REPÚBLICA DEL ECUADOR

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

PLAN ESTRATÉGICO DE CIBERSEGURIDAD PARA LA EMPRESA IN-PLANET S.A.

TUTOR

Ing. Richard Ramirez-Anormaliza, PhD.

AUTOR

FREDDY XAVIER VALENZUELA ORTEGA

MILAGRO, 2022

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

Milagro, 17 octubre, 2022

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor del Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro.

CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **PLAN ESTRATÉGICO DE CIBERSEGURIDAD PARA LA EMPRESA IN-PLANET S.A., DE LA CIUDAD DE MILAGRO**, elaborado por **FREDDY XAVIER VALENZUELA ORTEGA** el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**.

RICHARD IVAN RAMIREZ ANORMALIZA
C.I: 1203238132

DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

El autor de esta investigación declara ante el Comité Académico de Maestría en Tecnología de la Información de la Universidad Estatal de Milagro, que el trabajo presentado es de mi propia autoría, no contiene material escrito por otra persona, documento o en su totalidad no ha sido aceptado para el otorgamiento de cualquier otro Título de una institución nacional o extranjera.

Milagro, a los 10 días del mes de Marzo de 2023

Firmado electrónicamente por:
FREDDY XAVIER
VALENZUELA ORTEGA

FREDDY XAVIER VALENZUELA ORTEGA

C.I: 0913961439

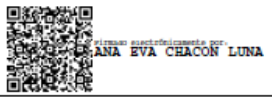
UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO
DIRECCIÓN DE POSGRADO
CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. VALENZUELA ORTEGA FREDDY XAVIER**, otorga al presente proyecto de investigación denominado "PLAN ESTRATÉGICO DE CIBERSEGURIDAD PARA LA EMPRESA IN-PLANET S.A.", las siguientes calificaciones:

TRABAJO DE TITULACION	60.00
DEFENSA ORAL	38.67
PROMEDIO	**98.67**
EQUIVALENTE	**Excelente**

Msc. AREVALO CORDOVILLA FELIPE EMILIANO
PRESIDENTE/A DEL TRIBUNAL



Mgti. CHACON LUNA ANA EVA
VOCAL

Mgti. CORREA PERALTA MIRELLA AZUCENA
SECRETARIO/A DEL TRIBUNAL

DEDICATORIA

El presente trabajo es dedicado primeramente a Dios, a mi esposa, a mis hijos y a mis padres quienes han sido una parte fundamental para la realización de esta tesis y por el apoyo incondicional que me han brindado.

Agradezco también a mis maestros y a la universidad en general por compartirme todos los conocimientos que me han otorgado.

AGRADECIMIENTO

En primera instancia agradezco a mis formadores, personas con un gran conocimiento quienes se han esforzado por ayudarme a llegar al punto en el que me encuentro.

Tan sencillo no ha sido el proceso, pero gracias a las ganas de transmitirme sus conocimientos y dedicación que los ha regido, he logrado importantes objetivos como culminar el desarrollo de mi tesis con éxito y obtener una afable titulación profesional.

CESIÓN DE DERECHOS DE AUTOR

Doctor

ING. FABRICIO GUEVARA VIEJÓ, PhD

Rector de la Universidad Estatal de Milagro

Presente

Mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor al Trabajo realizado como requisito previo para la obtención de mi Título de Cuarto Nivel, cuyo tema fue **PLAN ESTRATÉGICO DE CIBERSEGURIDAD PARA LA EMPRESA IN-PLANET S.A.**, elaborado por **ING. FREDDY XAVIER VALENZUELA ORTEGA** y que corresponde alVicerrectorado de Investigación y Posgrado.

Milagro, 10 de Abril del 2023

Firmado electrónicamente por:
FREDDY XAVIER
VALENZUELA ORTEGA

FREDDY XAVIER VALENZUELA ORTEGA

C.I: 0913961439

ÍNDICE GENERAL

INTRODUCCIÓN **1**

CAPÍTULO 1 ..... **4**

1.1 Planteamiento del problema **4**

1.2 Objetivos **6**

1.2.1 Objetivo General 6

1.2.2 Objetivos Específicos 6

1.3 Alcance **6**

1.4 Estado del arte **7**

CAPÍTULO 2 ..... **16**

2.1 Metodología **16**

CAPÍTULO 3 ..... **22**

3.1 Propuesta de solución **22**

3.1.1 Razones de Ausencia de Disponibilidad de Servicio de Internet por ciberataques .. 22

3.1.2 Mejores prácticas para la gestión de los riesgos e incidentes 23

3.1.3 Criterios de buenas prácticas de ciberseguridad 26

3.2 Plan Estratégico de Ciberseguridad **26**

3.2.1 Fase 1: Conocer la situación actual de la empresa 26

3.2.2 Fase 2: Conocer la estrategia de la organización 59

3.2.3 Fase 3: Definición de proyectos e iniciativas 60

3.2.4 Fase 4: Clasificar y priorizar los proyectos a realizar 62

3.2.5 Fase 5: Aprobar el plan de ciberseguridad 64

3.2.6 Fase 6: Implementar el plan de ciberseguridad 64

CONCLUSIONES Y TRABAJO FUTURO **65**

RECOMENDACIONES 67

BIBLIOGRAFÍA GENERAL..... 69

ÍNDICE DE TABLAS

Tabla 1 Tipos de Activos Informáticos Red Externa. 28

Tabla 2 Distribución de vulnerabilidades por dirección IP Red Externa. 30

Tabla 3 Riesgos Críticos Red Externa. 33

Tabla 4 Riesgos Altos Red Externa. 34

Tabla 5 Riesgos Medio Red Externa. 35

Tabla 6 Riesgos Bajos Red Externa. 37

Tabla 7 Tipo de vulnerabilidad en función del plazo y prioridad – Red Externa. 38

Tabla 8 Tipos de Activos Informáticos Red Interna. 38

Tabla 9 Distribución de vulnerabilidades por dirección IP Red Interna. 41

Tabla 10 Riesgos Críticos Red Interna. 43

Tabla 11 Riesgos Altos Red Interna. 43

Tabla 12 Riesgos Medio Red Interna. 45

Tabla 13 Riesgos Bajos Red Interna. 48

Tabla 14 Tipo de vulnerabilidad en función del plazo y prioridad – Red Externa. 50

Tabla 15 Cantidad de tipos de vulnerabilidades distribuidas por severidad. 51

Tabla 16 Distribución de vulnerabilidades distribuidas por severidad. 53

Tabla 17 Cantidad de tipos de vulnerabilidades distribuidas por severidad. 57

Tabla 18 Código de colores por vulnerabilidad. 58

Tabla 19 Proyectos e Iniciativas. 60

Tabla 20 Clasificación de los Proyectos e Iniciativas. 62

ÍNDICE DE FIGURAS

Figura 1 Distribución de vulnerabilidades por dirección IP Red Externa – Gráfico 1..... 30

Figura 2 Distribución de vulnerabilidades por dirección IP Red Externa – Gráfico 2..... 33

Figura 3 Distribución de vulnerabilidades por dirección IP Red Interna – Gráfico 1..... 40

Figura 4 Distribución de vulnerabilidades por dirección IP Red Interna – Gráfico 2..... 42

Figura 5 Número de vulnerabilidades por categoría. 52

Figura 6 Distribución de Incidencias. 53

Figura 7 Distribución sin vulnerabilidades informativas. 54

RESUMEN

El presente trabajo de investigación se realizó en base a una necesidad de la empresa IN PLANET S.A., donde se realizó de manera exhaustiva un análisis de la seguridad de la información con la finalidad de desarrollar un plan estratégico de ciberseguridad que garantice los pilares básicos de la seguridad de la información como lo son: confidencialidad, integridad y disponibilidad de la misma. En el capítulo 1 del presente trabajo, se especifica el planteamiento de la problemática en donde se evidencia que las empresas actualmente a nivel mundial sufren de ataques informáticos, y es por ello que, las instituciones que manipulan grandes cantidades de datos tengan un plan de contingencia si llega a ocurrir alguna eventualidad que comprometa la seguridad de la información. También, se indicaron los objetivos a cumplir dentro del trabajo de investigación y el alcance que tendrá la misma, donde se desarrolló un plan estratégico de ciberseguridad para la empresa IN PLANET S.A., mediante la serie de las normativas ISO/IEC 27000 y las políticas estipuladas por la ARCOTEL. En el capítulo 2, se desarrolló mediante la Metodología de Gestión de Riesgos ISO/IEC 27005:2018 que se caracteriza por ser una norma internacional publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), para ser más específico, esta normativa se basa en la seguridad de la información mediante un enfoque de gestión de riesgos. Por último en el capítulo 3, se desarrolló la propuesta de solución en donde se realizó un análisis técnico de seguridad a los equipos informáticos internos y externos de la institución, con la finalidad de obtener una visión detallada de las posibles amenazas cibernéticas en la empresa y las capacidades para gestionar los riesgos asociados.

Palabras claves: Seguridad, ISO, Normas, Información

ABSTRACT

The present research work was carried out on the basis of a need of the company IN PLANET S.A., an exhaustive analysis of information security was conducted with the aim of developing a strategic cybersecurity plan that guarantees the basic pillars of information security such as confidentiality, integrity and availability. In chapter 1 of the present paper, the approach to the problem is specified in which it is evident that companies currently worldwide suffer from computer attacks, and that is why, institutions that handle large amounts of data have a contingency plan if any eventuality occurs that compromises information security. Also, the objectives to be met within the research work and the scope that will have it, where a strategic cybersecurity plan was developed for the company IN PLANET S.A., using the series of ISO/IEC 27000 regulations and the policies stipulated by ARCOTEL. In chapter 2, it was developed using the ISO/IEC 27005:2018 Risk Management Methodology, which is characterized as an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), to be more specific, this regulation is based on information security through a risk management approach. Finally, in chapter 3, the solution proposal was developed where a technical security analysis was carried out to the internal and external computer equipment of the institution, in order to obtain a detailed view of the possible cyber threats in the company and the capabilities to manage the associated risks.

Keywords: Security, ISO, Standards, Information

INTRODUCCIÓN

En la actualidad, el desarrollo de las tecnologías de la información y comunicación (TIC) se ha incrementado de forma rápida, por lo tanto, se evidencia el cambio en la optimización de los procesos que se realizan en el trabajo y en el hogar; por ello, las TIC se han convertido en un activo fundamental para el desarrollo de las instituciones que han optado por la utilización de este tipo de herramientas. En ese mismo contexto, las instituciones diariamente utilizan la World Wide Web (WWW o web) siendo un sistema a nivel mundial que hace uso de la Internet con el objetivo de transmitir datos a través de protocolos de red.

Por lo expuesto en párrafo anterior, la utilización de la web en las instituciones u hogares en todo el mundo se ha convertido en una necesidad indispensable, debido a que se puede aplicar diferentes procesos con la información en la web tales como: obtener, enviar, publicar, almacenar, entre otras. La transmisión de los datos que se envía de un punto a otro debe ser segura, de tal forma que el mensaje codificado pueda llegar al receptor sin tener que ser interceptado por algún tipo de ciberataque.

Con la utilización de la web los datos que se envían están propensos a sufrir algún ataque informático por cualquier persona mal intencionada. Es así como, la seguridad de la información se convierte en parte esencial para las instituciones o las personas que deseen enviar información, en tal sentido, el área especializada en la protección de la información se la conocen como ciberseguridad o también conocida como seguridad informática.

La ciberseguridad puede describirse como los métodos, tecnologías y procesos combinados para ayudar a proteger la confidencialidad, integridad y disponibilidad de los sistemas informáticos, que son los pilares de la seguridad de la información, contra los ciberataques o el acceso no autorizado. El objetivo de la ciberseguridad es proteger

la información de ser robada, comprometida o atacada, en donde se puede medir por al menos uno de los tres objetivos: proteger la confidencialidad de los datos, preservar la integridad de los datos y asimismo promover la disponibilidad de datos para usuarios autorizados.

En razón a lo antes mencionado, la importancia de la seguridad de la información se convierte en parte primordial para el crecimiento económico de cualquier institución, cuando una empresa aplica un plan de respuesta a incidentes eficaz y tiene una seguridad de red sólida, está mejor posicionada para mitigar y prevenir los ciberataques.

Según la Comisión Económica para América Latina y el Caribe (CEPAL) expuso lo siguiente:

> El crecimiento actual de ciberataques en las empresas a nivel global ha causado pérdidas económicas sustanciales para ciertas instituciones, según la Comisión Económica para América Latina y el Caribe (CEPAL) demostraron que los incidentes de ciberseguridad que han sido denunciados se han incrementado exponencialmente en estos últimos 5 años (CEPAL, 2021).

En consecuencia, como caso de estudio del presente trabajo investigativo se enfocará en la empresa proveedora de Internet IN-PLANET S.A., ubicada en Ecuador, provincia del Guayas, ciudad Milagro la cual cuenta actualmente con una amplia cartera de clientes haciendo uso del servicio de Internet. Por lo tanto, la empresa antes mencionada preocupada por brindar un servicio seguro y de calidad para los clientes, desea proponer un plan estratégico de ciberseguridad que permita establecer procedimientos preventivos para evitar los ciberataques.

