguridad Nacional (NSA) de Estados Unidos.

Estas herramientas de hacking eran de primera calidad y tuvieron un impacto inmediato. Un mes después de la última filtración de Shadow Brokers, una de las herramientas se utilizó como motor principal del brote global de ransomware WannaCry.

3.1.17. Vault7

Vault7 fue la última filtración buena de WikiLeaks. Se trataba de un conjunto de archivos de documentación que describían las armas cibernéticas de la CIA. Nunca se incluyó el código fuente; sin embargo, la filtración proporcionó una mirada a las capacidades técnicas de la CIA, algunas de las cuales incluían herramientas para hackear iPhones, todos los principales sistemas operativos de escritorio, los principales navegadores e incluso televisores inteligentes. En ese momento, WikiLeaks dijo que había recibido los datos de Vault7 de un informante, que más tarde fue identificado como Joshua Adam Schulte.

3.1.18. MongoDB

Conocido informalmente como el Apocalipsis de MongoDB, comenzó a finales de diciembre de 2016, pero cobró fuerza en enero del año siguiente,

con hackers que accedían a las bases de datos, borraban su contenido y dejaban notas de rescate, pidiendo criptomonedas para devolver los datos (inexistentes).

La primera oleada de ataques tuvo como objetivo servidores MongoDB expuestos, pero los hackers se extendieron posteriormente a otras tecnologías de bases de datos como MySQL, Cassandra, Hadoop, Elasticsearch, PostgreSQL y otras.

3.1.19. Gnosticplayers

El hacker que se hizo famoso en 2019 es Gnosticplayers. Siguiendo el modus operandi de Peace_of_Mind y Tessa88 de 2016, Gnosticplayers hackeó empresas y comenzó a vender sus datos en los mercados de la web oscura.

Entre las empresas a las que Gnosticplayers robó sus datos y luego los puso a la venta en línea se encuentran Canva, Gfycat, 500px, Evite y muchas otras. En total, el hacker se responsabilizó de más de 45 hacks y brechas que afectaron a más de mil millones de usuarios.

3.1.20. CapitalOne

El hackeo de Capital One que se dio a conocer en julio de 2019 afectó a más de 100 millones de estadounidenses y seis millones de canadienses. Los datos de la brecha no han sido compartidos públicamente en masa, por lo que la mayoría de los usuarios que tuvieron sus datos robados son probablemente seguros.

Sin embargo, la brecha destaca por la forma en que se produjo. Una investigación reveló que el sospechoso detrás del hackeo era un ex empleado de Amazon Web Services, que está acusado de acceder ilegalmente a los servidores AWS de Capital One para recuperar los datos, junto con los datos de otras 30 empresas.

3.2. Grandes ciberataques ocurridos en todo el mundo con daños colaterales en el Ecuador

3.2.1. WannaCry

WannaCry es un tipo de ataque de ransomware que se desarrolló en la primavera de 2017 y que llevó la idea de las amenazas de ransomware a la corriente principal.

Este ataque global inutilizó muchos sistemas, incluidos los de servicio público, como los que dan soporte a los hospitales y a las fuerzas del orden. Los expertos clasificaron WannaCry como un criptogusano. La comunidad de seguridad respondió con un "kill switch" y parches que detuvieron en gran medida la infección de los ordenadores con WannaCry.

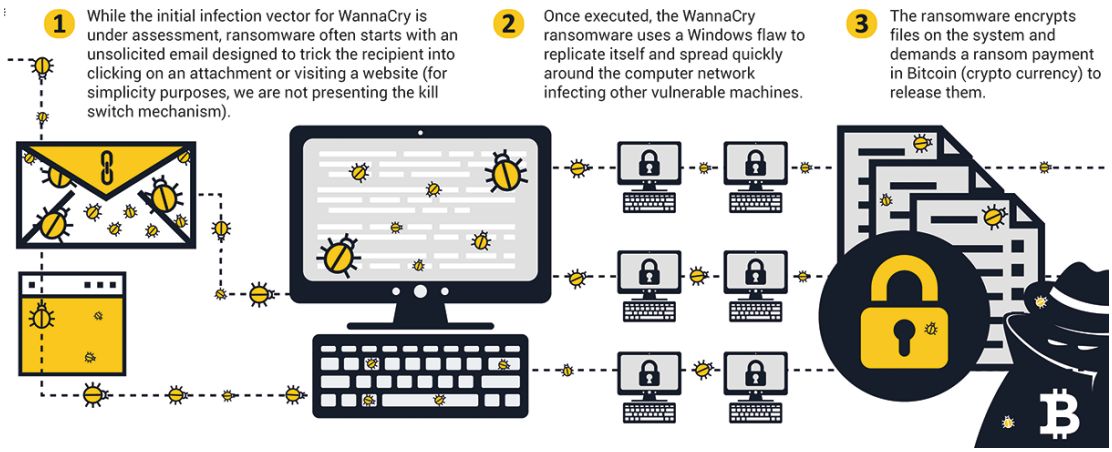
WannaCry suele comenzar con un correo electrónico no solicitado, diseñado para engañar al destinatario para que haga clic en un archivo adjunto o visite un sitio web.

Una vez ejecutado, el ransomware WannaCry utiliza un fallo de Windows para replicarse y propagarse rápidamente por la red informática infectando otras máquinas vulnerables. El ransomware cifra los archivos del sistema y exige el pago de un rescate en Bitcoin (criptomoneda) para liberarlos como se muestra en la figura 3.1.

En Ecuador, los sensores del sistema informático comenzaron a detectar amenazas. En las pantallas de los laboratorios se podía ver cómo el virus aparecía en Europa y se extendía a América Latina. Los mapas identificaban ciudades como Quito, Guayaquil y Manta con puntos rojos. Esto significaba que el virus había intentado penetrar en cuentas personales y corporativas para apoderarse de los ordenadores. Dmitry Bestuzhev, de la empresa de seguridad Kaspersky, advirtió que Ecuador es el tercer país de la región más afectado por WannaCry. México y Brasil fueron los primeros países afectados (Sandoval, 1d. C.).

Figura 3. 1

Funcionamiento del Ransomware WannaCry.



Nota. Adaptado de *Wannacry Ransomware*, de Europol, 2017, Página web de investigación.

3.2.2. Duqu 2.0

Duqu 2.0 es una versión de un malware del que se informó en 2015 que había infectado ordenadores en hoteles de Austria y Suiza que eran sedes de las negociaciones internacionales con Irán sobre su programa nuclear y las sanciones económicas.

Se cree que el malware, que infectó a Kaspersky Lab durante meses sin su conocimiento, es obra de la Unidad 8200. El New York Times alega que esta filtración de Kaspersky en 2014 es lo que permitió a Israel notificar a Estados Unidos la colaboración de Kaspersky con el FSB.

Kaspersky descubrió el malware y Symantec confirmó esos hallazgos. El malware es una variante de Duqu, y Duqu es una variante de Stuxnet. El software utilizó tres exploits de día cero, y habría requerido una financiación y una organización acordes con una agencia de inteligencia gubernamental.

