Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ANÁLISIS GAP BASADO EN EL NIST CYBER SECURITY FRAMEWORK (CSF) Y DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA EMPRESA DE SERVICIOS EN GUATEMALA

Werner Rodrigo Solórzano Valdizón
Asesorado por MA. Ing. Aura María Chamalé Lira

Guatemala, enero de 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS GAP BASADO EN EL NIST CYBER SECURITY FRAMEWORK (CSF) Y DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA EMPRESA DE SERVICIOS EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

WERNER RODRIGO SOLÓRZANO VALDIZÓN
ASESORADO POR MA. ING. AURA MARÍA CHAMALÉ LIRA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, ENERO DE 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Ing. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIA	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
EXAMINADOR	Ing. Walter Giovanni Alvarez Marroquín
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
SECRETARIO	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS GAP BASADO EN EL NIST CYBER SECURITY FRAMEWORK (CSF) Y DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA EMPRESA DE SERVICIOS EN GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Postgrado, con fecha de 19 de noviembre de 2022.

Werner Rodrigo Solórzano Valdizón

EEPFI-PP-2185-2022
Guatemala, 19 de noviembre de 2022

Director
Armando Alonso Rivera Carrillo
Escuela De Ingenieria Mecanica Electrica
Presente.

Estimado Ing. Rivera

Reciba un cordial saludo de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

El propósito de la presente es para informarle que se ha revisado y aprobado el Diseño de Investigación titulado: **ANÁLISIS GAP BASADO EN EL NIST CYBER SECURITY FRAMEWORK (CSF) Y DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA EMPRESA DE SERVICIOS EN GUATEMALA**, el cual se enmarca en la línea de investigación: **Telecomunicaciones - Telecomunicaciones**, presentado por el estudiante **Werner Rodrigo Solórzano Valdizón** carné número **201400448**, quien optó por la modalidad del "PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO". Previo a culminar sus estudios en la Maestría en ARTES en Ingeniería Para La Industria Con Especialidad En Telecomunicaciones.

Y habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Décimo, Inciso 10.2 del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Atentamente,

"Id y Enseñad a Todos"

Aura María Chamalé Lira
Ingeniera en Sistemas de Información y Ciencias de la Computación
Colegiado No. 20551

Mtra. Aura María Chamalé Lira
Asesor(a)

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POSTGRADO
FACULTAD DE INGENIERIA
DE GUATEMALA

Mtro. Mario Renato Escobedo Martinez
Coordinador(a) de Maestría

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCIÓN
ESCUELA DE POSTGRADO

Mtro. Edgar Darío Alvaréz Cotí
Director
Escuela de Estudios de Postgrado
Facultad de Ingeniería

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIME-1795-2022

El Director de la Escuela De Ingenieria Mecanica Electrica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador y Director de la Escuela de Estudios de Postgrado, del Diseño de Investigación en la modalidad Estudios de Pregrado y Postgrado titulado: **ANÁLISIS GAP BASADO EN EL NIST CYBER SECURITY FRAMEWORK (CSF) Y DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA EMPRESA DE SERVICIOS EN GUATEMALA**, presentado por el estudiante universitario **Werner Rodrigo Solórzano Valdizón**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería en esta modalidad.

ID Y ENSEÑAD A TODOS

Ing. Armando Alonso Rivera Carrillo
Director
Escuela De Ingenieria Mecanica Electrica

Guatemala, noviembre de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.074.2023

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **ANÁLISIS GAP BASADO EN EL NIST CYBER SECURITY FRAMEWORK (CSF) Y DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) PARA UNA EMPRESA DE SERVICIOS EN GUATEMALA,** presentado por: **Werner Rodrigo Solórzano Valdizón,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, enero de 2023

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Infinitas gracias por haberme brindado entendimiento, perseverancia y fortaleza para finalizar esta etapa de mis estudios.
Mis padres	Colombia Valdizón (q. e. p. d.) y Pablo Solórzano, por todo el amor, esfuerzo, consejos y dedicación para guiarme a alcanzar este éxito a través de su ejemplo de excelencia, honradez y humildad.
Mis hermanos	Nancy, Wendy, Leyder (q. e. p. d.), Heidy, José Pablo y Luis Pedro por todo el cariño y apoyo recibido a lo largo de mis proyectos.
Mis amigos	Por compartir experiencias inolvidables y alentarme a seguir para cumplir este objetivo.
Mi familia	Por todo el cariño y apoyo siempre.

AGRADECIMIENTOS A:

Pueblo de Gutemala	Por permitirme el acceso a la educación superior.
Universidad de San Carlos de Guatemala	Por la oportunidad de pertenecer y formarme como profesional en esta casa de estudios.
Facultad de Ingeniería	Por brindarme los conocimientos necesarios para la formación académica.
Departamento de Física	Por darme la oportunidad de laborar y la confianza depositada en mí en las tareas asignadas, que me permitieron crecer como persona y profesional.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
@	Arroba
Q	Quetzales

GLOSARIO

Eficacia Relación entre un objeto hecho para realizar una función y el resultado obtenido.

Eficiencia Relación correlativa entre los recursos y el uso que se hace de ellos dentro de un proceso.

RESUMEN

En este trabajo se aborda el tema: *Análisis GAP basado en el NIST Cyber Security Framework (CSF) y diseño de un plan estratégico de seguridad de la información (PESI) para una empresa de servicios en Guatemala.* Se introduce el estudio y se presentan los antecedentes, para luego explicar lo relacionado con el planteamiento del problema y la justificación. Con base en ello, se presentan los objetivos de la investigación a desarrollar, y se abarcan también las necesidades a cubrir.

Después se desarrolla cuidadosamente el marco teórico, con los conceptos básicos sobre el tema en estudio. Luego de este apartado, se presenta el índice de contenidos, la metodología y las técnicas de análisis de la información recabada, teniendo en cuenta, además, el cronograma y los aspectos que hacen factible el trabajo. Por último, se presentan las referencias consultadas.

1. INTRODUCCIÓN

En los últimos años, el avance de la tecnología ha sido significativo respecto a los avances a lo largo de la historia, sobre todo con la creación de dispositivos inteligentes conectados a través del Internet. En un mundo cada vez más sofisticado, casi cualquier actividad, servicio o producto está relacionado a Internet. Esto implica que hay un intercambio continuo de información y que, tanto información como usuario final, son vulnerables a algún tipo de amenaza digital.