El plan de ciberseguridad no solo se realiza cuando existe alguna falencia en las redes o el sistema de la empresa, sino que se puede emplear como una necesidad de

control para evitar riesgos o mejorar algún punto informático vulnerable, siendo desarrolladas por profesionales con conocimientos en dicha área.

En razón a lo antes expuesto, se propone realizar el plan estratégico de ciberseguridad mediante las normas de la Organización Internacional de Estandarización (ISO), las serie ISO/IEC 27000 las cuales se enfocan en la gestión de la seguridad de la información y prevenir diferentes tipos de riesgos, estas normativas se basan en identificar las vulnerabilidades y amenazas existentes. Asimismo, cumpliendo con las condiciones estipuladas de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) que se encarga de regular, administrar y controlar las telecomunicaciones del Ecuador.

De esa manera, obtener información pertinente que se utilice para lograr clasificar las vulnerabilidades y amenazas mediante prioridades, asimismo puedan ser resueltas realizando acciones correctivas y preventivas en el ámbito de seguridad informática dentro y fuera de la empresa.

CAPÍTULO 1

1.1 Planteamiento del problema

IN PLANET S.A., ubicada en Ecuador, provincia del Guayas, ciudad Milagro es una empresa dedicada a brindar el servicio de Internet, ventas de productos tecnológicos y soporte técnico. En tal sentido, la empresa antes mencionada cuenta con un área de sistema la cual es responsable de garantizar el correcto funcionamiento de los equipos tecnológicos disponibles en la empresa.

El personal del área de sistemas actualmente no se encuentra especializado en normativas de seguridad, asimismo la empresa no cuenta con un plan de gestión de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de la información cuando se suscite algún incidente de ciberataque, es así como, se propone la realización de un plan estratégico de ciberseguridad cumpliendo con la serie de las normativas ISO/IEC 27000 y las políticas de la ARCOTEL.

En razón a lo anteriormente expuesto, la problemática del presente caso de estudio es que existe un alto índice de insatisfacción de clientes relacionados por eventos de servicio no disponible, debido al incremento de incidentes de ciberataques en las redes de la empresa IN PLANET S.A., donde el tiempo en respuesta a solución de estos es excesivo.

¿Qué importancia tiene investigar el tema propuesto?

> Con la globalización digital de las empresas, compañías y gobiernos, los usuarios se han convertido cada día en blancos más atractivos para los criminales cibernéticos, quienes aprovechan la web para mantenerse en el anonimato mientras realizan sus ataques. Con la finalidad de minimizar las probabilidades de ser víctimas de ciberataques, han incrementado la inversión en una cultura de ciberseguridad (Gamboa, 2020).

En la actualidad, todas las empresas que brinden servicios de redes informáticas tienen la necesidad de recurrir a la inversión en la ciberseguridad, debido a que este tipo de empresas se encuentran más propensas a sufrir ciberataques, por parte de personas malintencionadas que desean causar daño a la reputación de la institución o a su vez causar pérdidas económicas que puedan afectar en gran manera al crecimiento de la misma.

> Los avances informáticos han posibilitado que un individuo que use un ordenador como arma pueda realizar acciones con la posibilidad de interferir en las dinámicas comerciales, financieras, de infraestructuras e incluso en los equipos médicos, teniendo la potencialidad de causar graves daños a un individuo, una organización comercial o gubernamental (Machin & Gazapo, 2016).

En consideración a lo expuesto, la importancia de realizar el presente trabajo de investigación es optimizar los procesos, métodos y procedimientos en la seguridad de la información que se utilizan en la empresa IN PLANET S.A., mediante un plan estratégico de ciberseguridad. Por lo tanto, la ciberseguridad es la protección del software, el hardware y los sistemas de datos conectados a Internet frente a los ciberataques. Como tal, la seguridad en el contexto informático comprende la seguridad física y la ciberseguridad; ambas son utilizadas por las organizaciones empresariales para impedir el acceso no autorizado a los sistemas informatizados y a los centros de datos.

Es por ello que, la seguridad de la información y sus riesgos se pueden llevar a cabo de manera muy dinámica, puesto a que tienen una tendencia de fácil adaptación en las distintas situaciones de la organización, con el objetivo de mantener o mejorar la eficiencia y eficacia al implementar controles y niveles de seguridad.

1.2 Objetivos

1.2.1 Objetivo General

Desarrollar un plan estratégico de ciberseguridad para la empresa INPLANET S.A, mediante la serie de las normativas ISO/IEC 27000 acorde con los lineamientos del modelo de seguridad y privacidad de la información de la política de Gobierno Digital establecido por el ente regulador ARCOTEL.

1.2.2 Objetivos Específicos

- Determinar las cusas de los ciberataques que afectan la disponibilidad del servicio de Internet en la empresa IN-PLANET S.A. de la ciudad de Milagro.
- Establecer mejores prácticas para la gestión de los riesgos e incidentes en temas de seguridad de la información en la empresa IN-PLANET S.A.
- Establecer criterios para la implementación de buenas prácticas de Ciberseguridad en la empresa IN-PLANET S.A.

1.3 Alcance

En el presente trabajo investigativo se tiene como alcance el desarrollo de un plan estratégico de ciberseguridad para la empresa IN PLANET S.A, mediante la serie de las normativas ISO/IEC 27000 y las políticas estipuladas por la ARCOTEL. En la institución antes mencionada la cual brinda servicio de Internet, tendrá una eficiente gestión de incidentes y vulnerabilidades aplicando procedimientos a seguir para la seguridad de la información y disponibilidad del servicio de Internet que se provee.

En razón a lo expuesto, se realizará una auditoria de seguridad informática con el objetivo de recopilar información pertinente sobre los diferentes equipos tecnológicos, software y sistemas operativos que se hayan instalados en la empresa IN PLANET S.A., basándose en las normativas ISO/IEC 27005.

Por tal motivo, se realizará un plan capacitación a todos los involucrados internos y externos de la empresa tales como: clientes, proveedores y empleados, con la finalidad de especificar y dar a conocer los procedimientos a seguir ante algún incidente de la seguridad de la información que afecte al correcto desempeño de la institución.

1.4 Estado del arte

> Durante los últimos años, los ataques informáticos se han direccionado constantemente a las organizaciones en los sectores de energía, servicios públicos y otros. Los ciberataques a infraestructuras críticas se han vuelto cada vez más complejos y difíciles de controlar, lo que hace que los sistemas informáticos se apaguen, interrumpan las operaciones, entre otros procesos malintencionados que puedan provocar los ciberdelincuentes (Roca, 2022).

Sin embargo, las tecnologías de seguridad y las mejores prácticas pueden ayudar a prevenir o reducir las consecuencias de una brecha y mitigar los riesgos asociados con los sistemas de control industrial conectados a Internet, así como las interrupciones y el impacto que un ataque pueda tener en una ciudad o país.

Por consiguiente, en este apartado se enfocará en conocer de manera conceptual los diferentes términos correspondientes a la ciberseguridad y asimismo trabajos similares que se hayan realizado, con la finalidad de tener un conocimiento ampliado sobre la temática del presente trabajo investigativo:

> **Amenaza**: Es cualquier evento que pueda explotar las vulnerabilidades. Causa potencial de un incidente indeseado, que puede resultar en daños para los sistemas, personas o la propia organización. Las amenazas poden ser clasificadas en: Amenazas intencionadas, Amenazas por acción de la naturaleza y Amenazas no intencionadas (ESCUELA SUPERIOR DE REDES RED CEDIA, 2019).
>
> Las ciberamenazas también se refieren a la posibilidad de un ciberataque con éxito cuyo objetivo es obtener acceso no autorizado, dañar, interrumpir o robar

un activo de tecnología de la información, una red informática, propiedad intelectual o cualquier otra forma de datos confidenciales. Las ciberamenazas pueden proceder de usuarios de confianza dentro de una organización o de ubicaciones remotas de personas desconocidas (TECNISEGUROS, 2022).

Política de Seguridad: Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. Una política de seguridad se define a alto nivel, esto es, qué se debe proteger y cómo, es decir, el conjunto de controles que se deben implementar. Esta se desarrolla en una serie de procedimientos e instrucciones técnicas que recogen las medidas técnicas y organizativas que se establecen para dar cumplimiento a dicha política. La definición de una política de seguridad debe estar basada en una identificación y análisis previo de los riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización (UNIR, 2020).

Una política de seguridad de la tecnología de la información (TI) identifica las reglas y los procedimientos para todas las personas que acceden y utilizan los activos y recursos de TI de una organización. La política de seguridad de TI eficaz es un modelo de la cultura de la organización, en el que las reglas y los procedimientos se basan en el enfoque de sus empleados sobre la información y el trabajo.

Por lo tanto, una política de seguridad de TI eficaz es un documento único para cada organización, desarrollado desde la perspectiva del personal encargado sobre la tolerancia al riesgo, cómo visualizan y valoran la información y la disponibilidad resultante que mantienen de la información. Por esta razón, muchas empresas encontrarán inapropiada una política de seguridad de TI inconsistente, debido a su falta

de consideración sobre la forma en que los empleados de la institución utilizan y comparten la información entre ellos y el público.

> **Riesgo**: Combinación de probabilidad (probabilidad de que la amenaza se concrete) de que un evento indeseado ocurra y de sus consecuencias para la organización. Es la incertidumbre resultante de la combinación de la probabilidad de la ocurrencia de un evento y sus consecuencias. En seguridad de la información, esta incertidumbre reside en los aspectos tecnológicos involucrados, en los procesos ejecutados y principalmente en las personas que en algún momento interactúan con la tecnología y se involucran con los procesos (ESCUELA SUPERIOR DE REDES RED CEDIA, 2019).

El término riesgo de seguridad de la información se refiere al daño que pueden causar los ataques contra los sistemas de TI. El riesgo de TI abarca una amplia gama de eventos potenciales, como filtraciones de datos, acciones de aplicación de normativas, costes financieros, daños a la reputación, y mucho más.

Aunque el riesgo a menudo se combina con la amenaza, los dos son ligeramente diferentes. Riesgo es un término más conceptual: algo que puede o no suceder y una amenaza es un peligro específico y real.

> **Seguridad de la información**: Es la protección de la información en relación con varios tipos de amenazas, a fin de garantizar la continuidad del negocio, minimizando los riesgos que puedan comprometerlo, y maximizando el retorno sobre las inversiones y las oportunidades de la organización. La seguridad de la información se logra mediante la implementación de un conjunto de controles: políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software (ESCUELA SUPERIOR DE REDES RED CEDIA, 2019).

La seguridad de la información es un conjunto de prácticas destinadas a mantener los datos seguros contra accesos no autorizados o alteraciones. Asimismo, se refiere a los procesos y herramientas diseñados e implementados para proteger la información empresarial confidencial de modificaciones, interrupciones, destrucción e inspección.

> **Seguridad Informática**: La seguridad informática también llamada ciberseguridad se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros (UNIR, 2021).

La seguridad informática es básicamente la protección de los sistemas informáticos y de la información frente a daños, robos y usos no autorizados. Existen varios tipos de seguridad informática que se utilizan ampliamente para proteger la información valiosa de una organización. Una forma de determinar las similitudes y diferencias entre la seguridad informática es preguntar qué se está protegiendo. Por ejemplo:

- La seguridad de la información es proteger la información contra el acceso, la modificación y la eliminación no autorizados.
- La seguridad de las aplicaciones protege una aplicación mediante la creación de funciones de seguridad para evitar amenazas cibernéticas como la inyección SQL, los ataques DoS, Filtraciones de datos, etc.
- La seguridad informática significa proteger un equipo independiente manteniéndolo actualizado y parcheado.

- La seguridad de la red consiste en proteger las tecnologías de software y hardware.

Los componentes de un sistema informático que se deben proteger son:

- **Hardware**: la parte física del ordenador, como la memoria del sistema y la unidad de disco.
- **Firmware**: software permanente grabado en la memoria no volátil del dispositivo de hardware y que es casi invisible para el usuario.
- **Software**: la programación que ofrece servicios, como sistema operativo, procesador de textos, navegador de internet al usuario.

De la misma manera, la seguridad informática se ocupa principalmente de tres áreas principales:

- La confidencialidad es garantizar que la información sólo esté disponible para el público al que va dirigida.
- La integridad está protegiendo la información contra la modificación por parte de partes no autorizadas.
- La disponibilidad está protegiendo la información contra la modificación por parte de partes no autorizadas.

Vulnerabilidad: "es cualquier debilidad que puede ser explotada para comprometer la seguridad de sistemas de la información. Fragilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas" (ESCUELA SUPERIOR DE REDES RED CEDIA, 2019, pág. 22).

Una vulnerabilidad es una debilidad o un error en el código de un sistema o dispositivo que, cuando se explota, puede poner en peligro la confidencialidad, disponibilidad e integridad de los datos almacenados en ellos mediante el acceso no

autorizado, la elevación de privilegios o la denegación de servicio. Un código o herramienta que se utiliza para aprovechar una vulnerabilidad se denomina exploit.