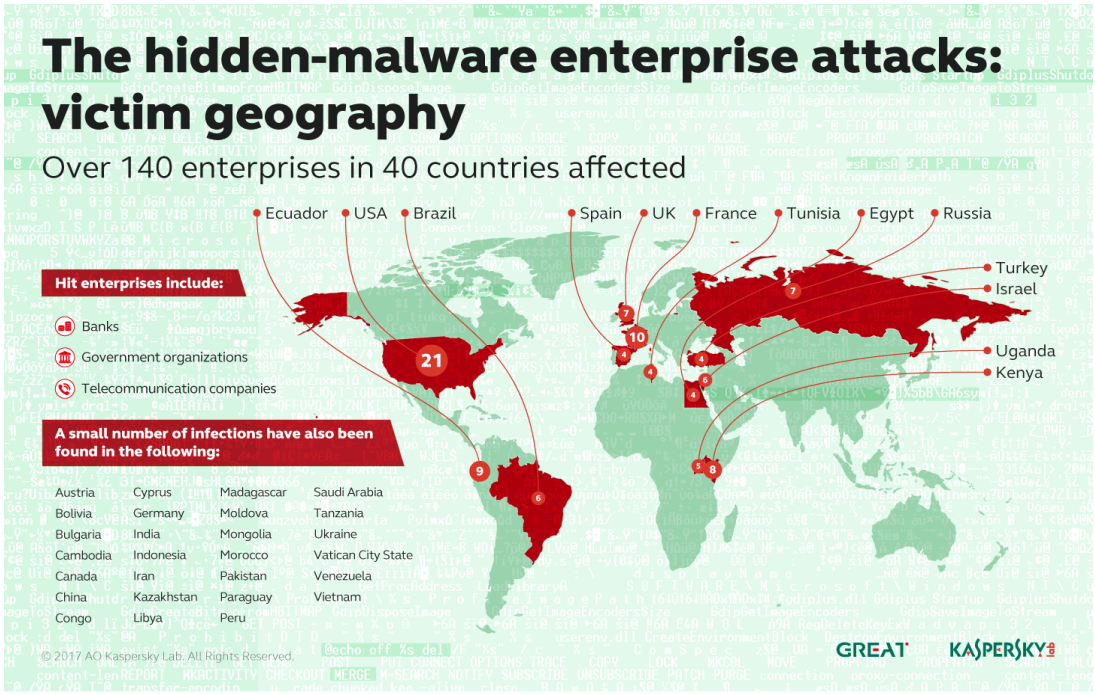
Según Kaspersky, "la filosofía y la forma de pensar del grupo "Duqu 2.0" está una generación por delante de todo lo visto en el mundo de las amenazas persistentes avanzadas". Duqu 2.0 es una plataforma de malware muy sofisticada que explota hasta tres vulnerabilidades de día cero con infecciones vinculadas a los eventos del P5+1 y a los lugares de reunión de alto nivel entre

líderes mundiales. Los ataques incluían algunas características únicas e inéditas, como que el código sólo existía en la memoria operativa. Casi no dejaba rastros. La filosofía y la forma de pensar del grupo "Duqu 2.0" está una generación por delante de todo lo visto en el mundo de las amenazas persistentes avanzadas.

Según la empresa de seguridad, las 140 organizaciones que se han visto afectadas son de 40 países diferentes, siendo Estados Unidos, Francia, Ecuador, Kenia y Reino Unido los cinco países más afectados. En Ecuador hay al menos 9 instituciones, según la figura 3.2 (ElUniverso, 2017).

Figura 3. 2

Estudio de países afectados por el malware oculto.



Nota. Adaptado de *Kaspersky detectó malware que ha infectado bancos de todo el mundo, entre esos de Ecuador*, de ElUniverso, 2017, Página web de noticias.

3.3. Estudio de ciberataques acontecidos en Ecuador

La figura 3.3. presenta la evolución de los incidentes de seguridad relacionados con el malware desde 2009 hasta 2016 en América Latina. Es evidente que en los últimos años una tendencia creciente, en gran parte debido a la cantidad de códigos maliciosos que se desarrollan actualmente,

los métodos utilizados para su propagación y las ganancias económicas obtenidas por los ciberdelincuentes que los desarrollan y/o financian.

Ecuador ha sido víctima de la ciberdelincuencia durante un período considerable de tiempo y cada vez es más evidente que esta amenaza supera las capacidades del país. La ciberdelincuencia en Ecuador comenzó a ser tratada como una amenaza seria en el año 2009, registrándose 3.143 casos en los cinco años siguientes; sin embargo, se estima que el 80% de los ciberdelitos no son denunciados (ElUniverso, 2019).

El martes 17 de septiembre de 2019, el Gobierno de Ecuador anunció que había sido víctima del cibercrimen al filtrarse los datos de seis entidades públicas por una brecha de seguridad. Según la BBC, un equipo de investigadores de vpnMentor, firma especializada en información sobre Redes Piratas Virtuales y privacidad en Internet, descubrió que se había filtrado la información de unos veinte millones de ecuatorianos. Esta cifra supera en cuatro millones a la población total de Ecuador, lo que significa que también se filtró información de personas fallecidas. La información contenía datos sensibles de carácter personal, familiar, laboral y de vehículos, que podrían ser utilizados por los ciberdelincuentes para cometer diversos delitos. Los datos tienen dos orígenes, el público y el privado. Sin embargo, la mayor parte de la información robada fue adquirida del Instituto Ecuatoriano de Seguridad Social y del Registro Civil de Ecuador (BBC, 2019).

El contenido robado del Registro Civil, la Dirección de Impuestos Internos, la Secretaría de Educación Superior, el Instituto Ecuatoriano de Seguridad Social, el Banco del Instituto Ecuatoriano de Seguridad Social; los investigadores creen que las bases de datos fueron robadas o compradas ilegalmente a exfuncionarios públicos que trabajaban en algunas de las seis entidades públicas mencionadas.

El 74% de las entidades públicas ecuatorianas aún no cuentan con el aparato de seguridad que la Organización Internacional de Normalización considera necesario para evitar ciberataques. Asimismo, según el Índice

Global de Ciberseguridad 2018, Ecuador ocupa la posición 98 de 175 naciones. Esto demuestra que Ecuador tiene un nivel medio de compromiso hacia la participación en programas e iniciativas de ciberseguridad para enfrentar las amenazas cibernéticas. Ecuador es uno de los pocos países de la región que aún no ha desarrollado un proyecto de ley de protección de datos (Espinosa, 1d. C.).

En 2019 Ecuador sufrió la mayor fuga de información de su historia. Además, el Gobierno ecuatoriano anunció que se ha enviado a la Asamblea Nacional un proyecto de ley en materia de protección de datos que pretende apoyar el Código Penal Integral de Ecuador en materia de ciberdelitos y que se han destinado 11 millones de dólares para la protección de datos de Ecuador (Jara, 1d. C.).