En ese sentido, la ciberseguridad es un esfuerzo continuo de proteger individuos, organizaciones y gobiernos de ataques cibernéticos, protegiendo sus sistemas e información de daños o usos no autorizados.

La propuesta del trabajo de investigación abarca como problema principal que una organización no utilice o haga poco uso de una metodología apropiada de ciberseguridad orientada a los objetivos del negocio, independientemente el que sea. La importancia de la solución propuesta es brindar varios métodos, guías o lineamientos que una empresa pueda adoptar, de tal forma que se mejore su ciberseguridad y se minimice el riesgo de daño o pérdida de sus activos, y que sea acorde a sus propios objetivos.

La solución está basada en la construcción de la investigación a partir de marcos teóricos previamente definidos, sobre todo porque los métodos de trabajo, como el de NIST, están fundamentados en normas existentes. En paralelo a la investigación, se contempla conversaciones con profesionales

expertos en el área de ciberseguridad para ayudar a enriquecer aún más el contenido propuesto.

En el primer capítulo se desarrollará un análisis GAP para contrastar el estado actual de la organización frente a un marco de referencia conocido, el NIST Cyber Secucity Framework (CSF), con el objetivo de desarrollar el plan que ayude a mitigar las posibles deficiencias encontradas.

En el segundo capítulo se presentará un Plan Estratégico de Seguridad de la Información (PESI) de forma detallada, ordenada y calendarizada, según la prioridad y severidad de los resultados obtenidos del análisis GAP.

2. ANTECEDENTES

Guatemala, a diferencia de Estados Unidos, no posee leyes generales para la protección de información o regulaciones específicas según la industria. Se han presentado distintas iniciativas como la 5254 de 2017, titulada *Ley contra la ciberdelicuencia*, y la 5601 de 2019, titulada *Ley de prevención y protección contra la ciberdelincuencia,* pero estas han sido enfocadas más bien hacia el hecho de tipificar figuras delictivas y adecuar las normas penales existentes en las leyes vigentes. Esta última fue aprobada en el decreto 39-2022 el 4 de agosto del presente año, sin embargo, el 1 de septiembre se publica en el diario oficial que se archiva al tener múltiples objeciones, ya que podría poner en riesgo la libertad de expresión y la crítica hacia funcionarios públicos.

Al no contar con este tipo de leyes, tampoco se ha definido qué sectores u organizaciones se consideran como infraestructura crítica, contrario a lo que establece el marco de trabajo NIST en Estados Unidos.

A nivel gubernamental, en específico en el Ministerio de Energía y Minas, se posee un documento realizado por Monterroso (2006) titulado *Políticas, normas y procedimientos. Departamento de informática*, que, a pesar de estar limitado a dicho ministerio, expresa la importancia de la aplicación de normas y directrices como una herramienta organizacional para hacer conciencia a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva.

Sobre investigaciones realizadas se destacan algunas a nivel latinoamericano como la titulada *Diseño de un modelo de políticas de seguridad informática para la Superintendencia de Industria y Comercio de Bogotá,* por Palacios, (2015) en Colombia, en la cual, inicialmente, se realizaron pruebas para diagnosticar vulnerabilidades a nivel de seguridad informática y así proponer un modelo a implementar con la infraestructura actual. Un aspecto importante a destacar es que este se fundamenta en los lineamientos de la norma ISO 270001 para asegurar la confidencialidad, integridad y disponibilidad de la información.

Una segunda investigación previa fue llevada a cabo por Gavino (2018) en Perú y se titula *Ciberseguridad en la actividad organizacional de la era digital*, que está enfocada en la medida en que la ciberseguridad mejora aspectos como los gastos operativos, tiempos de operación, disponibilidad de los datos y los problemas de infraestructura de una organización, y concluye que influye positivamente en aspectos como mejora de la actividad organizacional, planificación y aplicación de la gestión institucional.

La investigación realizada por Alvarado Llano y Changoluisa Pachacama (2019), titulada *Análisis de la ciberseguridad a la infraestructura tecnológica de la universidad técnica de Cotopaxi,* en Ecuador, se realizó bajo la norma ISO/IEC 27032/2012 a través de pruebas de penetración desde una máquina física, dirigidas hacia la infraestructura de la universidad tomando como base una serie de pruebas y encuestas a los empleados y estudiantes del área de seguridad, denotando una alta falta de conocimiento que resultó en varias brechas de seguridad después de las pruebas. El trabajo concluye con recomendaciones como mantener abiertos los puertos exclusivamente necesarios, mantener las firmas de la base de datos del antivirus actualizadas y asegurar la red Wireless del área de TI con Mac Address.

En el trabajo de investigación titulado *Diagnóstico de las vulnerabilidades informáticas en los sistemas de información para proponer soluciones de seguridad a la rectificadora Gabriel Mosquera S.A.,* el cual fue realizado por Pintado Cuji y Hurtado Valero (2015) en Ecuador, se realiza un diagnóstico de las vulnerabilidades para proponer soluciones haciendo énfasis en las políticas de seguridad y las responsabilidades de cada participante. Se toman en cuenta procedimientos para prevenir, detectar y responder a amenazas. Esta investigación fue basada en los estándares de las normas ISO 270001, 17799 y NIST-800.x, utilizando las metodologías MSAT y OCTAVE -S.

3. PLANTEAMIENTO DEL PROBLEMA

3.1. Descripción del problema

Cualquier individuo, empresa o gobierno que posea acceso o no a Internet es vulnerable a múltiples riesgos, tanto físicos como cibernéticos; riesgos a los que se es vulnerable por una mala administración de los recursos, desconocimiento o por falta de importancia. Entre los riesgos de seguridad física se pueden encontrar la ubicación, seguridad perimetral y el acceso no autorizado a las instalaciones, robo de documentos físicos e identificaciones, mientras que entre los riesgos en ciberseguridad se podrían mencionar algunos como acceso no autorizado a la red y servicios, robo de credenciales, suplantación de identidad, explotación de vulnerabilidades, ingeniería social, entre otros.

El origen del problema radica en que no se conocen todos los activos que se poseen como hardware, software, personas, políticas, entre otros. De igual forma, se podría tener información incompleta, desactualizada o incluso nula de los inventarios de estos, por lo que no se podría definir cuáles son más vulnerables que otros y cuáles son de mayor importancia para proteger.