A continuación en la siguiente sección, se indicará los antecedentes más recientes relacionados con el tema de estudio del presente trabajo investigativo, en donde la ciberseguridad es el eje principal de la investigación:

> La seguridad informática se basa principalmente en tres pilares fundamentales: integridad, disponibilidad y confidencialidad. Estos pilares deben de ser forjados mediante el uso de herramientas, la implementación de políticas y el cumplimiento de procesos. Es aquí donde interviene el rol de un especialista en seguridad informática. Los especialistas de seguridad informática son los idóneos para determinar si un sistema o servicio es seguro y para ello se realizan una serie de análisis que ayudarán a determinar si el objeto de estudio cumple con los tres conceptos fundamentales (Alvarado & Changoluisa, 2019).
>
> La Ciberseguridad es una pieza crítica dentro de la política de seguridad IT integral de las empresas para asegurar la continuidad del negocio, y el mayor desafío de las organizaciones actuales (independientemente de su tamaño o actividad) es la implementación de un Plan de Ciberseguridad, debido a las nuevas tecnologías y al uso extensivo de internet, generando una red en el que la mayoría de los elementos y objetos de uso cotidianos están conectados, por lo cual se denominan, internet en las cosas (Amancha & Freddy, 2020).
>
> La Seguridad en las Empresas Públicas, encuentra un espacio para ser consolidado, como la necesidad de encontrar soluciones que permitan disminuir las vulnerabilidades. Por otra parte, el estudio permite discriminar las alteraciones en las seguridades, permitiendo que mejore la calidad de la conservación de los datos, sin arriesgar la seguridad de la información. El uso de

plataformas de seguridad, pueden ser aplicados de manera directa e indirecta, como un soporte para contribuir a la Gestión de las instituciones Públicas con el constante crecimiento de vulnerabilidades, el manejo de los recursos tecnológicos ha tenido que incrementar la incorporación de tecnologías de seguridad, las cuales no evitan, pero si disminuyen las incidencias de acceso no autorizado (Morán, 2021).

En razón a lo expuesto anteriormente, se indica que la ciberseguridad es de vital importancia para todas las instituciones que desean optimizar la seguridad de la información que tienen almacenada. Las tecnologías de comunicación integradas en diversos sistemas de control exponen a riesgos las infraestructuras y organizaciones, es por ello que, mientras más dispositivos inteligentes estén conectados y asimismo conectados a redes de infraestructura crítica, mayor será la superficie de ataque y los posibles daños. Por ejemplo, un sensor inteligente vulnerable conectado a Internet puede actuar como puerta de enlace para desplegar ataques o poner en peligro otros sistemas críticos de la misma red, si los agentes de amenazas lo ponen en peligro.

En consecuencia, la identificación de vulnerabilidades y la obtención de visibilidad del número de dispositivos inteligentes y su función dentro de la infraestructura pueden ayudar a reducir el riesgo de un ciberataque exitoso. Por tal motivo, es importante mantener un inventario detallado de todos los dispositivos tecnológicos, comprobar constantemente nuevas actualizaciones de seguridad que aborden vulnerabilidades conocidas y mantenerlas en una red segregada que esté completamente aislada de otros sistemas críticos.

La ISO27005:2018 es un conjunto de lineamientos con un enfoque en seguridad informática usada para el desarrollo de este proyecto como un conjunto de directrices orientados en la gestión de riesgos de seguridad de la información

> basada en un ciclo PHVA que permite la identificación del alcance del sistema y a partir de allí se reconocen los activos con sus respectivos escenarios de riesgos a los cuales se les realiza una evaluación del impacto de acuerdo a las probabilidades que se puedan presentar, con el objeto de identificar los riesgos que son inadmisibles para las organizaciones a fin de iniciar procesos de priorización que permiten la implementación de controles enmarcados dentro de un plan de tratamiento que debe ser medible, monitoreado y comunicado a toda la organización dentro de ciclos iterativos que permitan la implementación de estrategias enfocadas a la mejora continua (Giraldo, 2021).

En la tesis antes mencionada, expone que mediante los lineamiento de seguridad que brinda la ISO27005 para identificar los riesgos existentes de la seguridad de la información que se encuentran en la empresa IN PLANET S.A., con la finalidad de realizar una gestión preventiva y correctiva de los riesgos que se encuentren mediante el monitoreo que se realice por parte de personal autorizado y capacitado en seguridad informática.

> La ciberseguridad de los sistemas TO, en particular, se ve comprometida por vulnerabilidades sobrevenidas en un entorno con exigencias de seguridad específicas orientadas a la producción y considerablemente diferenciadas de las exigencias y estándares de los sistemas de información corporativos. A ello hay que añadir un escenario de crecientes amenazas de distinta naturaleza, bien intencional o accidental (errores, fraudes, espionaje, sabotaje, causas naturales, etc.), canalizadas en su mayor parte a través del ciberespacio y en no pocas ocasiones dirigidas a perturbar desde terceros países el funcionamiento de las infraestructuras críticas por razones geopolíticas o económicas (Gómez & Valencia, 2021).

Como respuesta a esta situación, gobiernos como el de Estados Unidos vienen trabajando en estrategias que proporcionan al Departamento de Seguridad Nacional un marco para identificar las responsabilidades de seguridad cibernética durante los próximos cinco años. De esta manera buscan mantener el ritmo del panorama de riesgo cibernético en evolución, mediante la reducción de las vulnerabilidades y la creación del concepto de ciber resiliencia; contrarrestar a los actores maliciosos en el ciberespacio; responder a incidentes, además de que el ecosistema cibernético sea más seguro y resistente. Igualmente actores de alcance regional y global articulados desde instituciones como el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA), gobiernos de la región y organizaciones multilaterales vienen trabajando de manera conjunta para enfrentar los retos de la ciberseguridad, desde la generación de políticas de ciberseguridad fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, y la protección de infraestructuras críticas entre otros (Gómez & Valencia, 2021).

En conclusión de lo expuesto anteriormente, se puede indicar que una sólida infraestructura de seguridad incluye varias capas de protección dispersas por los equipos, programas y redes de una empresa, donde los ataques cibernéticos se presentan en todas las formas y algunos pueden ser ataques manifiestos de ransomware (secuestrar importantes productos o herramientas empresariales a cambio de dinero para liberarlos), mientras que otros son operaciones encubiertas por las que los delincuentes se infiltran en un sistema para obtener datos valiosos que sólo se descubren meses después del hecho, si es que se descubren.

CAPÍTULO 2

2.1 Metodología

En el siguiente apartado se desarrolló mediante la Metodología de Gestión de Riesgos ISO/IEC 27005:2018 que se caracteriza como un estándar internacional que describe cómo realizar una evaluación de riesgos de seguridad de la información de acuerdo con los requisitos de la ISO 27001.

ISO/IEC 27005 es una norma internacional publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Para ser más específico, esta normativa se basa en la seguridad de la información mediante un enfoque de gestión de riesgos.

Según la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) expuso sobre la ISO 27005 que:

> Esta norma describe todo el proceso necesario para la gestión del riesgo de seguridad de la información y las actividades necesarias para la perfecta ejecución de la gestión. Presenta prácticas para gestión del riesgo de la seguridad de la información. Las técnicas en ella descritas siguen el concepto, los modelos y los procesos globales especificados en la norma ICONTEC NTC-ISO/IEC 27001, además de presentar la metodología de evaluación y tratamiento de los riesgos requeridos por la misma norma. (ESCUELA SUPERIOR DE REDES RED CEDIA, 2019)

La ISO/IEC 27005:2018 que forma parte de la norma ISO 27000 desde 2008, establece las mejores prácticas de gestión de riesgos específicamente orientadas a la gestión de riesgos para la seguridad de la información, en particular en lo que respecta al cumplimiento de los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI), según lo establecido por ABNT NBR ISO/IEC 27001.

Por consiguiente, la gestión de riesgos en relación con la seguridad de la información debe definir el contexto, evaluar los riesgos y abordarlos a través de un plan, con el fin de implementar las recomendaciones y decisiones. La gestión de riesgos analiza los eventos potenciales y sus consecuencias antes de decidir qué hacer y cuándo hacerlo, a fin de reducir los riesgos a un nivel aceptable.

Las evaluaciones de riesgos son una de las partes más importantes del proyecto de cumplimiento de la norma ISO 27001 de una organización. La norma ISO 27001 requiere que demuestre la existencia de pruebas de la gestión de riesgos de seguridad de la información, las acciones de riesgo adoptadas y la aplicación de los controles pertinentes.

Las directrices ISO 27005 son un subconjunto de una gama más amplia de prácticas recomendadas para evitar filtraciones de datos en la organización. La especificación proporciona orientación sobre la identificación, evaluación y tratamiento formales de las vulnerabilidades de seguridad de la información, procedimientos que son fundamentales para un sistema de gestión de la seguridad de la información.

En el mundo interconectado, globalizado y dependiente de la tecnología digital, los ciberataques han llegado a ser una de las principales preocupaciones. Además, la nueva legislación, como el Reglamento General de Protección de Datos (RGPD), ha presionado a las organizaciones a mantener su información segura. En general, el riesgo es abundante, y la necesidad de reconocer y abordar el persistente potencial de filtraciones de datos hace que la norma ISO/IEC 27005:2018 sea tan significativa.

El objetivo de la ISO/IEC 27005:2018 es asegurar que las organizaciones planifiquen, ejecuten, administren, supervisen y administren racionalmente sus controles de seguridad de la información y otros arreglos relacionados con sus riesgos de seguridad de la información.

Es por ello que, esta metodología implica un proceso continuo de gestión de riesgos de información basado en seis componentes claves:

- ✓ Establecimiento del contexto.
- ✓ Evaluación de riesgos.
- ✓ Tratamiento de riesgos.
- ✓ Aceptación de riesgos.
- ✓ Comunicación de riesgos.
- ✓ Supervisión y revisión de riesgos.

En razón a lo expuesto anteriormente, se detallará cada una de las fases que indica la ISO/IEC 27005:2018:

Establecimiento del contexto: En esta primera fase, la contextualización consiste en determinar dónde comienza y dónde termina la gestión de riesgo. Es por ello que, el contexto de la gestión de riesgos establece los criterios para identificar los riesgos, quién es responsable de la propiedad del riesgo, cómo los riesgos afectan a la confidencialidad, integridad y disponibilidad de la información, y cómo se calculan el impacto y la probabilidad del riesgo.

Por lo tanto, se establecen una serie de criterios:

- Los criterios de evaluación le ayudan a identificar los activos amenazados por los riesgos cibernéticos y los umbrales por encima de los cuales se deben abordar los riesgos.
- Los criterios de impacto corresponden al nivel mínimo de consecuencias, por encima del cual se debe tener en cuenta un riesgo.
- Los criterios de aceptación del riesgo representan un umbral, por debajo del cual se puede tolerar el riesgo.

Evaluación de riesgos: Durante esta fase, primero se determinará los elementos que se encuentra en riesgo, tales como: la organización en su conjunto, pero también los sistemas de información, los servicios y los grupos de datos. A continuación, tendrá que realizar el proceso de identificar las amenazas y vulnerabilidades que giran en torno con las necesidades de seguridad de la estructura de la institución.

Por consiguiente, el proceso antes realizado le ayudará a clasificar las prioridades según los criterios de evaluación que se definió en la primera fase. Aunque el estándar ISO 27005 ayuda a identificar vulnerabilidades de ciberseguridad, no ofrece una escala de clasificación de riesgos. Por tal motivo, el equipo encargado deberá aplicar las normativas de evaluación mediante la construcción de un sistema de evaluación propio. Este sistema puede basarse en aspectos cualitativos o cuantitativos

Muchas organizaciones deciden seguir un proceso de evaluación de riesgos basado en activos que consta de cinco etapas clave:

- Compilación de activos de información.
- Identificar las amenazas y vulnerabilidades aplicables a cada activo.
- Asignar valores de impacto y probabilidad basados en criterios de riesgo.
- Evaluar cada riesgo frente a niveles predeterminados de aceptabilidad.
- Priorizar los riesgos que deben abordarse y en qué orden.

Tratamiento de riesgos: Durante esta fase, la estructura debe establecer objetivos de seguridad de la tecnología de información teniendo en cuenta los resultados obtenidos durante la segunda fase, una vez establecidos esos objetivos se puede elaborar un borrador de las especificaciones, lo que debería ayudar a diseñar medidas para tratar los riesgos.

En esta metodología, conceptualizar estas medidas significa comparar un riesgo con su coste de tratamiento. A continuación, surgen cuatro formas de tratar un riesgo:

- **Rechazo o Evitación**: Evitar el riesgo eliminándolo por completo en donde la institución deberá considerar que el riesgo cibernético es demasiado grave y afirmar que debe evitarse de cualquier manera. A continuación, puede decidir poner fin a la actividad que pueda causarla.
- **Transferencia**: Compartir el riesgo con un tercero a través de seguros o externalización, en donde la estructura de la institución comparte el riesgo con un tercero, un subcontratista de seguros o ciberseguridad, capaz de protegerlo del riesgo, al menos financieramente.
- **Mitigación**: Modificar el riesgo aplicando controles de seguridad, en donde el personal encargado deberá diseñar medidas para mitigar el impacto o la probabilidad de ocurrencia de un riesgo con el fin de hacerlo más tolerable.
- **Conservación**: el riesgo se considera soportable y no suficiente de una amenaza, su estructura decide no abordarlo.