En base a los datos estadísticos del informe de seguridad de países de habla hispana de ESET seguridad a nivel de países de habla hispana en Latinoamérica, mostrados en la Figura 3.4., se distingue que Ecuador ocupa el quinto lugar entre los países, donde sus empresas fueron víctimas de algún tipo de malware en 2016, mientras que ocupa el primer lugar en la recepción de ataques de phishing, muy por encima de otros países en el mismo año, como se muestra en la Figura 3.5.

Las características de la era tecnológica moderna hacen que la ciberdelincuencia se considere una amenaza asimétrica, especialmente para los países poco desarrollados en materia técnica como Ecuador.

Las herramientas con las que cuenta Ecuador no son suficientes para defenderse, cuando la información se filtra es poco probable que se recupere, y para los investigadores es casi imposible determinar los autores de los ciberdelitos.

La continua amenaza de la ciberdelincuencia requiere que el gobierno ecuatoriano implemente una respuesta adaptable para proteger la información de su población.

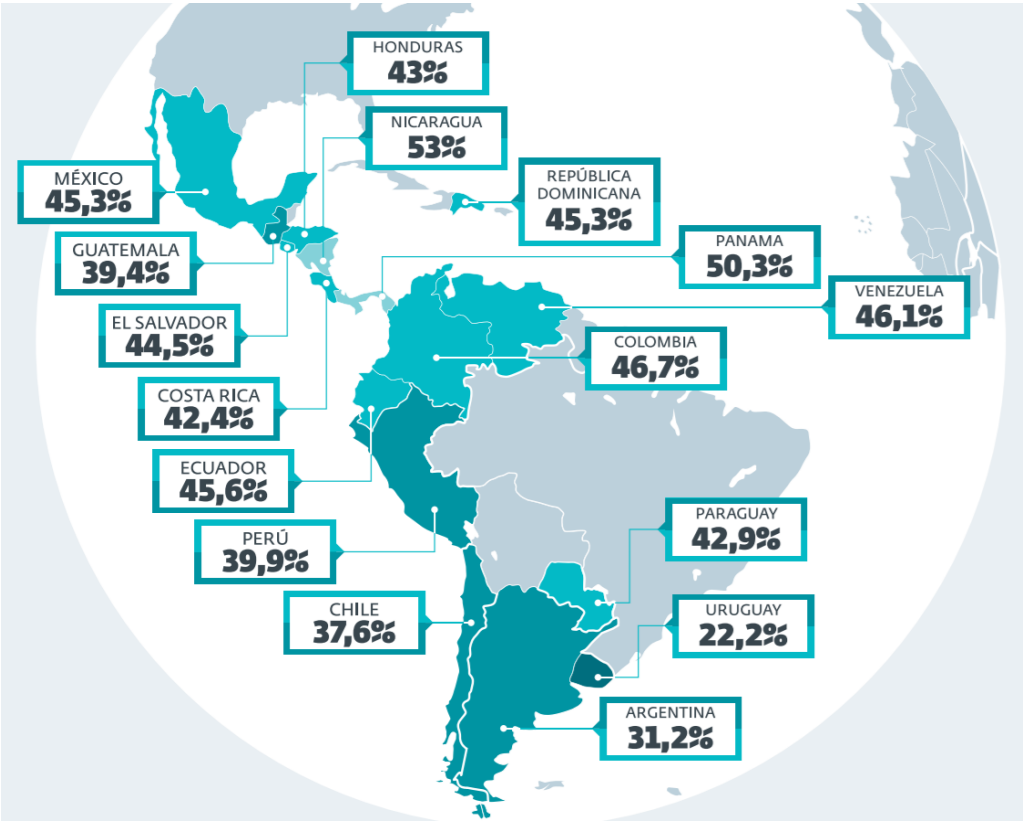
Figura 3. 3

Comparativa de malware en América Latina (2009-2016).

Nota. Adaptado de *ESET Security Report Latinoamérica 2017*, de ESET, 2017, Documento de investigación.

Figura 3. 4

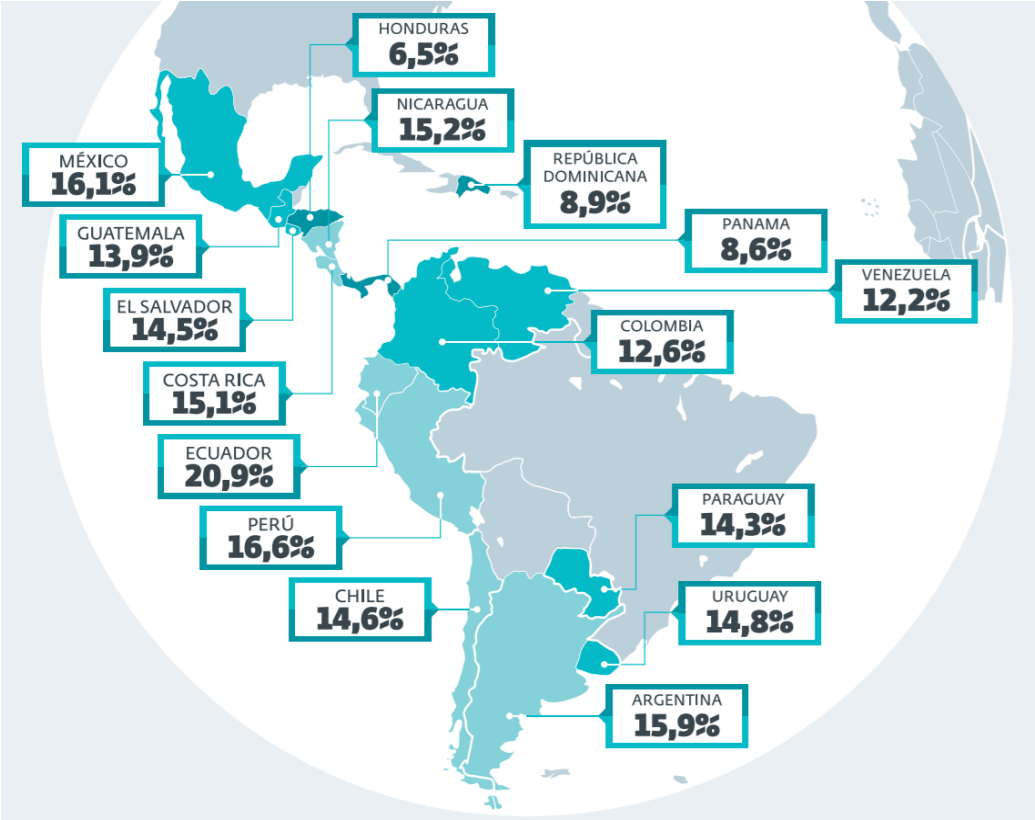
Comparativa de Infecciones de malware (2016).