Por lo tanto, al no conocer de manera íntegra los activos, se podría no manejar de manera correcta las vulnerabilidades, controles de seguridad, detección de ataques, respuesta a incidentes, recuperación, cumplimiento, reportes, asumiendo que estos ya se aplican.

El problema principal puede ser que no se siga un marco de trabajo o referencia en específico que pudiera reducir, de cierta forma, los riegos y mejorar la postura de ciberseguridad. Aunado a esto, es vital resaltar la importancia de la revisión constante de la postura de ciberseguridad, para generar una mejora continua, sobre todo por el hecho de que en el mundo digital todo es cambiante, a diario se descubren nuevas amenazas y brechas y formas de explotarlas. Esto provoca que se haga una revisión minuciosa a la postura de ciberseguridad.

3.2. Delimitación

El trabajo de investigación se limita a la evaluación y propuesta de mejora de la postura de seguridad. Se limita también a una empresa mediana que, según el Acuerdo Gubernativo 211-2015, posee un mínimo de 81 y un máximo de 200 empleados.

El tipo de empresa según la actividad económica a la que se dedica se limita al sector de servicios tales como banca, casinos, telecomunicaciones, educación, hotelería, transporte, hospitales, entre otros. Este tipo de empresas son objetivos comunes para ciberataques por el tipo, calidad y cantidad de información y recursos que poseen.

Por último, se limita a una empresa en Guatemala, país donde se realizará el trabajo de investigación y porque se pretende que pueda ser implementado a nivel nacional y escalable.

3.3. Pregunta principal de investigación

¿Cómo alcanzar los objetivos propuestos por la compañía a través de un Plan Estratégico de Seguridad de la Información (PESI), tomando en cuenta los resultados obtenidos del análisis GAP basado en el NIST CSF?

3.4. Preguntas complementarias

- ¿Cómo realizar un análisis GAP basado en el NIST CSF?
- ¿Cómo interpretar los resultados de un análisis GAP basado en el NIST CSF?
- ¿Cómo se diseña un Plan Estratégico de Seguridad de la Información (PESI) tomando en cuenta el análisis GAP?
- ¿Cuáles son los resultados de ejecutar un Plan Estratégico de Seguridad de la Información (PESI)?

4. JUSTIFICACIÓN

Una empresa se puede dedicar a un tipo de actividad económica u otra según los objetivos de la misma. Sin importar el tipo se debe considerar la ciberseguridad como un elemento más de vital importancia para el negocio. En estos tiempos modernos ya no es aceptable considerar que solo las grandes empresas, aquellas que se dedican a la banca, generación de energía o gobiernos son los objetivos de los cibercriminales, sobre todo cuando durante la pandemia del Covid-19 los ciberataques aumentaron considerablemente a nivel general.

Tampoco es aceptable que, si en una empresa, institución o fábrica se poseen dispositivos con acceso a Internet o conectados a la red, es viable pensar que solo una configuración inicial e instalación de software como antivirus es suficiente y que no se mantenga en una constante revisión, monitoreo o actualización. Al igual que el recurso humano, brindar seguridad a los empleados o servidores de un dispositivo móvil y una computadora portátil tampoco es suficiente. Se debe concientizar y capacitar al personal sobre los riesgos a los que están expuestos, sin importar el área o puesto en que se desempeñe y, de esta forma, reducir los riesgos de ingeniería social.

La ciberseguridad no debe ser un tema de gustos o preferencias, decidir si implementarlo o no, o peor aún, pensar que es un gasto innecesario y que nunca se ven resultados reflejados a corto plazo. La ciberseguridad debería ser una inversión en una empresa como medio preventivo.

De cierta forma, el objetivo es proveer una serie de guías y lineamientos para las empresas, independientemente de su actividad económica, para que lleven a cabo controles de seguridad, monitoreo, contención y respuesta a incidentes, así como recuperación y otros, con base en los activos de la compañía y su importancia dentro de la misma.

Uno de los marcos de trabajo que más adelante se detallará es el de NIST. Este fue creado como una iniciativa del presidente de los Estados Unidos de 2009 a 2016: Barack Obama, para la protección de la infraestructura considerada como crítica del sector privado. El objetivo de este es manejar y reducir de mejor forma el riesgo cibernético. Infraestructura considerada como crítica para la seguridad nacional en este marco son químicos, comercio, manufactura, defensa industrial, servicios de emergencia, energía, sector financiero, sector comida y agricultura, gobierno, sector salud y salud pública, tecnología de la información, así como reactores nucleares, materiales y desperdicios; transporte; agua y aguas residuales.

En este sentido, varias o muchas empresas de distintos sectores que pudieran ser comprometidas podrían provocar una crisis en la seguridad nacional de una nación, por ejemplo la paralización de servicios bancarios, agua, energía, telecomunicaciones o combustibles.

5. OBJETIVOS

5.1. Objetivo general

Proporcionar un Plan Estratégico de Seguridad de la Información (PESI) a la compañía estudiada para alcanzar los objetivos propuestos, tomando en cuenta el análisis GAP.

5.2. Específicos

- Evaluar el desempeño actual de la compañía a través de un análisis GAP basado en el NIST CSF.

- Analizar los resultados obtenidos del análisis GAP para priorizar las estrategias para el Plan Estratégico de Seguridad de la Información (PESI).

- Elaborar el Plan Estratégico de Seguridad de la Información (PESI) para los objetivos propuestos de la compañía para los próximos tres años.

- Proponer soluciones para la implementación del Plan Estratégico de Seguridad de la Información (PESI).

6. NECESIDADES A CUBRIR

6.1. Descripción

Todo individuo, empresa o gobierno tiene objetivos claros respecto a las actividades a las que se dedica. Por ejemplo, una compañía de telecomunicaciones, una manufactura, una farmacéutica, el ministerio de defensa, por mencionar algunos. Independientemente del negocio o actividad a la que se dedique una empresa, tiene otras áreas que son muy importantes para el funcionamiento como una misma organización, por ejemplo, recursos humanos, red de distribución, capacitación, contabilidad, informática. La ciberseguridad también debe ser un pilar para toda empresa y no específicamente como un área más sino un elemento que debe ser priorizado.