Aceptación del riesgo: La institución debe determinar criterios propios para la aceptación del riesgo, se debe tener en cuenta las políticas, metas, objetivos e intereses de los accionistas existentes.

La estrategia de tratamiento de riesgos y los riesgos residuales deben pasar por una fase de aceptación, durante esta fase, los jefes de departamento pueden cuestionar los costes que consideran demasiado altos o considerar aceptar ciertos riesgos, por las cuales estas excepciones deben justificarse.

En conclusión, la metodología ISO 27005 termina aquí teóricamente, aunque se debe tener en cuenta que todo el trabajo que la institución ha realizado para implementarla puede ser utilizado como parte de un procedimiento de monitoreo y

revisión. Debido a que, proporciona una historia de los riesgos que se han identificado, los escenarios que se han imaginado, el análisis de riesgos que se ha realizado y las estrategias de tratamiento que se han establecido.

Por supuesto, esta metodología debería repetirse si las amenazas y vulnerabilidades evolucionaran y asimismo puede servir como un apoyo para la comunicación con sus partes interesadas.

Comunicación y consulta de riesgos: Una comunicación eficaz es fundamental para el proceso de gestión de riesgos de seguridad de la información, debido a que garantiza que los responsables de la implementación de la gestión de riesgos comprendan la base sobre la que se toman las decisiones y por qué se requieren ciertas acciones.

Por consiguiente, compartir e intercambiar información sobre el riesgo también facilita el acuerdo entre los responsables de la toma de decisiones y otros interesados sobre cómo manejar el riesgo. La actividad de comunicación de riesgos debe realizarse continuamente, y las organizaciones deben desarrollar planes de comunicación de riesgos para operaciones normales, así como para situaciones de emergencia.

Supervisión y revisión de riesgos: Los riesgos no son estáticos y pueden cambiar bruscamente. Por lo tanto, deben ser monitoreados continuamente para identificar rápidamente los cambios y mantener una visión completa del panorama de riesgo. A diferencia de otros estándares populares de gestión de riesgos que adoptan un enfoque único, la norma ISO 27005 es de naturaleza flexible y permite a las organizaciones seleccionar su propio enfoque para la evaluación de riesgos basándose en sus objetivos empresariales específicos.

CAPÍTULO 3

3.1 Propuesta de solución

En la actualidad, los ataques cibernéticos pueden tener impactos devastadores en una empresa, que van desde pérdidas financieras, retenciones operativas, daños a la reputación, crisis legales y regulatorias e incluso el riesgo de que la empresa se cierre de forma permanente. Por tal motivo, una estrategia de ciberseguridad sólida reduce en gran medida las posibilidades de que su empresa caiga presa de un ciberdelincuente y mitiga las repercusiones anteriores si se produjera un incidente de seguridad.

En tal sentido, una estrategia de ciberseguridad está compuesta por planes de alto nivel sobre cómo una organización va a proteger sus activos y minimizar el riesgo cibernético. Al igual que una política de ciberseguridad, la estrategia de ciberseguridad debe ser un documento vivo y respirable, adaptable al panorama actual de amenazas y al clima empresarial en constante evolución. Normalmente, las estrategias de ciberseguridad se desarrollan con una visión de tres a cinco años, pero deben actualizarse y revisarse con la mayor frecuencia posible.

Entonces, un enfoque de ciberseguridad proactivo no solo le sitúa por delante de los atacantes, sino que también le puede ayudar a mantener e incluso superar los requisitos normativos. Las estrategias proactivas ofrecen la estructura y la orientación que le ayudan a mantenerse preparado y evitar la confusión que pueda surgir. Con la minimización de la incertidumbre y la confusión, las medidas de prevención, detección y respuesta a incidentes mejoran drásticamente.

3.1.1 Razones de Ausencia de Disponibilidad de Servicio de Internet por ciberataques

Falta de asistencia de seguridad: Muy pocas personas son conscientes de los pasos más simples para aumentar la seguridad cibernética. Además, la mayoría no tiene

fácil acceso a los recursos que necesitan, cuando los necesitan. Tome contraseñas. Se sabe que cuanto más fuerte sea su contraseña, más segura será su cuenta.

Vulnerabilidades del sistema: Cuando los ciberdelincuentes detectan una debilidad, se abalanzan sobre ella. Es por eso que las vulnerabilidades del sistema pueden ser tan peligrosas. Minimizar la amenaza de tales ataques requiere un enfoque reactivo y preventivo combinado. Además de tener el software de seguridad y la configuración de red adecuados, es importante mantener el software actualizado. Esto significa instalar actualizaciones de software y parches tan pronto como estén disponibles, ya que pueden corregir vulnerabilidades.

3.1.2 Mejores prácticas para la gestión de los riesgos e incidentes

Los atacantes cibernéticos encuentran constantemente nuevas formas de acceder a datos confidenciales, por lo que la detección de amenazas se ha vuelto más desafiante. Además, con la reciente tendencia del trabajo remoto y la concesión de acceso privilegiado a numerosos empleados, los usuarios privilegiados y remotos se encuentran ahora entre los principales actores internos.

Por consiguiente, lo principal para gestionar correctamente los riesgos e incidentes es construir una comunicación efectiva con todos los empleados, así como lograr educarlos sobre las posibles amenazas de ciberseguridad y formas de mitigarlas. A continuación se mencionan algunas de las prácticas más importantes para evitar ataques cibernéticos:

- **Emplear un enfoque de seguridad centrado en las personas**: Las personas pueden ser su mayor riesgo de seguridad o su defensa de seguridad más fuerte. Hoy en día, un enfoque centrado en la tecnología para la ciberseguridad no es suficiente para garantizar una protección integral porque los atacantes cibernéticos a menudo utilizan a las personas como punto de entrada. Es por eso

que es mejor utilizar un enfoque centrado en las personas para mitigar los riesgos relacionados con los humanos.

Es vital comprender la importancia de los trabajadores para la ciberseguridad, así como los peligros que pueden plantear. Educar y monitorear a los empleados son las dos cosas principales a considerar para lograr la defensa de su entorno cibernético.

- **Reducir el nivel de negligencia de los empleados**: Esto implica ayudar a los empleados a comprender por qué es vital seguir las reglas de ciberseguridad mediante un plan de concientización de la seguridad de la información. Por tal motivo, se deberá tratar a los empleados como parte de defensa y se evidenciará que los casos de negligencia y errores se vuelven menos frecuentes. Se recomienda mejor enseñar a los empleados las mejores prácticas de ciberseguridad en la capacitación adecuada, que lidiar con una violación de datos causada por acciones accidentales.
- **Informar a los empleados sobre técnicas comunes de phishing**: Esto implica capacitar a los empleados a cómo evitar este tipo de ataque, debido a que los atacantes cibernéticos a menudo utilizan técnicas de phishing para obtener las credenciales de los empleados e infectar los sistemas de una organización con malware, o para adquirir información financiera de los empleados.
- **Proteger el acceso desde dispositivos remotos**: Esto implica garantizar eficientemente la gestión del acceso para cualquier tipo de usuario.

  Proteger el acceso a los datos confidenciales desde cualquier ubicación y dispositivo es fundamental para la institución.

- **Gestionar las contraseñas eficientemente**: Las credenciales de acceso de los usuarios con un privilegio que manipulan información sustancial para la empresa se convierte en un punto clave para los ciberdelincuentes, debido a que intentan obtener acceso a los datos confidenciales.
- **Gestionar copias de seguridad de la información**: Esto implica gestionar eficientemente respaldos de la información mediante copias de seguridad de manera periódica. Debido a que, con la llegada del ransomware, es muy importante tener copias de seguridad completa y actual de todos los datos. La copia de seguridad de los datos es una de las mejores prácticas de seguridad de la información que ha adquirido una mayor relevancia en los últimos años.
- **Aplicar políticas de ciberseguridad**: Esto implica adaptar normas y reglamentos para la empresa que va a servir como una guía formal para todas las medidas de ciberseguridad utilizadas en la empresa, en consecuencia, va a permitir que los especialistas en seguridad y los empleados tengan el conocimiento de las normativas a cumplir.
- **Realizar auditorías de ciberseguridad periódicas**: Esto implica que el análisis oportuno de acciones o movimientos extraños de los empleados, usuarios privilegiados o proveedores externos es clave para lidiar con incidentes repentinos de manera oportuna. La calidad de una auditoría depende de la integridad de los datos recopilados de diferentes maneras o que se encuentran en varias fuentes: registro de auditoría, registros de sesión, metadatos, entre otros.
- **Simplificar la infraestructura tecnológica**: Esto implica que al tener demasiadas herramientas de ciberseguridad pueden dificultar la detección de amenazas.

  Si la infraestructura de ciberseguridad de la empresa está dirigida a disminuir el

riesgo de violaciones de datos, entonces no debe contener demasiadas partes y dividirse entre diferentes soluciones.

- **Emplear seguridad biométrica**: La biometría garantiza una autenticación rápida, una gestión de acceso segura y un monitoreo preciso de los empleados. El reconocimiento de voz, los escaneos de huellas dactilares, la biometría de la palma de la mano y el comportamiento, el reconocimiento, entre otras, son opciones perfectas para identificar si los usuarios son quienes dicen ser. Verificar las identidades de los usuarios antes de proporcionar acceso a activos valiosos es vital para la empresa. La biometría proporciona una autenticación más confiable que las contraseñas y la verificación por SMS, es por eso que la biometría ya se ha convertido en una parte esencial de la autenticación multifactor.

3.1.3 Criterios de buenas prácticas de ciberseguridad

En razón a lo expuesto anteriormente, con la finalidad de garantizar la seguridad de la información se desarrollará un plan estratégico de ciberseguridad para la empresa INPLANET S.A., mediante la metodología ISO/IEC 27005, con la finalidad de obtener una visión detallada de las posibles amenazas cibernéticas en la empresa y las capacidades para gestionar los riesgos asociados.

En tal virtud, se debe contemplar las siguientes fases para elaboración del plan de ciberseguridad:

3.2 Plan Estratégico de Ciberseguridad

3.2.1 Fase 1: Conocer la situación actual de la empresa

INPLANET S.A. es una empresa de soluciones y asistencia para el servicio de Internet, ventas de productos tecnológicos, soporte técnico y mucho más, actualmente cuenta con varias sucursales: Milagro, Babahoyo, Montalvo, Samborondón y Naranjito.

Análisis Técnico de Seguridad: Una auditoria informática tiene como finalidad la evaluación de los sistemas computacionales efectuado por profesionales en el área de

ciberseguridad, que busca identificar, describir y enumerar las vulnerabilidades que pueden existir en las redes de comunicaciones o servidores.

Una vez detectados los posibles problemas de seguridad podrá reducir el riesgo de la institución mediante la planificación y priorización de las mejoras de seguridad con respecto al procesamiento y almacenamiento de datos. En base a la importancia de este proceso, es necesario demostrar el compromiso con los procesos de aseguramiento de la información y generar confianza en los clientes, socios y organismos reguladores para garantizar un aseguramiento de los sistemas.

Dentro del proceso de auditoría externa se verifico y efectuó las siguientes fases:

- Enumeración de redes, topologías y protocolos externos
- Identificación de puertos y Sistemas Operativos instalados para los sitios públicos.
- Análisis de servicios y aplicaciones publicadas.
- Detección, comprobación y evaluación de vulnerabilidades de los sitios públicos.
- Informe Técnico de Resultados.

Por consiguiente, se detalla a continuación el listado de equipos de comunicación que se encuentran habilitados actualmente:

Red externa (44 Dispositivos)

Tabla 1 Tipos de Activos Informáticos Red Externa.

Dirección IP	Tipo de activo informático (APP WEB, BDD, WEBSITE, WEBSERVICE, ETC)
138.122.109.193	ROUTER
138.122.108.77	ROUTER
138.122.109.65	ROUTER
138.122.109.129	ROUTER
138.122.109.89	ROUTER
138.122.110.193	ROUTER
138.122.109.130	ROUTER
138.122.108.73	ROUTER
138.122.109.189	ROUTER
138.122.110.1	ROUTER
138.122.110.177	ROUTER
138.122.109.1	ROUTER
138.122.108.1	ROUTER
138.122.109.145	ROUTER
138.122.108.229	ROUTER
179.51.142.1	ROUTER
138.122.108.26	DNS
138.122.108.29	DNS
179.51.140.8	MONITOREO
179.51.140.3	WEBSITE
138.122.108.16	WEBSITE

138.122.108.15	WEBSITE
138.122.108.13	WEBSITE
138.122.108.19	BDD
138.122.108.8	WEBSITE
138.122.108.14	WEBSITE
138.122.108.6	WEBSITE
138.122.108.12	GITLAB
138.122.108.11	ONLYOFFICE WEB
138.122.108.23	CLOUD
138.122.108.30	DNS
138.122.108.24	WEBSITE
138.122.108.28	WEBSITE,BDD
179.51.140.2	WEBSITE
179.51.140.5	WEBSITE
179.51.140.6	WEBSITE
138.122.108.10	WEBSITE,MAILSERVER
138.122.108.4	WEBSITE,REPOSITORIO
179.51.140.16	WEBSITE,APP
179.51.143.251	WEBSITE,APP
138.122.108.27	WEBSITE
138.122.108.25	SAMBA
179.51.140.187	WEBSITE
179.51.141.123	WEBSITE

Fuente: Elaboración Propia

La mayor cantidad de tipos de fallos que se encontraron representan un riesgo de seguridad de categoría media con un total de 8.59%, mientras que las vulnerabilidades de riesgo crítico representan 3.07%.