Nota. Adaptado de *ESET Security Report Latinoamérica 2017*, de ESET, 2017, Documento de investigación.

Figura 3. 5

Comparativa de Infecciones de phishing (2016).



Nota. Adaptado de *ESET Security Report Latinoamérica 2017*, de ESET, 2017, Documento de investigación.

3.4. Análisis de vulnerabilidades de ciberseguridad en Instituciones educativas durante la pandemia del Covid-19

Los ciberataques han golpeado a las escuelas y universidades más que a cualquier otra industria durante la pandemia. En 2020, el ataque medio de ransomware costó a las instituciones educativas 2,73 millones de dólares.

Esto supone 300.000 dólares más que el siguiente sector más afectado: las empresas de distribución y transporte. Entre el 14 de agosto y el 12 de septiembre de 2021, las organizaciones educativas fueron el objetivo de más de 5,8 millones de ataques de malware, o el 63% de todos los ataques de este tipo. Solo los ataques de ransomware afectaron globalmente al 44% de las instituciones educativas. Existen algunas formas importantes de que los ciberdelincuentes ataquen a las escuelas, colegios y universidades.

3.4.1. Dispositivos inseguros

Los dispositivos que se prestaron a los estudiantes durante la pandemia suelen carecer de actualizaciones de seguridad. Una de estas vulnerabilidades puede permitir a los piratas informáticos obtener privilegios de nivel superior en un sistema o una red, lo que puede utilizarse para robar datos e instalar malware. A medida que los estudiantes, profesores y administradores regresan a la escuela con dispositivos que no han sido parcheados en un tiempo, es probable que un gran número de dispositivos vulnerables se vuelvan a conectar a las redes escolares.

3.4.2. Personal de ciberseguridad distraído

El cambio a la enseñanza a distancia también ha distraído la atención del limitado personal de ciberseguridad de importantes cuestiones de seguridad. En al menos un caso, las personas responsables de la ciberseguridad fueron asignadas a investigar el mal comportamiento en línea, como los insultos, que los profesores y administradores manejaban antes.

3.4.3. Víctimas propensas a cumplir

En 2020, 77 ataques de ransomware a escuelas y universidades de Estados Unidos afectaron a más de 1,3 millones de estudiantes y provocaron 531 días de inactividad. Se estima que este tiempo de inactividad costó 6.600 millones de dólares en términos económicos. El impacto económico se basó en un coste medio estimado de 8.662 dólares por minuto. Algunos ciberataques durante la pandemia cerraron completamente los principales distritos escolares durante muchos días.

Al mismo tiempo, las escuelas públicas se enfrentaron a la presión política y social para garantizar el acceso de los estudiantes a las oportunidades de aprendizaje durante la pandemia. La presión para restaurar rápidamente las redes puede hacer que las víctimas se desesperen y estén dispuestas a cumplir con las exigencias de los delincuentes.

3.4.4. Plataformas vulnerables

Cuando la pandemia obligó a las escuelas a utilizar plataformas en línea para impartir clases y evaluar a los estudiantes, creó nuevos puntos de entrada para que los ciberdelincuentes los atacaran.

Estas plataformas incluyen programas de videochat como Zoom y Microsoft Teams, así como proveedores de planes de estudio, tecnología y servicios, como K12, recientemente renombrado como Stride.

También incluyen servicios de evaluación en línea, como ProctorU y Proctorio. En conjunto, estas plataformas fueron el blanco de tres cuartas partes de las violaciones de datos en los distritos escolares que involucraron información personal.

En noviembre de 2020, el proveedor de educación en línea K12 informó de que la información de algunos estudiantes en su sistema podría haber sido robada durante un ataque de ransomware, aunque la empresa pagó el rescate.

3.4.5. Oportunidades de cebo

Los ciberdelincuentes recurrieron cada vez más a los ataques de ingeniería social durante la pandemia. Se trata de ataques en los que los ciberdelincuentes utilizan apelaciones emocionales a cosas como el miedo, la compasión o la excitación para provocar que la gente proporcione información sensible.

El miedo y la incertidumbre hacen que los individuos sean más susceptibles a los ataques de ingeniería social. Un análisis de 3,5 millones de ataques de ingeniería social entre junio y septiembre de 2020 reveló que más de 1.000 escuelas y universidades fueron el objetivo. Además, las instituciones educativas tenían más del doble de probabilidades que otras instituciones de ser víctimas de estos ataques.

3.5. Ciberseguridad en la educación del Ecuador

En 2020, debido a la pandemia del Covid-19 se ha incrementado el empleo de apps para educación virtual y videollamadas. Esto aceleró el traslado de la educación presencial a la educación virtual, por lo que Senescyt implementó plataformas tecnológicas (IES) y acceso a dispositivos tecnológicos para los estudiantes.

Esto trae consigo peligros al acceder a recursos virtuales, por esta razón la Asociación Ecuatoriana de Ciberseguridad (AECI), efectuó un estudio donde se descubrió que en Ecuador uno de los principales problemas es la falta de gestión de la ciberseguridad en las instituciones educativas; aun así, Ecuador ha alcanzado cierta madurez en materia de ciberseguridad, debido a que ha entendido que uno de los mejores recursos son los usuarios capacitados en ciberseguridad. El gobierno además contribuye a la seguridad en redes de telecomunicaciones. Debido a esto, se quiere correlacionar a los usuarios de Ecuador con la información, los servicios y la participación electrónica segura (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018).

3.6. Métodos y prácticas de ciberseguridad aplicables en instituciones privadas y públicas

La ciberseguridad debe ser una preocupación para cada empleado de la institución, no sólo para los profesionales y los altos directivos. Las políticas de ciberseguridad establecen las normas de comportamiento para actividades como el cifrado de los archivos adjuntos al correo electrónico y las restricciones en el uso de diferentes programas ajenos.

Las políticas de ciberseguridad son importantes debido a que los ciberataques y los robos de datos son potencialmente costosos. Los empleados suelen compartir contraseñas, utilizar aplicaciones no aprobadas anteriormente y no se encargan de cifrar archivos sensibles. La mejora de las

políticas de ciberseguridad puede ayudar a los empleados y consultores a entender mejor cómo mantener la seguridad de los datos y las aplicaciones.

3.6.1. Introducción

Este tipo de políticas son especialmente críticas en las instituciones públicas. Estas organizaciones corren el riesgo de recibir grandes sanciones si sus procedimientos de seguridad se consideran inadecuados.

Incluso las pequeñas instituciones deben cumplir unas normas mínimas de seguridad informática o podrían ser procesadas por un ciberataque que provoque la pérdida de datos de los clientes.

Las políticas de ciberseguridad también son fundamentales para la imagen pública y la credibilidad de una institución. Los clientes, socios y posibles empleados quieren pruebas de que la organización puede proteger sus datos sensibles. Sin una política de ciberseguridad, una institución puede no ser capaz de proporcionar esa evidencia.