El presente documento tiene como objetivo proponer un trabajo de investigación basado en guías, instrucciones, prácticas y lineamientos estándar que una empresa puede adoptar, independientemente si ya posee una base de ciberseguridad o no. El fin es mejorar y aumentar la ciberseguridad para tratar de reducir el riesgo de vulnerabilidades al estar mejor preparados y ordenados.

6.2. Esquema de solución

A continuación se muestra un esquema con el cual se pretende llegar a la solución de esta propuesta de trabajo de graduación. La forma de interpretarlo es de arriba hacia abajo, iniciando con la revisión bibliográfica en paralelo con conversaciones con expertos, esto último en el área laboral en que se desempeña el autor. Se eligió de esta forma para que el enriquecimiento,

producto de conversaciones, pueda ser aprovechado para definir métodos de mejoramiento de la postura de ciberseguridad que no fueron considerados inicialmente y el contenido se actualice de mejor forma que realizándolo en las revisiones finales.

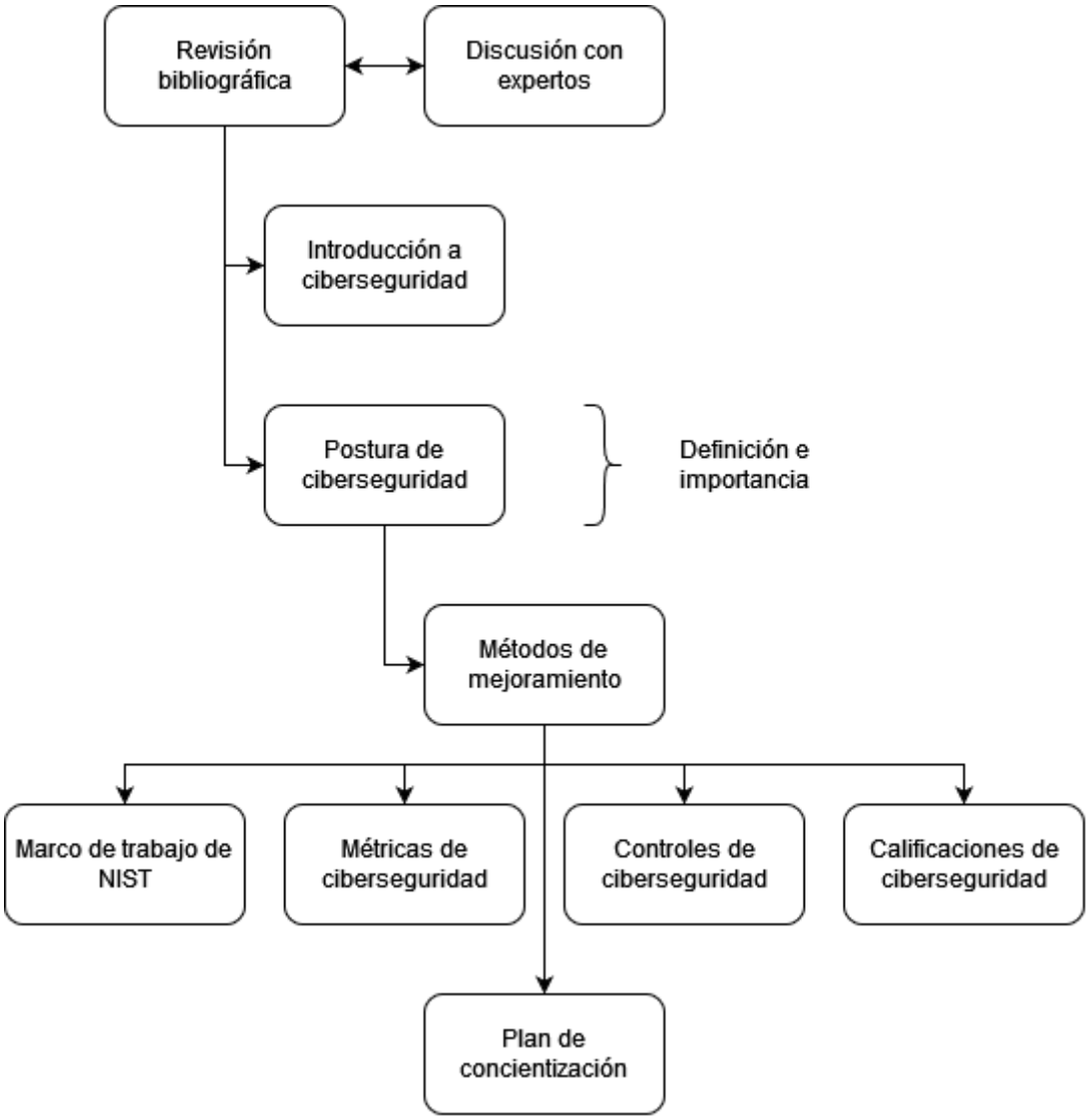
Luego se propone un capítulo para desarrollar una introducción a la ciberseguridad de una forma muy general y amplia, sin términos muy técnicos o específicos, que sirva de familiarización al lector con el contenido que encontrará en capítulos posteriores.

Los siguientes capítulos desarrollan el trabajo de investigación, empezando por definir la importancia de la postura de ciberseguridad y qué aspectos se toman en cuenta para mejorarla, siendo descritos en los siguientes subcapítulos.

Por último, se propone un plan de concientización para que pueda ser utilizado como base en una organización, es un plan dirigido hacia los empleados, con el fin de mitigar los efectos de la ingeniería social. La ingeniería social es uno de varios aspectos a considerar como mejoramiento de la postura de ciberseguridad y se ha decidido hacer énfasis realizando un capítulo dedicado a ella.

A continuación puede observarse el esquema de solución propuesto:

Figura 1. **Esquema de solución propuesto**



Fuente: elaboración propia, realizado con Flowchart Maker & Online Diagram Software.

7. MARCO TEÓRICO

7.1. Ciberseguridad

La ciberseguridad es la práctica de proteger los sistemas críticos e información sensible de ataques digitales. También conocida como seguridad de la tecnología de la información (IT), las medidas de ciberseguridad están diseñadas para combatir amenazas contra sistemas interconectados y aplicaciones, sin importar si esas amenazas se originan dentro o fuera de la organización (IBM, s.f.).