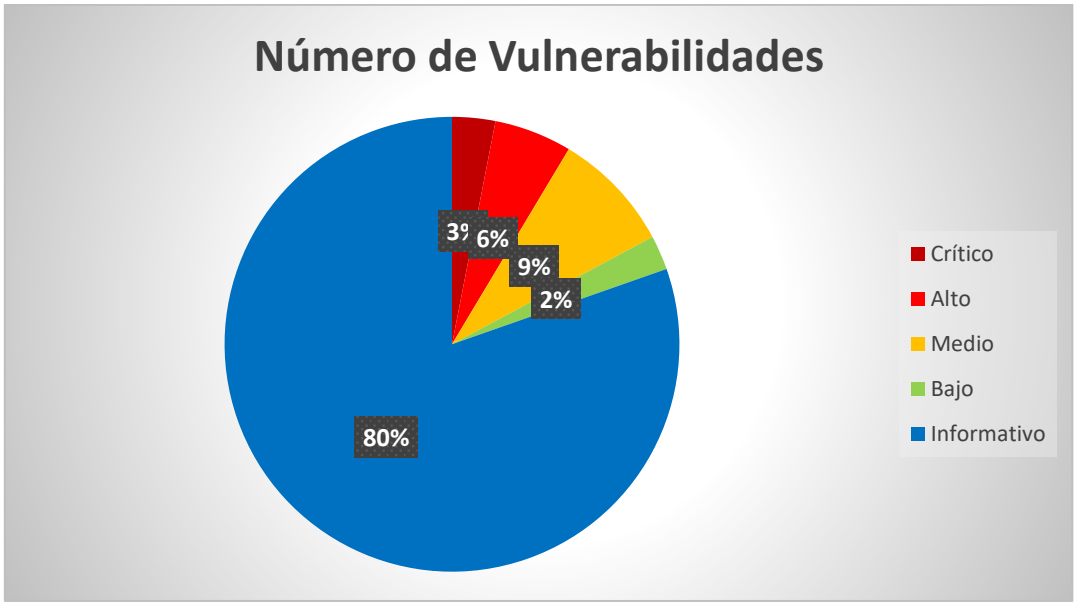


Figura 1 Distribución de vulnerabilidades por dirección IP Red Externa – Gráfico 1.

En la siguiente tabla de Distribución de vulnerabilidades por dirección IP Red Externa, se puede identificar la cantidad de vulnerabilidades encontradas en los dispositivos agrupados por nivel de riesgo.

Tabla 2 Distribución de vulnerabilidades por dirección IP Red Externa.

Host	Crítico	Alto	Medio	Bajo	Info	Total general
138.122.108.229		1			16	17
138.122.109.129					9	9
138.122.109.130					2	2
138.122.109.145		1			10	11
138.122.109.189					9	9
138.122.109.193					9	9
138.122.110.177					7	7

138.122.110.193					9	9
138.122.108.1					7	7
138.122.108.10	4	4	7	4	76	95
138.122.108.11					10	10
138.122.108.12			1		33	34
138.122.108.13	1	1	6		34	42
138.122.108.14			3		32	35
138.122.108.15			3		31	34
138.122.108.16			2		31	33
138.122.108.19					16	16
138.122.108.23			1		27	28
138.122.108.24	2	1	4		32	39
138.122.108.25			1		28	29
138.122.108.26					14	14
138.122.108.27	2	3	7		33	45
138.122.108.28			2		31	33
138.122.108.29					12	12
138.122.108.4	1		1		34	36
138.122.108.6					17	17
138.122.108.73					9	9
138.122.108.77					9	9
138.122.108.8			2		32	34
138.122.109.1					7	7
138.122.109.65					9	9

138.122.109.89					9	9
138.122.110.1					11	11
179.51.140.16		2	3		35	40
179.51.140.187			1		23	24
179.51.140.2		1	4		26	31
179.51.140.3	1		2		33	36
179.51.140.5			1		24	25
179.51.140.6			1		14	15
179.51.140.8	1		1		38	40
179.51.141.123			1		23	24
179.51.142.1					6	6
179.51.143.251					9	9
138.122.108.30						-
Total	12	14	54	4	886	970

Fuente: Elaboración Propia

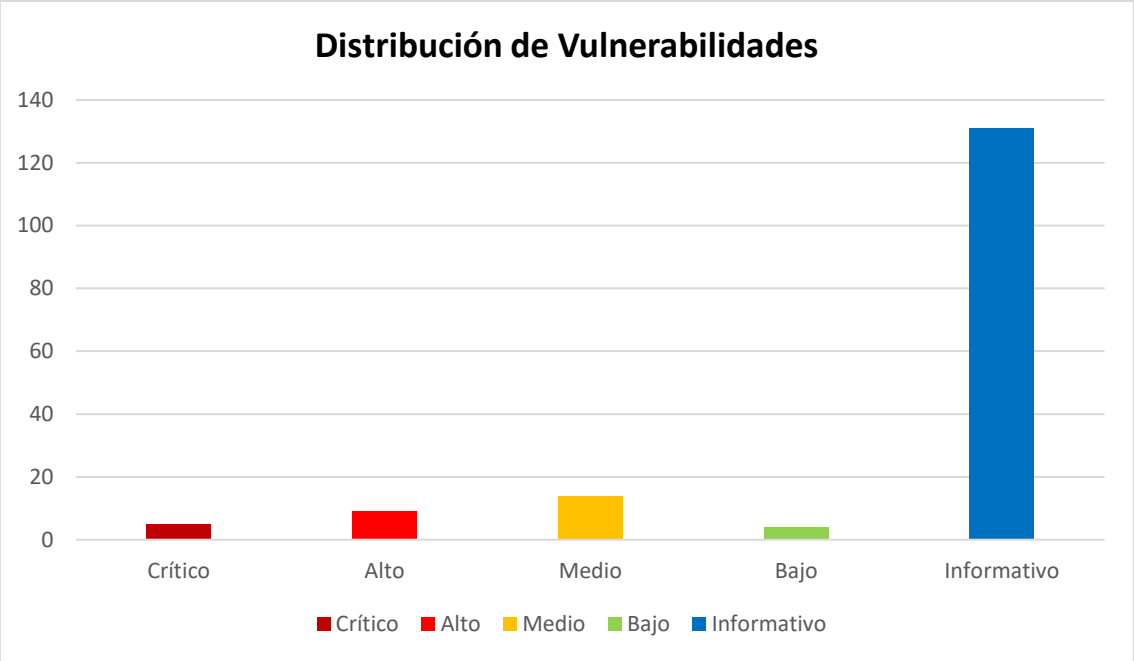


Figura 2 Distribución de vulnerabilidades por dirección IP Red Externa – Gráfico 2.

A continuación, se muestra el detalle de las vulnerabilidades con sus respectivas remediaciones por aplicar en función de su nivel de criticidad.

Tabla 3 Riesgos Críticos Red Externa.

Nombre	Riesgo	Recomendación
Apache < 2.4.49 Multiple Vulnerabilities	Crítico	Actualizar a Apache versión 2.4.49 o posterior.
Apache 2.4.x < 2.4.47 Multiple Vulnerabilities	Crítico	Actualizar a Apache versión 2.4.47 o posterior.
Apache 2.4.x < 2.4.52 Multiple Vulnerabilities	Crítico	Actualizar a Apache versión 2.4.52 o posterior.
nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE	Crítico	Actualizar a nginx 1.20.1 o posterior.
Python Unsupported Version Detection	Crítico	Actualizar a una versión de Python que se admite actualmente

Fuente: Elaboración Propia

Tabla 4 Riesgos Altos Red Externa.

Nombre	Riesgo	Recomendación
Apache >= 2.4.17 < 2.4.49 mod_http2	Alto	Actualizar a Apache versión 2.4.49 o posterior.
Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi	Alto	Actualizar a Apache versión 2.4.49 o posterior.
MTA Open Mail Relaying Allowed (thorough test)	Alto	Volver a configurar el servidor SMTP para que no se pueda utilizar como una retransmisión SMTP indiscriminada. Asegúrese de que el servidor utiliza los controles de acceso adecuados para limitar la medida en que es posible la retransmisión.
nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities	Alto	Actualizar a nginx versión 1.16.1 / 1.17.3 o posterior.
NTMail3 Arbitrary Mail Relay	Alto	Volver a configurar el servidor SMTP para que no se pueda utilizar como una retransmisión SMTP indiscriminada. Asegúrese de que el servidor utiliza los controles de acceso adecuados para limitar la medida en que es posible la retransmisión.
PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x < 8.0.2 DoS	Alto	Actualizar a php versión 7.3.27, 7.4.15, 8.0.2 o posterior.
PHP 7.3.x < 7.3.32	Alto	Actualizar a php versión 7.3.32 o posterior.
SNMP Agent Default Community Name (public)	Alto	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza. Filtrar los paquetes UDP entrantes que van a este puerto o

		cambie la cadena de comunidad predeterminada.
SSL Medium Strength Cipher Suites Supported (SWEET32)	Alto	Volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.

Fuente: Elaboración Propia

Tabla 5 Riesgos Medio Red Externa.

Nombre	Riesgo	Recomendación
HSTS Missing From HTTPS Server (RFC 6797)	Medio	Configurar el servidor web remoto para que utilice HSTS.
HTTP TRACE / TRACK Methods Allowed	Medio	Deshabilitar estos métodos HTTP. Consulte la salida del plugin para obtener más información.
JQuery 1.2 < 3.5.0 Multiple XSS	Medio	Actualizar a JQuery versión 3.5.0 o posterior.
nginx < 1.17.7 Information Disclosure	Medio	Actualizar a nginx versión 1.17.7 o posterior.
nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilities	Medio	Actualizar a nginx 1.14.1 / 1.15.6 o posterior.
PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error	Medio	Actualizar a php versión 7.3.26, 7.4.14, 8.0.1 o posterior.
PHP 7.3.x < 7.3.33	Medio	Actualizar a php versión 7.3.28 o posterior.
SMB Signing not required	Medio	Aplicar la firma de mensajes en la configuración del host. En Windows,

		esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft:
SSL Anonymous Cipher Suites Supported	Medio	Volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados débiles.
SSL Certificate Cannot Be Trusted	Medio	Comprar o generar un certificado SSL adecuado para este servicio.
SSL Certificate with Wrong Hostname	Medio	Comprar o generar un certificado SSL adecuado para este servicio.
SSL Self-Signed Certificate	Medio	Comprar o generar un certificado SSL adecuado para este servicio.
SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	Medio	Configurar los servidores SSL/TLS para que solo usen TLS 1.1 o TLS 1.2 si es compatible. Configurar los servidores SSL/TLS para que solo admitan conjuntos de cifrado que no utilicen cifrados por bloques. Aplicar parches si están disponibles.
TLS Version 1.0 Protocol Detection	Medio	Habilitar la compatibilidad con TLS 1.2 y 1.3, y Deshabilitar la compatibilidad con TLS 1.0

Fuente: Elaboración Propia

Tabla 6 Riesgos Bajos Red Externa.

Nombre	Riesgo	Recomendación
POP3 Cleartext Logins Permitted	Bajo	Ponerse en contacto con su proveedor para obtener una solución o cifrar el tráfico con SSL / TLS usando stunnel.
SSH Server CBC Mode Ciphers Enabled	Bajo	Ponerse en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
SSH Weak Key Exchange Algorithms Enabled	Bajo	Ponerse en contacto con el proveedor o consultar la documentación del producto para desactivar los algoritmos débiles.
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Bajo	Reconfigurar el servicio para utilizar un módulo Diffie-Hellman único de 2048 bits o superior

Fuente: Elaboración Propia

En base a los riesgos de seguridad detectados se deben realizar cambios para mitigar los problemas en la seguridad, por lo que se sugiere seguir un plan de remediación que considere corregir los fallos más críticos con prioridad, y los menos severos después, considerando parámetros que son: el plazo y prioridad.

El plazo relaciona el tiempo medido en meses que debe tomar el recurso técnico de la institución para solucionar los riesgos de la seguridad, para lo cual se especifican los plazos de la siguiente manera:

- Corto (1-3 meses)
- Mediano (3-6 meses)
- Largo (6 meses en adelante)

La prioridad está relacionada con el grado de gravedad de la alerta encontrada. Se definen las siguientes categorizaciones para este parámetro:

- Crítico y Alto (recomendación muy urgente, debe efectuarse lo más pronto posible)
- Media (recomendación leve, puede esperar cierto tiempo)
- Baja (recomendación menos importante, puede tomarse un tiempo para implementarse).

Cada prioridad puede efectuarse respetando los tiempos establecidos en el plazo, donde se sugiere solventar las vulnerabilidades en función de la información mostrada en la siguiente tabla:

Tabla 7 Tipo de vulnerabilidad en función del plazo y prioridad – Red Externa.