Los procedimientos de ciberseguridad explican las normas sobre cómo los empleados, miembros de la junta directiva y otros usuarios finales acceden a las aplicaciones en línea y a los recursos de Internet, envían datos a través de las redes y practican una seguridad responsable.

Normalmente, la primera parte de una política de ciberseguridad describe las expectativas generales de seguridad, las funciones y las responsabilidades en la organización.

3.6.2. Información institucional

Se la utiliza en las operaciones de la institución para el cumplimiento de los objetivos de esta, se procesa en medios físicos, digitales y/o otro componente que se considere un activo y que se necesite para cumplir con

los compromisos legales y responsabilidades de la institución. El personal debe cumplir con lo siguiente:

- Serán responsables de la confidencialidad, la integridad, la fiabilidad y la disponibilidad de la información que usen.
- No está permitido facilitar información de la institución a terceros sin autorización.
- Cuando abandone sus servicios, deberá entregar la información completa resultante del trabajo elaborado.
- Una vez acabada la relación, se compromete a no utilizar, vender o divulgar la información conocida durante el desempeño de sus ocupaciones.
- Si se detecta un uso indebido de la información, el personal está obligado a reportar el incidente al departamento correspondiente.
- Cada área clasificará la información según su nivel de importancia y deberá informarla al administrador correspondiente.
- El personal, deberá realizar copias de seguridad de la información generada, en función de su importancia y frecuencia de modificación.
- El personal deberá realizar copias de seguridad de los datos que se guarden en unidades extraíbles y almacenarlos en un lugar seguro.

3.6.3. Clasificación de datos

La información contenida en bases de datos del sistema puede ser clasificada como confidencial o no, y la institución será la única encargada de clasificar la información.

La máxima autoridad está obligada de aprobar la clasificación de la información y establecer el nivel de seguridad adecuado para su correcta protección, la Tabla 3.1. muestra los niveles de seguridad de la información de la institución clasificados por colores.

Tabla 3. 1

Niveles de seguridad de la información.

Nivel	Definición	Ejemplo
Verde	Aquella información ausente de valor comercial o administrativo, la cual podría desecharse.	✓ Ficheros personales carentes de relación con la institución.
Amarillo	Aquella información no confidencial usada en los distintos departamentos de la institución, maniobrada por operarios sin ocupaciones de supervisión para sus diligencias profesionales.	✓ Documentos temporales o borradores. ✓ Ficheros personales relacionados con la institución.
Naranja	Aquella información confidencial usada en los distintos departamentos de la institución, maniobrada por operarios con ocupaciones de supervisión para sus diligencias profesionales.	✓ Presupuestos. ✓ Informes de ventas. ✓ Configuraciones a corto plazo.
Rojo	Aquella información confidencial la cual no debe ser expuesta a personal ajeno a la institución. Inclusive dentro de la institución el acceso se encuentra restringido, solo puede acceder la máxima autoridad.	✓ Contraseñas ✓ Contratos ✓ Registro de actividades dentro de la institución.

Nota. Adaptado de Elaboración propia.

3.6.4. Uso de sistemas informáticos

La mayor parte de las instituciones se basa en sus sistemas informáticos, por lo que éstos deben ser capaces de responder en cualquier situación, y a veces en cualquier momento del día.

La monitorización de estos sistemas se ha convertido en una tarea fundamental para gestionar toda la infraestructura informática de una institución, con los siguientes objetivos principales:

- Aprovechar al máximo los recursos de una empresa.
- Prevención de incidencias y detección de problemas.

- Notificación de posibles problemas.

Las herramientas de monitorización del sistema deben centrarse en los procesos, la memoria, el almacenamiento y las conexiones de red. Además de contar con una buena herramienta de monitorización, se debe establecer un protocolo de resolución de problemas, que será clave para solucionarlos de la mejor manera posible. Monitorizar sistemas no es tan complicado como parece. La prioridad es el orden y la disciplina.

A continuación, se muestran los pasos a seguir para realizar una monitorización del sistema que sea eficiente y completa:

- Realizar un análisis completo del sistema sobre los dispositivos que queremos monitorizar.
- Se debe reunir las diferentes partes responsables en las principales áreas de una instalación.
- Definir las principales alarmas, para cada tipo de componente, elemento y marca definidos en el primer paso.
- Para cada una se debe que definir unos umbrales con los parámetros y niveles correspondientes para lanzar la alarma.
- Establecer el protocolo de comunicación y actuación. Definir los canales de comunicación y cómo será el proceso de atención de alarmas.
- Hacer una comparación entre diferentes herramientas de monitorización y elegir la que mejor se adapte al presupuesto y a los requisitos establecidos en los pasos anteriores. Es primordial que la herramienta elegida sea capaz de monitorizar los elementos más prioritarios del inventario inicial.
- Redactar un plan de instalación del nuevo sistema de monitorización. Para ello se debe mantener las medidas de seguridad existentes, minimizar el número de sistemas intermedios que se interponen entre el sistema de supervisión y los sistemas de importancia crítica, minimizar el impacto en el

sistema a estudiar e instalar y configurar el paquete de software elegido.

3.7. Control de acceso a recursos

El control de acceso es una valiosa técnica de seguridad que puede utilizarse para regular quién o qué puede ver o utilizar un recurso determinado.

En un entorno de seguridad informática, esto podría traducirse en quién puede acceder y editar un archivo concreto, qué tipos de equipos pueden utilizarse o quién puede acceder a determinados dispositivos.

El objetivo final del control de acceso es proporcionar un nivel de seguridad que minimice el riesgo para la institución, ayudando a mantener seguros los edificios, los datos y a las personas.

Por ello, el control de accesos va de la mano de la seguridad informática y debería ser una consideración clave para todos los propietarios de las instituciones.

Sin un control de acceso adecuado, se podría dejar al personal y a la institución expuestos a problemas como la pérdida de datos, el robo o el incumplimiento de las leyes de privacidad y protección de datos.

Este control de acceso se realizado a partir del uso de una ID para iniciar sesión y una contraseña.

3.7.1. Acceso de personal no autorizado

El personal con acceso a la red tendrá un ID y una contraseña única para acceder al sistema.

La contraseña será confidencial, salvo que lo exija una autoridad superior.

El personal deberá cumplir las siguientes normas relativas a la creación y mantenimiento de contraseñas:

- No deberán coincidir con ninguna palabra del diccionario, en español o cualquier idioma.
- No establecer contraseñas en las inmediaciones del área de trabajo.
- Deberán cambiarse cada 60 días o según establezca la máxima autoridad.
- Las cuentas se bloquearán tras el 3 intento fallido al iniciar sesión y se suspenderán inmediatamente después de 30 días sin utilizarse.
- Al olvidar la contraseña se notificará al departamento correspondiente para adquirir una nueva contraseña.
- El personal no está autorizado a acceder, copiar, leer, borrar o modificar las contraseñas, le corresponde al departamento de seguridad de la red.
- Los usuarios que requieran iniciar sesión como administradores del sistema deben pedir una cuenta de acceso especial.
- El ID y la contraseña del personal despedido serán desactivados tan pronto como sea posible.
- Se deberá notificar a la máxima autoridad cuando se produzca un cambio en los privilegios de acceso.
- El personal se responsabilizará del intercambio de información durante los inicios de sesión, otros usuarios no pueden utilizar la unidad mientras la sesión esté activa.