En el 2020, el costo promedio de una brecha de información fue 3,86 mil millones de dólares americanos globalmente, mientras que 8,64 mil millones solo en los Estados Unidos de América. Estos costos incluyen gastos de descubrir y responder a la brecha, costos de tiempo de inactividad y pérdida de ingresos, y el daño a la reputación a largo plazo de una empresa y su marca (IBM, s.f.).

7.2. Pilares de la seguridad de la información

A continuación se explica cada pilar.

7.2.1. Confidencialidad

La confidencialidad implica mantener información de la organización, información de los clientes, propiedad intelectual patentada y cualquier otra información bajo el dominio de la seguridad de la información protegida del

acceso no autorizado. Los atacantes buscarán interrumpir un estado de confidencialidad para exfiltrar datos o vigilar información que debe mantenerse privada (Cranford, 2021).

7.2.2. Integridad

La pregunta sobre integridad que una empresa podría hacerse es si su información está corrupta, afectada o manipulada por amenazas externas. La falta de integridad en un ambiente puede guiar al uso indebido de credenciales, resultando en que los atacantes pueden manipular la información para lograr varios objetivos sin hacer algo tan ruidoso o notorio como cifrar y exfiltrar información. Algunos ejemplos comunes pueden incluir manipular registros financieros para eliminar rastros de transacciones y la manipulación de saldos de cuentas, el cambio de planos o fórmulas químicas para sabotear intencionalmente un producto que produce una organización (Cranford, 2021).

7.2.3. Disponibilidad

La CIA considera a la disponibilidad como el pilar fundamental, ya que la falta de esta es un signo visible de interrupción. Se sabe que los adversarios son conocidos por utilizar ataques distribuidos de denegación de servicio para interrumpir la disponibilidad de los sistemas de tecnología de la información, pero la amenaza más efectiva y alarmante del momento es el *ransomware* (Cranford, 2021).

7.3. Brecha de información

Una brecha de información expone información protegida, confidencial o sensible a una persona no autorizada. Los archivos en una brecha de

información son vistos y compartidos sin permiso. Cualquiera puede estar en riesgo de una brecha de información, desde individuos hasta grandes empresas y gobiernos. Más importante es que cualquiera puede poner a otros en riesgo si no está protegido (Kaspersky, s.f.). En general, las brechas de información ocurren debido a debilidades en tecnología y en el comportamiento de los usuarios.

A medida que las computadoras y dispositivos móviles obtienen más funciones de conexión, hay más lugares para que los datos se filtren. Las nuevas tecnologías se están creando más rápido de lo que se pueden proteger. Un ejemplo pueden ser productos de hogares inteligentes que tienen fallas como la falta de encriptación. Por otro lado, es suficiente un usuario sin hábitos digitales como objetivo para comprometer un sitio web o una red (Kaspersky, s.f.).

Las brechas de información puede que ocurran por ataques intencionales, pero no siempre es así, pueden ocasionarse por descuidos de individuos o fallas en la infraestructura de una empresa. Las brechas pueden ocurrir por tener acceso a información confidencial de manera accidental o maliciosa, pérdida o robo de dispositivos, y criminales externos (Kaspersky, s.f.).

7.4. Ciberataque

Un ciberataque es un intento malicioso y deliberado por parte de una persona u organización de violar el sistema de información de otra persona, organización o gobierno. Por lo general, el atacante busca algún tipo de beneficio al interrumpir la red de la víctima (Cisco, s.f.).

Un ciberataque puede ser ejecutado desde cualquier locación y por un individuo o grupo, haciendo uso de una o más tácticas, técnicas y procedimientos. Los individuos que lanzan ciberataques son usualmente conocidos como cibercriminales, actores de amenazas, malos actores, piratas informáticos o hackers (Imperva, s.f.).

Algunos ciberdelincuentes llevan a cabo ataques en beneficio personal o financiero. Otros son hacktivistas que actúan en nombre de causas sociales o políticas. Algunos ataques son parte de operaciones de guerra cibernética llevadas a cabo por estados nacionales contra sus oponentes, o que operan como parte de grupos terroristas conocidos (Imperva, s.f.).

Sin embargo, un ciberataque se considera evitable. La clave de la ciberdefensa es la arquitectura de seguridad cibernética, que sea multicapa y abarque todas las redes, equipos terminales, dispositivos móviles y la nube (Checkpoint, s.f.).

Otros factores a tomar en cuenta son:

- Mantener higiene de la seguridad
- Elegir prevención sobre detección
- Cubrir todos los vectores de ataque
- Implementar las tecnologías más avanzadas
- Mantener la inteligencia de amenazas actualizada

7.5. Tipos de ciberataques

A continuación se desarrolla cada tipo de ciberataque.

7.5.1. Ataques DoS y DDoS

Un ataque de denegación de servicio, DoS por sus siglas en inglés, está diseñado para abrumar los recursos de un sistema hasta el punto en no puede responder a las solicitudes de servicio legítimas. Un ataque de denegación de servicio distribuido, DDoS, es similar en el sentido de que busca drenar los recursos de un sistema. Este ataque es iniciado por un arreglo de máquinas afectadas por malware que son controladas por el atacante (Fortinet, s.f.).

Con un ataque de denegación de servicio, el sitio objetivo se inunda de solicitudes ilegítimas. Debido a que el sitio tiene que responder a cada solicitud, todas las respuestas consumen sus recursos. Esto hace que sea imposible para el sitio servir a los usuarios como normalmente lo hace y resulta en un completo apagado del sitio. El objetivo es interrumpir la efectividad del servicio de la víctima (Fortinet, s.f.).

7.5.2. *Phishing*

Los ataques de *phishing* ocurren cuando un actor malicioso envía correos electrónicos que parecen ser enviados de fuentes confiables o legítimas como intento de obtener información sensible de la víctima. Los ataques de *phishing* se combinan con ingeniería social y tecnología y son llamados de esta forma porque el atacante, en efecto, está pescando para acceder a un área prohibida al utilizar un cebo de un remitente aparentemente confiable (Fortinet, s.f.).

7.5.3. *Ransomware*

Con este ataque, el sistema de la víctima se mantiene como rehén hasta que acepte pagar un rescate al atacante. Después que el pago se haya enviado, normalmente a través de alguna criptomoneda, el atacante proporciona instrucciones sobre cómo la víctima puede recuperar el control de su computadora, sin embargo, tampoco hay seguridad de que el atacante cumpla con entregar el control (Fortinet, s.f.).