Tipo de Vulnerabilidad	Plazo	Prioridad
Críticas	Corto	Crítica – Alta
Altas	Corto	Crítica – Alta
Medias	Medio	Media
Bajas	Largo	Baja

Fuente: Elaboración Propia

Red Interna (47 dispositivos)

Tabla 8 Tipos de Activos Informáticos Red Interna.

Dirección IP	Tipo de activo informático (APP WEB, BDD, WEBSITE, WEBSERVICE, ETC)
172.31.12.194	VIRTUALIZACION
172.31.10.5	WEBSITE, BDD
10.9.0.26	DNS

172.31.9.178	VIRTUALIZACION
172.31.10.252	WEBSITE
172.31.10.164	WEBSITE
172.31.9.130	VIRTUALIZACION
172.31.9.131	LOG
172.31.9.202	VIRTUALIZACION
172.31.9.203	SAMBA
172.31.9.204	DUDE
10.9.0.210	DNS
172.31.10.242	VIRTUALIZACION
172.31.13.66	WEBSITE
172.31.10.2	WEBSITE, SYSLOG
172.31.15.9	VIRTUALIZACION
172.31.15.22	WEBSITE, IPAM
172.31.15.23	DOMAIN CONTROLLER
172.31.15.10	VIRTUALIZACION
172.31.16.3	WEBSIDE, MONITOREO
172.31.9.18	WEBSIDE, VoIP
172.31.10.165	CCTV
172.31.9.150	WEBSITE
172.31.15.2	BDD
10,112,136,206	DISPOSITIVO
10,112,136,210	DISPOSITIVO
10,112,208,134	DISPOSITIVO
10.2.4.33	DISPOSITIVO
10.2.2.34	DISPOSITIVO
10.2.2.14	DISPOSITIVO
10.2.4.9	DISPOSITIVO
10.2.2.10	DISPOSITIVO
10.2.2.94	DISPOSITIVO
10.2.2.237	DISPOSITIVO
10.2.2.245	DISPOSITIVO
10.2.3.10	DISPOSITIVO

10.2.3.30	DISPOSITIVO
10.2.2.70	DISPOSITIVO
10.2.2.193	DISPOSITIVO
10.2.2.110	DISPOSITIVO
10.2.2.173	DISPOSITIVO
10.2.2.130	DISPOSITIVO
172.31.12.90	DISPOSITIVO
10.1.1.27	DISPOSITIVO
172.31.9.26	DISPOSITIVO
172.31.14.78	DISPOSITIVO
172.31.15.1	DISPOSITIVO

Fuente: Elaboración Propia

La mayor cantidad de tipos de fallos representan un riesgo de seguridad contenido en la categoría Media con un total de 15.43%, mientras que las vulnerabilidades Críticas corresponden al 2.47% mostrado en la figura a continuación:

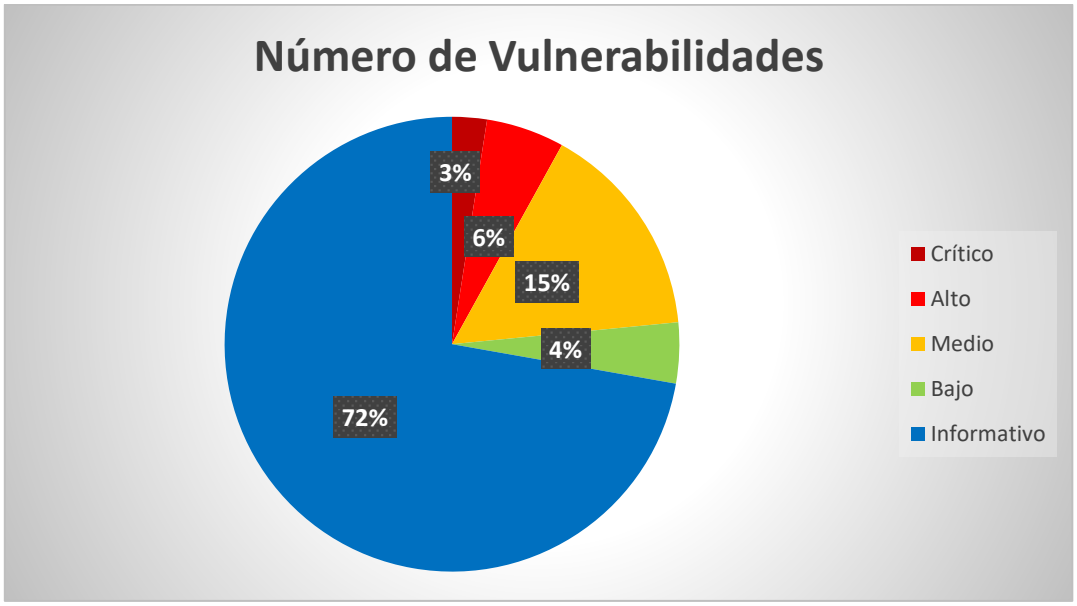


Figura 3 Distribución de vulnerabilidades por dirección IP Red Interna – Gráfico 1.

En la siguiente tabla de Distribución de vulnerabilidades por dirección IP Red Interna, se puede identificar la cantidad de vulnerabilidades encontradas en los dispositivos agrupados por nivel de riesgo.

Tabla 9 Distribución de vulnerabilidades por dirección IP Red Interna.

Host	Crítico	Alto	Medio	Bajo	Info	Total general
10.1.1.27		1			17	18
10.2.2.10					2	2
10.2.2.110	1	1	4		31	31
10.2.2.130					8	8
10.2.2.14					4	4
10.2.2.173					2	2
10.2.2.193	1	1	4		31	37
10.2.2.237					5	5
10.2.2.245					6	6
10.2.2.34			1		21	22
10.2.2.70					7	7
10.2.2.94					4	4
10.2.3.10					6	6
10.2.3.30					6	6
10.2.4.33					6	6
10.2.4.9	1	1	4		32	38
10.9.0.210					7	7
10.9.0.26			1		10	11
172.31.10.164	1	1	5		29	36
172.31.10.165		1	7		42	50
172.31.10.2	1		1		13	15
172.31.10.242					9	9
172.31.10.252			1		13	14
172.31.10.5					13	13
172.31.12.194	1	3	6		23	33
172.31.12.90		1			10	11
172.31.14.78	1	1	4		32	38
172.31.15.1					2	2
172.31.15.22		1	4		27	32
172.31.15.23		1	3		31	35

172.31.15.9					6	6
172.31.9.130	1	1	3		24	29
172.31.9.131	2	1	4		33	40
172.31.9.150	2	1	5		34	42
172.31.9.178	1	3	5		18	27
172.31.9.18		2	9	2	41	54
172.31.9.202	1	2	3		18	24
172.31.9.203		1	1		18	20
172.31.9.204		3	14	2	38	57
172.31.9.26			1	3	20	24
10.112.136.206						-
10.112.136.210						-
10.112.208.134						-
172.31.13.66						-
172.31.15.10						-
172.31.15.10						-
172.31.15.2						-
Total	14	27	90	7	699	837

Fuente: Elaboración Propia

Se muestra la distribución de incidencias de vulnerabilidades clasificadas por tipo:

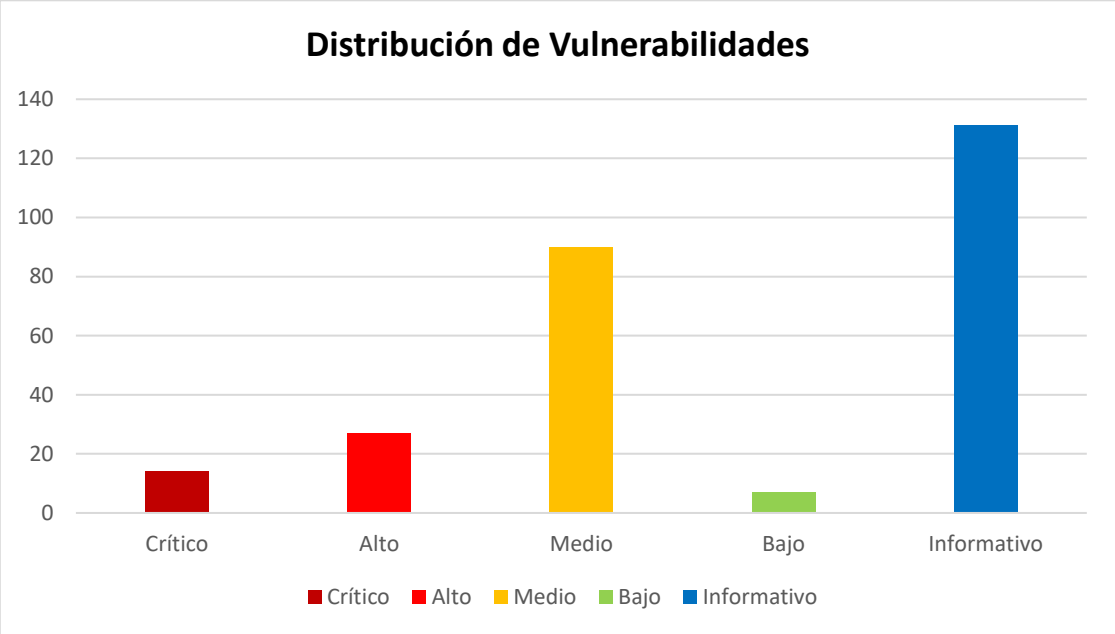


Figura 4 Distribución de vulnerabilidades por dirección IP Red Interna – Gráfico 2.

En esta sección se muestra a detalle las vulnerabilidades y sus correspondientes remediaciones que se deben aplicar de acuerdo al nivel de severidad dentro de la institución.

Tabla 10 Riesgos Críticos Red Interna.

Nombre	Riesgo	Recomendación
Apache Struts 2.3.x Struts 1 plugin RCE (remote)	Crítico	Consultar el aviso del proveedor s2-048 para conocer las opciones de mitigación.
nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE	Crítico	Actualizar a nginx 1.20.1 o posterior.
ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)	Crítico	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.
Python Unsupported Version Detection	Crítico	Actualizar a una versión de Python que se admite actualmente

Fuente: Elaboración Propia

Tabla 11 Riesgos Altos Red Interna.

Nombre	Riesgo	Recomendación
ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	Alto	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.
ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	Alto	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.
ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability	Alto	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.

(VMSA-2018-0026) (Remote Check)		
Microsoft Windows SMB Shares Unprivileged Access	Alto	Para restringir el acceso en Windows, abrir el Explorador, haga clic derecho en cada recurso compartido, vaya a la pestaña 'compartir' y haga clic en 'permisos'.
nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities	Alto	Actualizar a nginx versión 1.16.1 / 1.17.3 o posterior.
SNMP Agent Default Community Name (public)	Alto	Deshabilitar el servicio SNMP en el host remoto si no lo utiliza.Filtre los paquetes UDP entrantes que van a este puerto o Cambiar la cadena de comunidad predeterminada.
SSL Certificate Signed Using Weak Hashing Algorithm	Alto	Ponerse en contacto con la autoridad de certificación para que se Volver a emitir el certificado SSL.
SSL Medium Strength Cipher Suites Supported (SWEET32)	Alto	Volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.
SSL Version 2 and 3 Protocol Detection	Alto	Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.Use TLS 1.2 (con conjuntos de cifrado aprobados) osuperior en su lugar.

Fuente: Elaboración Propia

Tabla 12 Riesgos Medio Red Interna.

Nombre	Riesgo	Recomendación
Apache Multiviews Arbitrary Directory Listing	Medio	Actualizar a Apache versión 1.3.22 o posterior. Como alternativa, como solución alternativa, Deshabilitar Multiviews.
DNS Server Cache Snooping Remote Information Disclosur	Medio	Ponerse en contacto con el proveedor del software DNS para obtener una solución
ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)	Medio	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.
ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	Medio	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.
ESXi 6.5 / 6.7 / 7.0 DoS (VMSA-2020-0018)	Medio	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.
HTTP TRACE / TRACK Methods Allowed	Medio	Deshabilitar estos métodos HTTP. Consultar la salida del plugin para obtener más información.
JQuery 1.2 < 3.5.0 Multiple XSS	Medio	Actualizar a JQuery versión 3.5.0 o posterior.

Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medio	- Forzar el uso de SSL como capa de transporte para este servicio si es compatible, o/y - Seleccionar la configuración 'Permitir conexiones solo desde equipos que ejecutan Escritorio remoto con autenticación de nivel de red' si está disponible.
nginx < 1.17.7 Information Disclosure	Medio	Actualizar a nginx versión 1.17.7 o posterior.
nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilities	Medio	Actualizar a nginx 1.14.1 / 1.15.6 o posterior.
SMB Signing not required	Medio	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'.En Samba, la configuración se llama 'firma de servidor'. Consultar los enlaces "ver también" para obtener más detalles.
SSH Weak Algorithms Supported	Medio	Ponerse en contacto con el proveedor o Consultar la documentación del producto para eliminar los cifrados débiles.
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Medio	Ponerse en contacto con el proveedor para obtener información específica sobre los parches.