3.7.2. Acceso de administradores de sistemas

Los administradores tendrán este privilegio, aunque mantendrán otros accesos que sean necesarios para cumplir con sus compromisos laborales. Las contraseñas de los administradores deberán ser cambiadas inmediatamente cuando dejen de serlo.

3.7.3. Acceso especial temporal

Se proporcionarán cuentas de acceso temporal al personal que necesite privilegios de administrador para desempeñar sus funciones.

Se hará un seguimiento de las acciones realizadas por estas, creando informes que indiquen al personal el motivo y el tiempo de uso.

Estas cuentas expirarán después de 72 horas y no se renovarán sin permiso.

3.7.4. Acceso de terceros

Se garantizará una conectividad segura entre la institución y un tercero que requieran intercambiar información, por lo tanto, este tipo de conexión sólo se permitirá para fines empresariales.

La institución ajena garantizará que sólo personal autorizado pueda tener acceso a la información, cumpliendo con lo siguiente:

- Se terminará con la conexión si no cumple con las normas de autenticación de la institución ajena.
- En caso de que las conexiones con terceros no cumplan los requisitos se rediseñarán según se crea conveniente.
- Las solicitudes de conexión con terceros se realizarán únicamente si la institución aprueba la solicitud.
- Los recursos tecnológicos ajenos a la institución deberán garantizar su funcionamiento dentro de las instalaciones, para ello se firmará un acuerdo entre las partes.
- Los recursos tecnológicos usados que sean propiedad de la institución serán gestionados por el área técnica de la institución propietaria.

- La conexión con terceros debe ser aprobada por el área encargada de la seguridad de red, para no comprometer la seguridad de los datos.
- Se finalizará la conexión con terceros que no cumplan con los requisitos internos previamente establecidos.

3.7.5. Acceso de dispositivos autorizados

Sólo los dispositivos autorizados podrán conectarse a la red de la institución. Estos deben ser propiedad de esta y no se permitirá a otros usuarios vincular dispositivos particulares a la red.

3.7.6. Acceso remoto no autorizado

El acceso no autorizado se produce cuando un usuario intenta acceder a un área del sistema a la que no debería acceder. Al intentar acceder a esa área, se le negará el acceso. Los administradores de sistemas configurarán alertas para que les avisen cuando hay un intento de acceso no autorizado, de modo que puedan investigar el motivo. Estas alertas ayudarán a impedir que los hackers accedan a un sistema seguro o confidencial. Muchos sistemas seguros también pueden bloquear una cuenta con demasiados intentos de acceso fallidos.

Está estrictamente prohibido que el personal instale, bajo cualquier circunstancia, software externo creado para suministrar acceso remoto a los activos de TI sin autorización previa, ya que este elude los métodos de acceso autorizados y compone una amenaza para la ciberseguridad de la institución.

3.7.7. Acceso remoto autorizado

Únicamente los usuarios autorizados pueden acceder remotamente a los activos informáticos, con la debida supervisión. Se suministrará a usuarios que necesiten intercambiar información, copiar documentos y usar

aplicaciones. Se realizará a través de una aplicación o servicio que sea fidedigno, usando una ID y una contraseña determinada anteriormente.

3.8. Ciberseguridad en comunicación

La comunicación es la clave del éxito de una estrategia de seguridad institucional. Sin embargo, la complejidad de las personas y organizaciones involucradas puede llegar a ser abrumadora si no se incorpora a un programa de seguridad completo.

- El direccionamiento interno, las topologías y la información afín con los sistemas de comunicación, ciberseguridad e informática de la empresa se considerarán información confidencial.
- Una red de amplia cobertura deberá estar dividida en distintos segmentos de red, con sus correspondientes controles de seguridad.
- Las conexiones de terceros que accedan a la red interna deberán ser examinadas por cifrado y descifrado, verificación de datos y autenticación de usuarios.
- El intercambio de información electrónica con terceros debe estar justificada por escrito.
- La información confidencial que se transmita a través de las redes de la institución deberá estar encriptada.
-

3.9. Software implementado

El software se refiere a las aplicaciones, scripts y programas que se ejecutan en un dispositivo. Todos ellos proporcionan las indicaciones y los datos que los ordenadores necesitan para funcionar y satisfacer las necesidades de los usuarios. El software por utilizar en la institución se adquirirá siguiendo la normativa vigente y de acuerdo el procedimiento de adquisición, instalación y retirada de software, la descarga y uso de software no autorizado está prohibido.

Se realizarán auditorías periódicas para controlar el uso del software adquirido por la institución. El departamento administrativo, se encargará de velar por el correcto uso del software de la empresa y por la conservación de los documentos que avalan la adquisición legal. El software que se encargue de la gestión de los datos de la institución debe contar con los mecanismos más sofisticados para avalar los servicios de ciberseguridad que sean necesarios. Debe existir un inventario de las licencias de software de la empresa que permita su adecuado y control, para evitar sanciones por la instalación de software sin licencia.

3.10. Hardware implementado

Los cambios en los equipos de la institución, como sustitución o complemento de unidades, deberán ser evaluadas y autorizadas técnicamente con anterioridad, y sólo podrán ser reparados por personal acreditado. Los equipos de la institución no podrán ser trasladados sin una previa autorización.

3.11. Seguridad física

Las normas de ciberseguridad se emplearán en las áreas críticas, para controlar el acceso a la institución mediante el uso de puertas de seguridad, tarjetas inteligentes, alarmas y sistemas de CCTV en aquellas áreas consideradas críticas por la institución.

Es compromiso del personal cumplir con las siguientes medidas:

- Las áreas críticas de la institución deberán tener acceso restringido, en caso de que se requiera entrar se debe justificar adecuadamente el motivo de la entrada y deberá estar escoltado por el personal correspondiente.
- Todo el personal que ingrese a la institución debe llevar una identificación en un lugar visible.

- Todas las áreas deben estar equipados con elementos de control de inundaciones, incendios y alarmas.
- Las áreas críticas deben estar señalizadas. Las zonas restringidas deben contar con mecanismos de seguridad que sólo puedan ser operados por personal con acceso directo a estas zonas.

3.12. Plan para futura implementación para protección y prevención de ciberataques.

3.12.1. Niveles de ciberataques

Si se detecta un problema que amenace la ciberseguridad de la institución se notificará a la máxima autoridad del área responsable de gestionar la seguridad de red, la que se encargará de clasificar la amenaza de acuerdo con la tabla 3.2.

Tabla 3. 2

Niveles de amenazas de ciberseguridad en una institución.