La víctima puede descargar el *ransomware* a través de un sitio web o un documento adjunto a un correo electrónico. El malware está escrito para explotar vulnerabilidades que no han sido abordadas por el fabricante o el equipo de tecnología de la información. El *ransomware* encripta el equipo y lo mantiene rehén (Fortinet, s.f.).

7.5.4. Malware

Este término se refiere a varias formas software dañino tales como virus y *ransomware.* Una vez el malware esté en una computadora, puede causar múltiples daños como tomar control del equipo, monitorear actividad y pulsaciones del teclado, incluso enviar datos confidenciales de forma silenciosa desde la computadora o red hasta la base de operaciones del atacante (Rapid7, s.f.).

Los atacantes utilizan varios métodos para introducir malware a un equipo, pero a menudo se requiere una acción de parte del usuario. Esto puede incluir hacer *click* en un enlace para descargar un archivo, o abrir un documento adjunto que pareciese inofensivo como un archivo de Word o PDF (Rapid7, s.f.).

7.5.5. Ataque de inyección SQL

SQL significa lenguaje de consulta estructurado, por sus siglas en inglés. Es un lenguaje de programación que se utiliza para comunicarse con las bases de datos. Varios servidores que almacenan información crítica para sitios web o servicios utilizan SQL para administrar la información en sus bases de datos. Un ataque de inyección SQL se dirige a este tipo de servidores, utilizando un código malicioso para que el servidor divulgue información que normalmente no divulgaría. Esto es especialmente problemático si el servidor almacena información privada del cliente del sitio web como tarjetas de crédito, usuarios y contraseñas u otra información de identificación personal, que son objetivos tentadores y lucrativos para un atacante (Rapid7, s.f.).

7.5.6. Suplantación de DNS

Los cibercriminales han explotado durante mucho tiempo la naturaleza insegura de los servidores DNS para sobrescribir las direcciones IP almacenadas en los servidores DNS y los resolutores con entradas falsas, así las víctimas son dirigidas a un sitio web controlado por el *hacker* en lugar del sitio legítimo. Estos sitios falsos están diseñados para verse exactamente como el sitio que los usuarios esperaban visitar, por lo que no sospechan cuando se les solicita sus credenciales de inicio de sesión (Cobb, s.f.).

Estos sitios maliciosos están diseñados para instalar malware en los dispositivos de los usuarios, robar información sensible o redirigir el tráfico (Panda Security, 2022).

7.6. Postura de ciberseguridad

La postura de seguridad, o postura de ciberseguridad, de una organización es el estado de la seguridad de manera colectiva de todo el software, hardware, servicios, redes, información, vendedores y proveedores de servicios, de acuerdo a Tyas (2022).

La postura de ciberseguridad abarca información de la seguridad, seguridad de los datos, seguridad de las redes, pruebas de penetración, capacitación en concientización sobre seguridad para prevenir ataques de ingeniería social, gestión de riesgos de proveedores, gestión de vulnerabilidades, prevención de fuga de información y otros controles de seguridad (Tyas, 2022).

La ciberseguridad es la probabilidad de exposición o pérdida como resultado de ciber ataques, fuga de información y otras ciberamenazas. Dicho de otra forma, es la potencial pérdida o daño a la infraestructura de tecnología de la información o a confidencialidad, integridad y disponibilidad de los activos de la organización (Tyas, 2022).

7.7. El marco de trabajo de ciberseguridad de NIST

En febrero de 2013, el presidente Barack Obama emitió la orden ejecutiva 13636, sobre mejoramiento de la ciberseguridad de la infraestructura crítica, para mejorar la seguridad económica y nacional de los Estados Unidos de América, al mejorar la fiabilidad de su infraestructura crítica (Tyas, 2022).

Esta provee un marco de trabajo, basado en estándares, guías y prácticas existentes para organizaciones del sector privado de los Estados

Unidos de América, con el fin de manejar y reducir el riesgo en ciberseguridad (Tyas, 2022).

Los recursos que se consideran como infraestructura crítica, de acuerdo a NIST (2021), para este marco de trabajo son los siguientes:

- Sector químico
- Sector de instalaciones comerciales
- Sector de comunicaciones
- Sector de manufactura crítica
- Sector de presas
- Sector de defensa industrial
- Sector de servicios de emergencia
- Sector de energía
- Sector de servicios financieros
- Sector de comida y agricultura
- Sector de instalaciones del gobierno
- Sector de salud y salud pública
- Sector de tecnología de la información
- Sector de reactores nucleares, materiales y desperdicios
- Sector de sistemas de transporte
- Sector de agua y aguas residuales

8. PROPUESTA DE ÍNDICE DE CONTENIDOS

9. METODOLOGÍA

9.1. Diseño de investigación

Se utilizará un diseño no experimental, ya que en este no se realizan experimentos sino más bien está enfocado en la observación de sucesos existentes o que ya pasaron. En forma más específica, el trabajo de investigación está enfocado en métodos que fueron desarrollados con base en la observación de fenómenos que ocurrieron y que sirvieron como referencia para la creación de estos.

9.2. Alcance de la investigación

Se propone el alcance descriptivo, ya que por definición este busca especificar propiedades y características importantes de cualquier fenómeno que se analice (Hernández, Fernández y Baptista, 2014). De forma particular para esta investigación, se pretende especificar características de distintos métodos para la mejora de la postura de ciberseguridad de acuerdo a los lineamientos y requerimientos de cada compañía.

9.3. Enfoque de la investigación

Se ha elegido el enfoque cualitativo para el desarrollo de la investigación, ya que en este se utiliza la recolección y análisis de la información. La ventaja de este tipo de enfoque es que las preguntas de investigación se pueden afinar antes, durante y después de la recolección y el análisis de los datos, tal como lo indica el diagrama de la solución propuesta. La revisión bibliográfica en paralelo

con la conversación con expertos permitirá enriquecer aún más la investigación y que retome el objetivo principal.