SSL Certificate Cannot Be Trusted	Medio	Comprar o generar un certificado SSL adecuado para este servicio.
SSL Certificate Expiry	Medio	Comprar o generar un nuevo certificado SSL para reemplazar el existente.
SSL Certificate with Wrong Hostname	Medio	Comprar o generar un certificado SSL adecuado para este servicio.
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Medio	Deshabilitar SSLv2 y exporte conjuntos de cifrado de criptografía de grado. Asegúrese de que las claves privadas no se utilicen en ningún lugar con el software de servidor que admite conexiones SSLv2
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio	Volver a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4.Considere la posibilidad de usar TLS 1.2 con suites AES-GCM sujetas a soporte de navegador y servidor web.
SSL Self-Signed Certificate	Medio	Comprar o generar un certificado SSL adecuado para este servicio.
SSL Weak Cipher Suites Supported	Medio	Volver a configurar la aplicación afectada, si es posible para evitar el uso de cifrados débiles.
SSLv3 Padding Oracle On Downgraded Legacy Encryption	Medio	Deshabilitar SSLv3.Los servicios que deben admitir SSLv3 deben habilitar el

Vulnerability (POODLE)		mecanismo SCSV de reserva tls hasta que se pueda deshabilitar SSLv3.
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Medio	Habilitar la autenticación de nivel de red (NLA) en el servidor RDP remoto.Esto generalmente se hace en la pestaña 'Remoto' de la configuración de 'Sistema' en Windows.
Terminal Services Encryption Level is Medium or Low	Medio	Cambiar el nivel de cifrado RDP a uno de: 3. Alto 4. Compatible con FIPS
TLS Version 1.0 Protocol Detection	Medio	Habilitar la compatibilidad con TLS 1.2 y 1.3, y Deshabilitar la compatibilidad con TLS 1.0
VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)	Medio	Aplicar el parche apropiado como se hace referencia en el aviso del proveedor.

Fuente: Elaboración Propia

Tabla 13 Riesgos Bajos Red Interna.

Nombre	Riesgo	Recomendación
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Bajo	Volver a configurar el servicio para utilizar un módulo Diffie-Hellman único de 2048 bits o superior.
POP3 Cleartext Logins Permitted	Bajo	Ponerse en contacto con su proveedor para obtener una solución o cifrar el tráfico con SSL / TLS usando stunnel.
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Bajo	Reemplazar el certificado de la cadena con la clave RSA de menos de 2048 bits de longitud por una clave más larga y

		Volver a emitir los certificados firmados por el certificado anterior.
Terminal Services Encryption Level is not FIPS-140 Compliant	Bajo	Cambiar el nivel de cifrado RDP a: 4. Compatible con FIPS.
SSH Weak Key Exchange Algorithms Enabled	Bajo	Ponerse en contacto con el proveedor o Consultar la documentación del producto para desactivar los algoritmos débiles.
SSH Server CBC Mode Ciphers Enabled	Bajo	Ponerse en contacto con el proveedor o Consultar la documentación del producto para deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
SSH Weak MAC Algorithms Enabled	Bajo	Ponerse en contacto con el proveedor o Consultar la documentación del producto para deshabilitar los algoritmos MAC MD5 y de 96 bits.

Fuente: Elaboración Propia

En base a los riesgos de seguridad detectados se deben realizar cambios para mitigar los problemas en la seguridad, por lo que se sugiere seguir un plan de remediación que considere corregir los fallos más críticos con prioridad, y los menos severos después, considerando parámetros que son: el plazo y prioridad.

El plazo relaciona el tiempo medido en meses que debe tomar el recurso técnico de la institución para solucionar los riesgos de la seguridad, para lo cual se especifican los plazos de la siguiente manera:

- Corto (1-3 meses)
- Mediano (3-6 meses)
- Largo (6 meses en adelante)

La prioridad está relacionada con el grado de gravedad de la alerta encontrada. Se definen las siguientes categorizaciones para este parámetro:

- Crítico y Alto (recomendación muy urgente, debe efectuarse lo más pronto posible)
- Media (recomendación leve, puede esperar cierto tiempo)
- Baja (recomendación menos importante, puede tomarse un tiempo para implementarse).

Cada prioridad puede efectuarse respetando los tiempos establecidos en el plazo, donde se sugiere solventar las vulnerabilidades en función de la información mostrada en la siguiente tabla:

Tabla 14 Tipo de vulnerabilidad en función del plazo y prioridad – Red Externa.

Tipo de Vulnerabilidad	Plazo	Prioridad
Críticas	Corto	Crítica – Alta
Altas	Corto	Crítica – Alta
Medias	Medio	Media
Bajas	Largo	Baja

Fuente: Elaboración Propia

Análisis de Riesgos

La presente auditoría permitió conocer a detalle el estado sobre la seguridad de la institución y de la infraestructura tecnológica ante posibles ataques o sucesos que afecten a la seguridad de la información en modalidad externa.

Entre las actividades llevadas a cabo durante el proceso, se ejecutó un análisis de vulnerabilidades a partir de la evaluación de la seguridad de la red desde el exterior e interior de la institución, con la finalidad de evaluar los riesgos que se puedan presentar dentro del análisis a las direcciones IP públicas y los dominios que se pueden observar desde la red externa, se ejecutan pruebas para determinar el nivel de seguridad sobre el

sitio web principal de la institución. Se emplearon metodologías y estándares internacionales como OWASP (Open Web Application Security Project) en lo que se refiere al análisis web.

En la ejecución del análisis de seguridad se considera dos tipos de auditorías, el primero a nivel de seguridad informática sobre el host a través del análisis de la dirección IP y sus puertos abiertos. El segundo tipo de auditoría ejecuta un análisis sobre los sitios web y aplicativos webs.

A nivel de análisis se seguridad sobre los host y direcciones IP públicas se identificó un total de 163 tipos de vulnerabilidades o categorías distribuidas de la siguiente manera:

Tabla 15 Cantidad de tipos de vulnerabilidades distribuidas por severidad.

Severidad	Cantidad	Porcentaje
Crítico	5	3.07%
Alta	9	5.52%
Media	14	8.59%
Bajo	4	2.45%
Informativa	131	80.37%
Total	163	100.00%

Fuente: Elaboración Propia

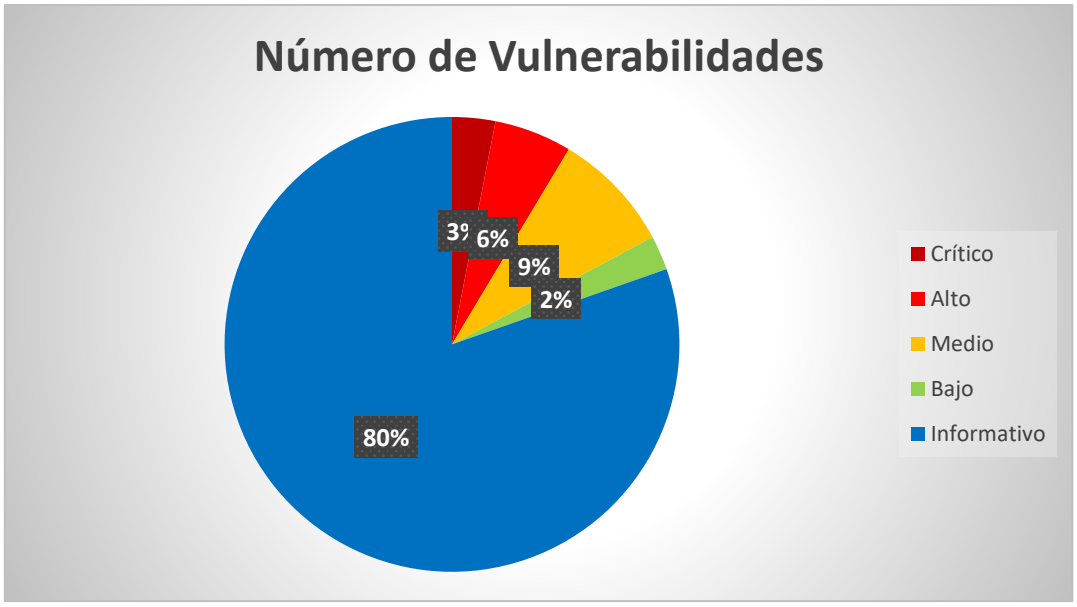


Figura 5 Número de vulnerabilidades por categoría.

En la auditoría de esta fase existen 5 categorías de vulnerabilidades riesgo crítico que representan 3.07% del total de vulnerabilidades, 9 vulnerabilidades de riesgo alto que representan 5.52% del total de vulnerabilidades, 14 vulnerabilidades de riesgo medio que representan 8.59% del total de vulnerabilidades encontradas, 4 vulnerabilidades de riesgo bajo que representan 2.45%, 131 vulnerabilidades informativas que representan 80.37% del total de vulnerabilidades encontradas. Es importante considerar que las vulnerabilidades informativas no representan riesgos informáticos, sino una oportunidad de mejoras.

Del total de las vulnerabilidades encontradas en cada dirección IP mediante el análisis externo se tiene que 1.24% representan las vulnerabilidades críticas, 1.44% pertenece a las vulnerabilidades altas, 5.57% representan las vulnerabilidades medias, 0.41% representan las distribuciones de riesgo bajo y 91.34 % pertenece a las vulnerabilidades de tipo informativas.

Tabla 16 Distribución de vulnerabilidades distribuidas por severidad.

Severidad	Cantidad	Porcentaje
Crítico	12	1.24%
Alta	14	1.44%
Media	54	5.57%
Bajo	4	0.41%
Informativa	886	91.34%
Total	970	100.00%

Fuente: Elaboración Propia

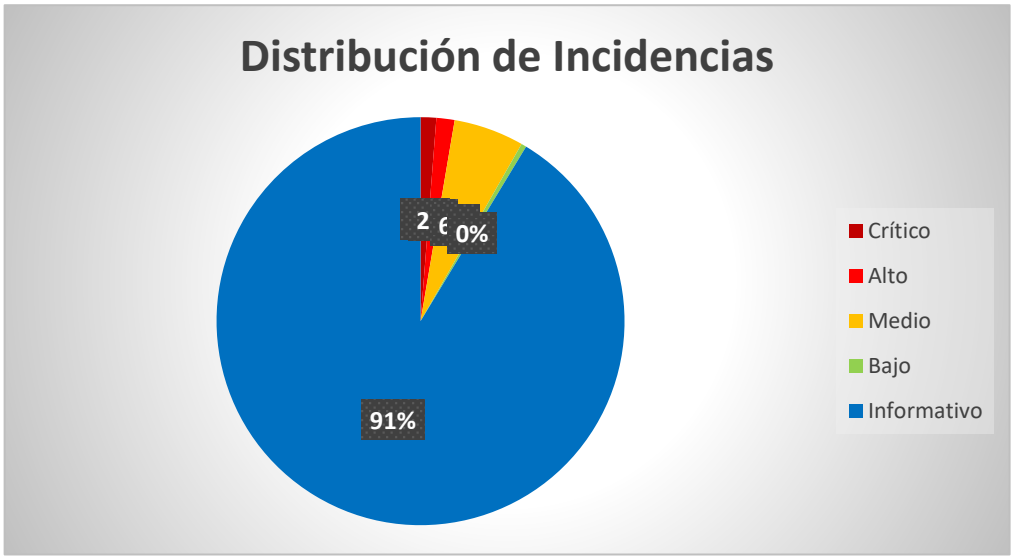


Figura 6 Distribución de Incidencias.

Es importante ejecutar un análisis sin considerar las vulnerabilidades informativas, por lo cual se obtiene que 14.29% pertenece a vulnerabilidades de riesgo crítico, 16.67% pertenece a vulnerabilidades altas, 64.28% pertenecen a vulnerabilidades medias, y 4.76% pertenece a vulnerabilidades bajas.

A continuación, se detalla la distribución gráfica de vulnerabilidades pertenecientes al número de incidencias.

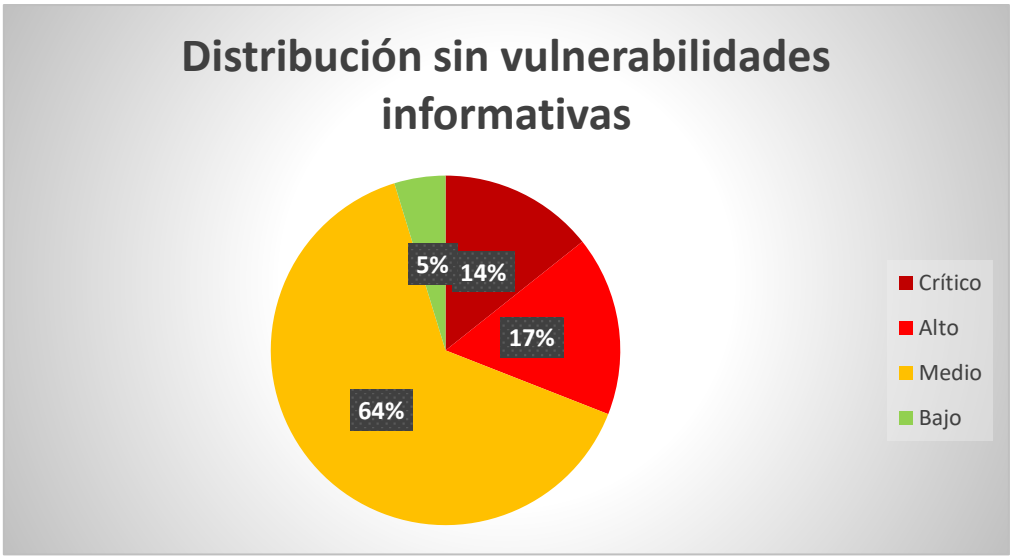


Figura 7 Distribución sin vulnerabilidades informativas.