Nivel	Descripción
Leve	Se contrarrestan con métodos comunes y conocidos.
Moderado	Es raro o difícil de detectar (fraude y estafa).
Potencial	Está programado para atacar una vulnerabilidad específica de ciberseguridad de la institución.
Alto	Son ataques globales, nacionales o dirigidos a más de una vulnerabilidad de la institución.

Nota. Adaptado de Elaboración propia.

3.12.2. Gestión de ciberataques

Después de clasificar la amenaza, se proporcionará una solución al suceso en función del tipo de amenaza correspondiente y de los activos tecnológicos en función del nivel de amenaza, tal como se muestra en la tabla 3.3.

Tabla 3. 3

Gestión de amenazas de ciberseguridad en una institución.

Nivel	Solución
Leve	La solución habitual para este tipo de acontecimientos leves es con el empleo de antimalware.
Moderado	El personal previamente capacitado en las estrategias para contrarrestar estafas y fraudes informáticos efectuará un análisis exhaustivo del software oculto en las unidades de almacenamiento, para lograr eliminarlo. Esta amenaza puede derivar en un ciberataque con daño colateral a la infraestructura informática de la institución, por lo que es obligatorio analizar si es necesario desinfectar o caso contrario aislar los equipos de la red infectada.
Potencial	Teniendo en cuenta las anteriores amenazas, se realizará una auditoría informática total, tomando como referencia los informes del CSIRT (Equipo de Respuesta a Incidentes de Seguridad), para limitar el acceso a los equipos hasta que se resuelva el problema.
Alto	Al tratarse de un ataque de esas magnitudes, no habrá conocimientos específicos para evitar o amortiguar los efectos que cause, por lo que será obligatorio reportar el suceso al CSIRT y mantener los componentes infectados aislados hasta que se apliquen las soluciones adecuadas.

Nota. Adaptado de Elaboración propia.

3.13. Actualización de políticas de ciberseguridad

El departamento encargado de gestionar la seguridad de las redes es responsable de examinar, renovar y anunciar las políticas de ciberseguridad, en caso de que se detecte alguna infracción, se deberá informar al departamento correspondiente para que determine una solución al problema.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

En base al análisis realizado en este trabajo de titulación se concluye que los ciberataques han afectado sobremanera durante la pandemia. Los dispositivos inseguros, la falta de concentración del personal, el tiempo de respuesta para restaurar las redes, las plataformas vulnerables; sumado esto al miedo y la incertidumbre de las víctimas crean oportunidades para que los ciberdelincuentes puedan aprovecharse de un sistema o una red.

De la misma forma se identificaron los métodos y prácticas de ciberseguridad para tomar las medidas adecuadas de protección. El personal deberá prestar la debida atención a la integridad de la información, la información de las bases de datos debe ser clasificada en el nivel de seguridad adecuado y los sistemas informáticos estarán en capacidad de dar una pronta respuesta en cualquier situación y en cualquier momento que amerite.

Además, se identificaron planes para una futura implementación de medidas y acciones para prevención y protección de ataques cibernéticos a instituciones educativas. Si se detecta un problema que amenace la ciberseguridad de la institución se notificará a la máxima autoridad del área responsable, esta se encargará de clasificar la amenaza y proporcionará una solución en función del tipo de amenaza y de los activos tecnológicos.

4.2. Recomendaciones

El área correspondiente realizará una evaluación de los procedimientos y políticas existentes en la institución educativa, si no cuenta con los protocolos pertinentes, los ciberdelincuentes perpetrarán fácilmente la información. Estos protocolos de la ciberseguridad se deben comparar con los

de otras instituciones similares y cuando la máxima autoridad esté segura de la trayectoria que tomará, evaluará riesgos e implementará auditorías.

En las instituciones educativas con muchos trabajadores, el departamento de sistemas debe plantear un plan de contingencia de ciberseguridad que incorpore soluciones a posibles problemas que se produzcan. En las instituciones que cuenten con menos trabajadores se cumplirá con las políticas de ciberseguridad específicas para la prevención de ciberataques.

Si la institución educativa no cuenta con equipos tecnológicos, se debe crear el presupuesto para adquirirlos. Si cuentan con los equipos, pero se adquirieron hace un tiempo considerable, se deberían remplazar por unidades nuevas; el Covid-19 ha elevado el nivel de riesgo, los dispositivos serán fundamentales para hacer frente a la mayoría de los ataques.

Se recomienda que las instituciones educativas tengan un plan de capacitación sobre ciberataques y sus objetivos principales, además determinarán las posibles debilidades informáticas de la institución para tomar las medidas correspondientes, e informar a los empleados sobre los ataques informáticos y las posibles consecuencias que pueden surgir y afectar el normal desarrollo de sus tareas.

REFERENCIAS

Almeida, C. A. T. (2019). *La ciberseguridad en el Ecuador, una propuesta de organización*. 14.

BBC. (2019, septiembre 16). Data on almost every Ecuadorean citizen leaked. *BBC News*. https://www.bbc.com/news/technology-49715478

Checkpoint. (2021). *What is Data Center Security?* Check Point Software. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-data-center/what-is-data-center-security/

Cisco. (2010). *Developing Network Security Strategies*. https://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2

Cisco. (2021). *What Is a Cyberattack? - Most Common Types*. Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Ecuador. Leyes y Reglamentos. (2014). *Codigo organico integral penal.* Ministerio de Justicia, Derechos Humanos y Cultos.

ElUniverso. (2017, febrero 11). *Kaspersky detectó malware que ha infectado bancos de todo el mundo, entre esos de Ecuador*. El Universo. https://www.eluniverso.com/vida-estilo/2017/02/10/nota/6041425/kaspersky-detecto-malware-que-ha-infectado-bancos-todo-mundo

ElUniverso. (2019, abril 15). *Ecuador ha recibido 40 millones de ataques cibernéticos, revela viceministro de Telecomunicaciones*. El Universo. https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela

ESET. (2017). *ESET Security Report Latinoamérica 2017*.

Espinosa, C. (1d. C., noviembre 30). *Ecuador ocupa el séptimo lugar en ciberseguridad en América Latina*. El Comercio. https://www.elcomercio.com/actualidad/seguridad/ecuador-ciberseguridad-region-informe-delitos.html

Europol. (2017). *Wannacry Ransomware*. Europol. https://www.europol.europa.eu/wannacry-ransomware

Fortinet. (2021). *What Is a Trojan Horse? Trojan Virus and Malware Explained*. Fortinet. https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

GeeksforGeeks. (2018, enero 23). *Hash Functions in System Security*. GeeksforGeeks. https://www.geeksforgeeks.org/hash-functions-system-security/

Georgescu, E. (2020, agosto 13). What Is Riskware? Cybersecurity Threats You Must Be Aware Of. *Heimdal Security Blog*. https://heimdalsecurity.com/blog/what-is-riskware/

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. *Journal of Cleaner Production*, *252*, 119869. https://doi.org/10.1016/j.jclepro.2019.119869

Gub. (2020). *Estadística de incidentes de Seguridad Informática 2020*. Centro Nacional de Respuesta a Incidentes de Seguridad Informática. https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas/estadistica-incidentes-seguridad-informatica-2020

Harrington, D. (2018, agosto 20). *Data Security: Importance, Types, and Solutions* | *Varonis*. Inside Out Security. https://www.varonis.com/blog/data-security/

Hussin, A. A. (2018). *Education 4.0 Made Simple: Ideas For Teaching*.