9.4. Fuentes de información

En su mayor parte, el desarrollo del trabajo de investigación es teórico, por lo que se utilizará cualquier medio físico o electrónico para la recopilación de información. Entre algunos medios se pueden mencionar sitios web de reconocidos proveedores de seguridad a nivel mundial, marcos de trabajo existentes, artículos, foros, conversatorios y paneles de discusión.

Como fuente secundaria, pero muy importante, se tienen conversatorios con colegas expertos en ciberseguridad que, de una u otra forma, pueden enriquecer al orientar de mejor forma el desarrollo del trabajo de investigación. Por otro lado, se consideran investigaciones previas o relacionadas a la ciberseguridad por medio de sus marcos teóricos como referencia.

10. TÉCNICAS DE ANÁLISIS DE INFORMACIÓN

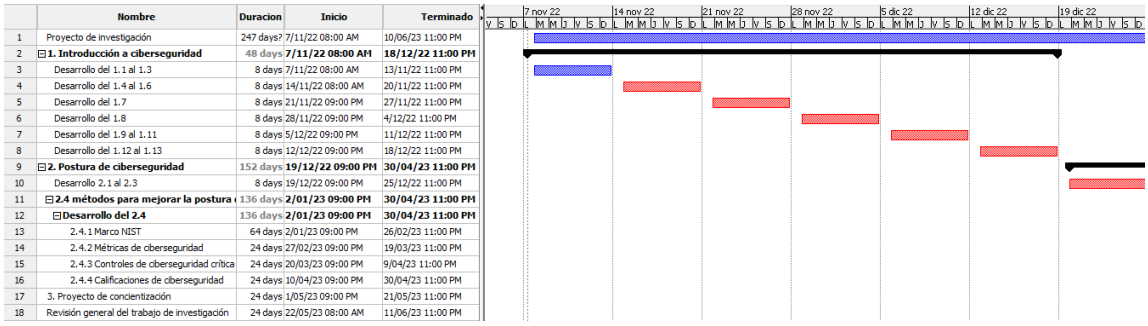
Debido a que el enfoque de la investigación es cualitativo, el análisis de la información se puede llevar a cabo en paralelo con la recolección de esta. Esta es una gran ventaja ya que, si la investigación se llegara a desviar o tomar otro rumbo, las técnicas de análisis pueden ayudar a retomar el objetivo central y definir las preguntas de investigación. De esta forma, las técnicas para el análisis de la información para datos cualitativos que se pueden emplear son:

- Análisis de contenido cualitativo
- Análisis comparativo constante
- Análisis del discurso
- Observación
- Entrevista
- Análisis documental
- Casos de estudio

11. CRONOGRAMA

A continuación se muestra el cronograma de actividades organizado por semanas desde el inicio del trabajo de investigación, pasando por la aprobación del protocolo hasta la finalización.

Figura 2. **Cronograma propuesto**



	Nombre	Duracion	Inicio	Terminado
1	Proyecto de investigación	247 days?	7/11/22 08:00 AM	10/06/23 11:00 PM
2	**1. Introducción a ciberseguridad**	48 days	**7/11/22 08:00 AM**	**18/12/22 11:00 PM**
3	Desarrollo del 1.1 al 1.3	8 days	7/11/22 08:00 AM	13/11/22 11:00 PM
4	Desarrollo del 1.4 al 1.6	8 days	14/11/22 08:00 AM	20/11/22 11:00 PM
5	Desarrollo del 1.7	8 days	21/11/22 09:00 PM	27/11/22 11:00 PM
6	Desarrollo del 1.8	8 days	28/11/22 09:00 PM	4/12/22 11:00 PM
7	Desarrollo del 1.9 al 1.11	8 days	5/12/22 09:00 PM	11/12/22 11:00 PM
8	Desarrollo del 1.12 al 1.13	8 days	12/12/22 09:00 PM	18/12/22 11:00 PM
9	**2. Postura de ciberseguridad**	152 days	**19/12/22 09:00 PM**	**30/04/23 11:00 PM**
10	Desarrollo 2.1 al 2.3	8 days	19/12/22 09:00 PM	25/12/22 11:00 PM
11	**2.4 métodos para mejorar la postura**	136 days	**2/01/23 09:00 PM**	**30/04/23 11:00 PM**
12	**Desarrollo del 2.4**	136 days	**2/01/23 09:00 PM**	**30/04/23 11:00 PM**
13	2.4.1 Marco NIST	64 days	2/01/23 09:00 PM	26/02/23 11:00 PM
14	2.4.2 Métricas de ciberseguridad	24 days	27/02/23 09:00 PM	19/03/23 11:00 PM
15	2.4.3 Controles de ciberseguridad crítica	24 days	20/03/23 09:00 PM	9/04/23 11:00 PM
16	2.4.4 Calificaciones de ciberseguridad	24 days	10/04/23 09:00 PM	30/04/23 11:00 PM
17	3. Proyecto de concientización	24 days	1/05/23 09:00 PM	21/05/23 11:00 PM
18	Revisión general del trabajo de investigación	24 days	22/05/23 08:00 AM	11/06/23 11:00 PM

Fuente: elaboración propia, realizado con Project Libre.

12. FACTIBILIDAD DEL ESTUDIO

La factibilidad técnica corresponde a los recursos como hardware (computadora personal de escritorio y teléfono móvil con acceso a Internet) y software (Microsoft Office y navegadores web como Firefox y Google Chrome). Actualmente el autor ya cuenta con dichos recursos y no representará un gasto adicional. Por otro lado, hay algunas herramientas de software como Balbix o BITSIGHT que proveen una demo gratis, por lo que tampoco representará un gasto. Estas herramientas son utilizadas para evaluación y manejo de la postura de seguridad, riesgos y vulnerabilidades, entre otros aspectos.

En la factibilidad operativa no se identifican procesos en específico que sean necesarios al ser una investigación basada en recursos bibliográficos tanto físicos como digitales. Una limitante que podría presentarse es que, hasta el momento, el autor ha encontrado mucha información de calidad en inglés, comparada a la disponible en español, lo cual podría suponer que el proceso de citación y traducción sea un poco más tardado.

Para la factibilidad financiera no se consideran gastos más allá de los recursos que el autor emplee para la obtención de fuentes de información. De utilizarse herramientas de software, se requerirán demos en sus versiones gratuitas. Los únicos gastos a considerar serán los descritos en las siguientes tablas y serán financiados en su totalidad por el autor.