IBM. (2021, octubre 28). *IBM Docs*. https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/en/ibm-mq/7.5?topic=concepts-cryptography

Imperva. (2021). What is Social Engineering | Attack Techniques & Prevention Methods | Imperva. *Learning Center*. https://www.imperva.com/learn/application-security/social-engineering-attack/

Jara, M. (1d. C., noviembre 30). *El Gobierno de Ecuador asegura que invertirá USD 11 millones para la protección de datos, tras filtración*. El Comercio. https://www.elcomercio.com/actualidad/negocios/gobierno-ecuatoriano-proteccion-datos-ataque.html

Kaspersky. (2021a, enero 13). *What is Spear Phishing? - Definition*. Usa.Kaspersky.Com. https://usa.kaspersky.com/resource-center/definitions/spear-phishing

Kaspersky. (2021b, julio 28). *What is Spyware?* Usa.Kaspersky.Com. https://usa.kaspersky.com/resource-center/threats/spyware

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2018). *Ministerio de Telecomunicaciones y de la Sociedad de la Información*.

Nmap. (2021). *Nmap: The Network Mapper—Security Scanner*. https://nmap.org/

Popkova, E. G., Ragulina, Y. V., & Bogoviz, A. V. (Eds.). (2019). *Industry 4.0: Industrial Revolution of the 21st Century* (Vol. 169). Springer International Publishing. https://doi.org/10.1007/978-3-319-94310-7

Proofpoint. (2020, diciembre 23). *What Is Ransomware? - Definition, Prevention & More | Proofpoint US*. Proofpoint. https://www.proofpoint.com/us/threat-reference/ransomware

Puncreobutr, V. (2016). *Education 4.0: New Challenge of Learning*.

Rosenthal, M. (2018, septiembre 5). *5 types of cyber security*. Mindcore. https://mind-core.com/blogs/cybersecurity/5-types-of-cyber-security/

Sader, S., Husti, I., & Daroczi, M. (2021). A review of quality 4.0: Definitions, features, technologies, applications, and challenges. *Total Quality Management & Business Excellence*, 1–19. https://doi.org/10.1080/14783363.2021.1944082

Sandoval, C. (1d. C., noviembre 30). *El ciberataque global impactó en Ecuador*. El Comercio. https://www.elcomercio.com/actualidad/seguridad/ciberataque-wannacry-impacto-ecuador-hackeo.html

Sangfor. (2021). *The Basics of Authentication in Cyber Security*. https://secure.livechatinc.com/

Sharma, P. (2019). Digital Revolution of Education 4.0. *International Journal of Engineering and Advanced Technology*, *9*(2), 3558–3564. https://doi.org/10.35940/ijeat.A1293.129219

Techopedia. (2021a). *Event Log—Techopedia*. Techopedia.Com. http://www.techopedia.com/definition/25410/event-log-networking

Techopedia. (2021b). *What is a Masquerade Attack? - Definition from Techopedia*. Techopedia.Com. http://www.techopedia.com/definition/4020/masquerade-attack

Tenable. (2021). *Tenable®—The Cyber Exposure Company*. Tenable®. https://www.tenable.com/homepage-rotator

WeLiveSecurity. (2015, mayo 18). *¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?* WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Zambon, I., Cecchini, M., Egidi, G., Grazia Saporito, M., & Colantoni, A. (2019). *Revolution 4.0: Industry vs. Agriculture in a Future Development for SMEs*.

GLOSARIO

E-Learning: Aprendizaje electrónico.

Big-Data: Conjuntos de datos de gran variedad, se generan en grandes volúmenes y a una velocidad cada vez mayor.

TIC: Tecnologías de la Información y la Comunicación.

PLC: Controlador Lógico Programable.

TI: Tecnología de la Información.

IoT: Internet de las Cosas.

ERP: Sistema de planificación de recursos empresariales.

IPv6: Protocolo de Internet Versión 6.

DSN: Red de Suministro Digital.

SCADA: Supervisión, Control y Adquisición de Datos.

QR: Respuesta Rápida.

UTM: Gestión Unificada de Amenazas.

TTP: Terceras Partes de Confianza.

SIEM: Gestión de Eventos e Información de Seguridad.

UDP: Protocolo de Datagramas de Usuario.

CSIRT: Equipo de Respuesta a Incidentes de Seguridad.

VPN: Red Privada Virtual.

MITM: Ataque del Hombre en el Medio.

DDoS: Denegación de servicio distribuida.

CCTV: Circuito Cerrado de Televisión.

NSA: Agencia de Seguridad Nacional.

EcuCERT: Centro de Respuestas a Incidentes Informáticos.

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Vélez Armijo, Efraín Alexander** con C.C: # 092168595-4 autor del Trabajo de Titulación: **Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 7 de marzo del 2022

Efraín Vélez A.

f._____

Nombre: Vélez Armijo, Efraín Alexander

C.C: 092168595-4

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador		
AUTOR(ES)	Vélez Armijo, Efraín Alexander		
REVISOR(ES)/TUTOR(ES)	Ing. Vallejo Samaniego, Luis Vicente, M.SC.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	7 de marzo del 2022	No. DE PÁGINAS:	92
ÁREAS TEMÁTICAS:	Seguridad en redes, Sistemas telemáticos		
PALABRAS CLAVES/ KEYWORDS:	Ciberseguridad, Ciberataque, Ciberamenaza, E-Learning, Malware, Ransomware, Phishing.		

RESUMEN/ABSTRACT (150-250 palabras):

La ciberseguridad es uno de los aspectos más importantes tanto en los países desarrollados como en los que están en vías de desarrollo, ayuda a defender los datos de distintos ataques maliciosos. Estos ciberataques son uno de los mayores retos a nivel nacional y requieren de un análisis que examine los aspectos que han convertido a las acciones de estos en uno de los desafíos más grandes para las instituciones educativas tanto públicas como privadas del Ecuador. Para solucionar estas ciberamenazas, es preciso implementar diferentes políticas de ciberseguridad en los puntos clave donde se ejecutan los procesos de recepción, envío y almacenamiento de información de las instituciones que lo necesiten con el fin de proteger la confidencialidad de los datos. Los ciberataques no sólo se originan interceptando el tránsito de datos entre el emisor y el receptor, sino también ingresando desde servidores y estaciones de trabajo, donde los operadores facilitan el acceso y permiten a los atacantes ingresar a la red.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593988071452	E-mail: efrain.velez99@hotmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez, Edwin Fernando	
	Teléfono: +593-9-67608298	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	