Tabla I. **Cuadro de costos**

Descripción	Costo
Consumo de energía eléctrica	Q 400.00
Uso de Internet residencial	Q 800.00
Plan de datos móviles	Q 800.00
Total	Q 2,000.00

Fuente: elaboración propia.

Aunado al cuadro de costo se debe considerar la inversión que el autor realizará hasta finalizar el trabajo de investigación, misma que se detalla a continuación:

Tabla II. **Inversión durante el trabajo de investigación**

Descripción	Costo
Consumo de energía eléctrica	Q 450.00
Uso de Internet residencial	Q 900.00
Plan de datos móviles	Q 900.00
Pago de maestría	Q 21,300.00
Total	Q 23,550.00

Fuente: elaboración propia.

Tal como se mencionó en la factibilidad técnica, se utilizarán herramientas (demos) gratuitas, por lo que los únicos gastos a considerar son energía eléctrica, Internet residencial y plan de datos móviles que, en su totalidad, serán cubiertos por el autor. En cuanto a la factibilidad temporal, se espera culminar el proceso de informe en un tiempo mínimo de 6 meses y máximo de 8 meses, debiéndose realizar en los tiempos libres del autor, en un tiempo esperado mínimo de 16 horas a la semana.

13. REFERENCIAS

1. Alvarado, W. y Changoluisa, I. (2019). *Análisis de la ciberseguridad a la infraestructura tecnológica de la Universidad Técnica de Cotopaxi.* Repositorio Digital de la Universidad Técnica de Cotopaxi, Ecuador. Recuperado de http://repositorio.utc.edu.ec/bitstream/27000/5323/1/PI-001347.pdf

2. Checkpoint. (s.f.). What is a Cyber Attack? [¿Qué es un ciberataque?] [Mensaje en un blog]. Recuperado de https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/#

3. Cisco. (s.f.). What Is a Cyberattack? - Most Common Types [¿Qué es un ciberataque? - Los tipos más comunes] [Mensaje en un blog]. Recuperado de https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

4. Cobb, M. (s.f.). 13 Common Types of Cyber Attacks and How to Prevent Them [13 tipos comunes de ciberataques y cómo prevenirlos] [Mensaje en un blog]. Recuperado de https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them

5. Cranford, J. (15 de septiembre de 2021). Three Pillars of Infosec: Confidentiality, Integrity and Availability [Tres pilares de seguridad

de la información: confidencialidad, integridad y disponibilidad] [Mensaje en un blog]. Recuperado de https://www.cybereason.com/blog/three-pillars-of-infosec-confidentiality-integrity-and-availability

6. Fortinet. (s.f.). Top 20 Most Common Types Of Cyber Attacks [Top 20 Tipos de ciberataque más comunes] [Mensaje en un blog]. Recuperado de https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

7. Gavino, M. (2018). *Ciberseguridad en la actividad organizacional de la era digital* (tesis de maestría). Universidad Nacional Federico Villareal, Perú. Recuperado de http://www.unfv.edu.pe/facultades/fiis/images/oficinas/unidad_investigacion/INVESTIGACION_2019/MIERCOLES8/FIIS_IF2018_GAVINO_RAMOS_MARTIN.pdf

8. Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación*. México: McGraw Hill.

9. IBM. (s.f.). What is Cybersecurity? [¿Qué es la ciberseguridad?] [Mensaje en un blog]. Recuperado de https://www.ibm.com/topics/cybersecurity

10. Imperva. (s.f.). What is a Cyber Attack | Types, Examples & Prevention [Qué es un ciberataque | Tipos, ejemplos y prevención] [Mensaje en un blog]. Recuperado de https://www.imperva.com/learn/application-security/cyber-attack/

11. Kaspersky. (s.f.). What is a Data Breach & How to Prevent One [Qué es una brecha de información y cómo prevenir una] [Mensaje en un blog]. Recuperado de https://www.kaspersky.com/resource-center/definitions/data-breach

12. Monterroso, A. (junio de 2006). *Políticas, normas y procedimientos del Departamento de Informática.* Ciudad de Guatemala: Ministerio de Energía y Minas. Recuperado de https://www.mem.gob.gt/wp-content/uploads/2012/05/MANUAL-DE-PROCEDIMIENTOS-INFORMATICA-PARTE-1.pdf

13. NIST. (2021). Critical Infrastructure Resources [Recursos de infraestructura crítica] [Mensaje en un blog]. Recuperado de https://www.nist.gov/cyberframework/critical-infrastructure-resources

14. Palacios, A. (2015). *Diseño de un modelo de políticas de seguridad informática para la Superintendencia de Industria y Comercio de Bogotá.* Repositorio Institucional de Unilibre, Colombia. Recuperado de https://repository.unilibre.edu.co/bitstream/handle/10901/8926/PROYECTO_DE_GRADO_ANDRES_PALACIOS.pdf?sequence=1

15. Panda Security. (20 de mayo de 2022). What Is DNS Spoofing and How Can You Prevent It? [¿Qué es la suplantación de DNS y cómo puedes prevenirla?] [Mensaje en un blog]. Recuperado de https://www.pandasecurity.com/en/mediacenter/security/dns-spoofing/

16. Pintado, K. y Hurtado, C. (abril de 2015). Diagnóstico de las vulnerabilidades informáticas en los sistemas de información para proponer soluciones de seguridad a la Rectificadora Gabriel Mosquera S.A. Repositorio Institucional de la Universidad Politécnica Salesiana, Ecuador. Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/10349/1/UPS-GT001276.pdf

17. Rapid7. (s.f.). Types of Cyber Attacks | Hacking Attacks & Techniques [Tipos de ciberataques | Ataques de hackeo y ténicas] [Mensaje en un blog]. Recuperado de https://www.rapid7.com/fundamentals/types-of-attacks/

18. Tyas, A. (7 de agosto de 2022). What is a Security Posture and How Can You Evaluate It? [¿Qué es la Postura de Seguridad y cómo evaluarla?] [Mensaje en un blog]. Recuperado de https://www.upguard.com/blog/security-posture

19. Tyas, A. (15 de agosto de 2022). What is the NIST Cybersecurity Framework? [¿Qué es el marco de trabajo de ciberseguridad de NIST?] [Mensaje en un blog]. Recuperado de https://www.upguard.com/blog/nist-cybersecurity-framework