A partir de esta premisa se puede definir que la institución posee un riesgo "Crítico" en la seguridad de la información debido a la presencia de un 14.29% de vulnerabilidades de este tipo.

Dentro de las vulnerabilidades altas encontradas hubo problemas relacionados a "Apache < 2.4.49 Multiple Vulnerabilities", "Apache 2.4.x < 2.4.47 Multiple Vulnerabilities", "Apache 2.4.x < 2.4.52 Multiple Vulnerabilities", "nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE" y "Python Unsupported Version Detection", los cuales se deben corregir en la brevedad posible debido a que ponen en riesgo la información y seguridad de la red.

Cabe destacar que los problemas relacionados con aspectos generales de seguridad de la información como la falta de manejo de certificados digitales, formularios sin protección frente a ataques, contraseñas enviadas en texto claro, divulgación de direcciones IPs, enlaces rotos, falta de control en métodos web, entre otros.

Es posible que algunas de estas vulnerabilidades puedan suponer falsos-positivos, de las cuales su existencia se debe comprobar manualmente o validar con el cliente luego de la entrega del informe.

Las métricas utilizadas para la apreciación indicada anteriormente se muestran a continuación:

Nivel Informativo: La posibilidad de acceder a la información de la institución a partir de las vulnerabilidades encontradas es muy baja, este tipo de vulnerabilidades hacen referencia a recomendaciones dadas al usuario, debido a que no representan mayor riesgo en la seguridad de la información.

Nivel Bajo: La posibilidad de acceder a la información de la institución es mínima, es decir que el tiempo que se requeriría para acceder a la información sensible de la institución por parte de un usuario con intenciones maliciosas podría tomar un tiempo mayor a 12 meses, tiempo promedio en que además se podrían identificar nuevas vulnerabilidades en los sistemas que la institución utiliza.

Nivel Medio o moderado: La posibilidad de acceder a la información sensible de la institución a partir de las vulnerabilidades encontradas es moderada, es decir el tiempo requerido por un usuario mal intencionado para acceder a la información es de 3 a 6 meses.

Nivel Alto o crítico: La posibilidad de acceder a la información sensible de la institución a partir de las vulnerabilidades encontradas es crítica, es decir que el tiempo podría requerir un usuario con malas intenciones es de aproximadamente 1 mes.

Test de Intrusión

Un test de intrusión permite la evaluación de los sistemas informáticos a cargo de profesionales especializados en seguridad de la información para identificar, enumerar y describir las vulnerabilidades que puede haber en las estaciones de trabajo, redes de comunicaciones y/o servidores.

El presente documento permite conocer los resultados que se obtuvieron durante el proceso de intrusión realizado desde la red interna de la institución mediante el uso de

la modalidad de escaneo del Tipo Caja Gris, en el cual se proporciona solo un punto de red en el interior de la infraestructura tecnológica, donde se realizaron los escaneos y pruebas de seguridad a cada dispositivo de red.

Este método permite escanear las vulnerabilidades de seguridad desde Intranet hacia los sistemas informáticos para posterior intentar obtener acceso mediante técnicas propias de explotación. Para llevar a cabo el Test de Intrusión Interna el departamento de networking de la empresa IN-PLANET S.A. proporcionó el segmento de red con sus respectivas direcciones IP, así como acceso físico y lógico a su red de datos, servidores de aplicaciones, bases de datos, y equipos, para simular el proceso de un ataque generado desde el interior de la organización (modalidad Caja Gris) que forma parte de los servicios de Hacking Ético.

Se procedió a la evaluación y búsqueda de vulnerabilidades en cada activo o dispositivo para posterior emitir recomendaciones generales que forman parte de este informe, así como recomendaciones específicas que conforman el "Plan de Mitigación de Vulnerabilidades", de esta forma optar por medidas correctivas para mitigar los problemas de seguridad de la infraestructura tecnológica.

Luego que se detectan las posibles vulnerabilidades o incidentes de seguridad se procede a planificar y priorizar las mejoras de seguridad respecto al procesamiento y almacenamiento de datos, de esta forma poder reducir el riesgo de la institución.

Como parte de la metodología de Ethical Hacking Interno se tiene las siguientes fases:

- Levantamiento de información (Segmentos de red a escanear) y preparación del ambiente.
- Análisis de vulnerabilidades de los objetivos.
- Detección, comprobación y evaluación de vulnerabilidades

- Medidas de corrección

De un total de 47 direcciones o dispositivos se obtuvieron 162 tipos de vulnerabilidades de seguridad, de los cuales se tiene 4 vulnerabilidades de riesgo crítico que representan 2.47% del total de vulnerabilidades, 9 vulnerabilidades de riesgo alto que representan 5.56% del total de vulnerabilidades, 25 vulnerabilidades de riesgo medio que representan 15.43% del total de vulnerabilidades, 7 vulnerabilidades de riesgo bajo que representan 4.32% del total de vulnerabilidades, 117 vulnerabilidades informativas que representan 72.22% del total de vulnerabilidades.

Tabla 17 Cantidad de tipos de vulnerabilidades distribuidas por severidad.

Severidad	Cantidad	Porcentaje
Crítico	4	2.47%
Alta	9	5.56%
Media	25	15.43%
Bajo	7	4.32%
Informativa	117	72.22%
Total	162	100.00%

Fuente: Elaboración Propia

En lo que concierne al análisis efectuado, se encontró que las direcciones IP presentan:

- Versiones de servicios desactualizadas.
- Versiones de cifrado débiles.
- Versiones desactualizadas de sistemas operativos de dispositivos de conexión.
- Configuraciones sujetas a revisión en sistemas de cifrado.
- Uso de cifrados obsoletos.

Cabe mencionar que algunas de estas vulnerabilidades pueden suponer falsos-positivos, por lo cual su existencia se debe comprobar manualmente o validar con el cliente luego de la entrega de este informe.

Las vulnerabilidades se hallan identificadas en 5 niveles en función del estándar de valoración de vulnerabilidades CVSS los cuales están fijados y asociados con el siguiente código de colores:

Tabla 18 Código de colores por vulnerabilidad.

Colores
Crítico
Alta
Media
Bajo
Informativa

Fuente: Elaboración Propia

La métrica utilizada para la apreciación indicada anteriormente se muestra a detalle a continuación:

- **Nivel Informativo:** La posibilidad de acceder a los sistemas informáticos de la organización a partir de las vulnerabilidades encontradas es nula. Vulnerabilidad que no representan un riesgo de seguridad.

- **Nivel Bajo:** La posibilidad de acceder a los sistemas informáticos de la organización a partir de las vulnerabilidades encontradas es muy baja, Vulnerabilidad que son referidas a una recomendación porque no representan un mayor riesgo de seguridad.

- **Nivel Medio:** La posibilidad de acceder a los sistemas informáticos de la organización a partir de las vulnerabilidades encontradas mínima. El tiempo requerido para acceder a la información de la institución por un usuario con intenciones maliciosas puede tomar aproximadamente 12 meses.

- **Nivel Alto:** La posibilidad de acceder a los sistemas informáticos de la organización a partir de las vulnerabilidades encontradas es moderada. El tiempo

requerido para acceder a la información de la institución por un usuario con intenciones maliciosas puede tomar aproximadamente de 3 a 6 meses.

- **Nivel Crítico:** La posibilidad de acceder a los sistemas informáticos de la organización a partir de las vulnerabilidades encontradas es moderada. El tiempo requerido para acceder a la información de la institución por un usuario con intenciones maliciosas puede tomar aproximadamente menos de 1 mes.

Dispositivos y Servicios Tecnológicos analizados

El listado de los dispositivos de red sobre los que se efectúan las pruebas de penetración y análisis de vulnerabilidades, se detallan en la tabla 8 Tipos de Activos Informáticos Red Interna.

3.2.2 Fase 2: Conocer la estrategia de la organización

En la presente fase se especifican las estrategias de la organización correspondientes a los proyectos en curso y a futuro que tenga la empresa IN PLANET S.A., los cuales son los siguientes:

- Implementar accesos a biométricos a los Data Center.
- Implementar accesos a biométricos a las oficinas.
- Implementar doble factor de autenticación de acceso a los routers y servidores.
- Proponer un plan de concientización de manera periódica a todos los departamentos de la empresa.
- Adquirir mejoras tecnológicas con la finalidad de tener una ventaja sustancial ante la competencia que aplica a la misma línea de negocio.

3.2.3 Fase 3: Definición de proyectos e iniciativas

En la presente fase se especifican los proyectos necesarios para tener un nivel de seguridad óptimo para proteger toda la información y los equipos tecnológicos de la empresa IN PLANET S.A., mediante el análisis de riesgos realizado se evidenció un total de 5 vulnerabilidades de riesgo crítico, 9 vulnerabilidades de riesgo alto, 14 vulnerabilidades de riesgo medio y 4 vulnerabilidades de riesgo bajo.

Tabla 19 Proyectos e Iniciativas.

Id	Proyecto	Descripción
1	Gestión de Tratamiento de la Información	Clasificar la información, para poder etiquetar según la criticidad de la misma, además de conocer quién puede acceder y quien no tiene los permisos suficientes.
2	Control de Acceso Físico	Implementar accesos a biométricos a los Data Center y a las oficinas.
3	Plan de Concientización	Capacitar de manera periódica al personal de la empresa, sobre la seguridad de la información.
4	Sistema de Gestión de la Información (SGSI)	Elaborar un sistema de gestión de la información donde se definan políticas y procedimientos con la finalidad de garantizar, gestionar, controlar y mejorar continuamente la seguridad de la información en la empresa IN-PLANET S.A.
5	Sistema de Detección de Intrusos (IDS)	Controlar mediante un sistema de detección de intrusos que permita supervisar el tráfico de red en busca de actividades sospechosas y emite alertas cuando se descubre dicha actividad, asimismo realizar el proceso de escaneo de una red para encontrar violaciones de políticas de seguridad.
6	Informe de Ethical Hacking	Este informe implica en ayudar al personal encargado a identificar amenazas potenciales en la red.
7	Test de Penetración Externo e Interno	Aplicar un test de penetración debido a que es recomendable realizar pruebas

		de penetración internas y externas regulares para identificar y ayudar a abordar las vulnerabilidades.
8	Gestión de Incidentes y Vulnerabilidades	Establecer los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información, ya sea notificada por la ARCOTEL, o que corresponda a los casos detectados por los prestadores de servicios de telecomunicaciones, será respaldada de manera que se garantice la confidencialidad, integridad y disponibilidad de la misma.
9	Informe de Remediación Externo	El objetivo fundamental de la auditoría de seguridad informática externa es obtener información eficaz del estado de los sistemas computacionales para generar un documento final donde se plasmen qué vulnerabilidades, problemas de configuración han sido detectados, y la criticidad de dichos fallos de seguridad, así como lo respectivos procedimientos para realizar correcciones, o al menos mitigar los fallos.
10	Informe de Remediación Interno	El principal objetivo del servicio de remediación de las vulnerabilidades encontradas en el Ethical Hacking, es realizar la identificación, seguimiento, control, la atención de vulnerabilidades sobre los sistemas y equipos informáticos administrados por la institución con la finalidad de mantener un nivel seguro y adecuado de las plataformas y mitigar los riesgos que se asocian.
11	Gestión de Inventarios de Activos	Tener un control eficiente de los activos críticos de software y de hardware.
12	Gestión de Equipos Informáticos	Realizar mantenimiento de manera periódica a todos los equipos informáticos de la empresa.

13	Gestión de Respaldo de la Información	Realizar una adecuada gestión del respaldo de la información, con la finalidad de que la información no se pierda.

Fuente: Elaboración Propia

3.2.4 Fase 4: Clasificar y priorizar los proyectos a realizar

En la presente fase se especifican la clasificación de los proyectos que se han mencionado en la fase anterior, en donde se va a priorizar mediante las siguientes opciones: alta, media o baja según amerite cada proyecto:

Tabla 20 Clasificación de los Proyectos e Iniciativas.

Prioridad	Proyecto	Descripción
Alta	Sistema de Gestión de la Información (SGSI)	Elaborar un sistema de gestión de la información donde se definan políticas y procedimientos con la finalidad de garantizar, gestionar, controlar y mejorar continuamente la seguridad de la información en la empresa IN-PLANET S.A.
Alta	Sistema de Detección de Intrusos (IDS)	Controlar mediante un sistema de detección de intrusos que permita supervisar el tráfico de red en busca de actividades sospechosas y emite alertas cuando se descubre dicha actividad, asimismo realizar el proceso de escaneo de una red para encontrar violaciones de políticas de seguridad.
Alta	Informe de Ethical Hacking	Este informe implica en ayudar al personal encargado a identificar amenazas potenciales en la red.
Alta	Test de Penetración Externo e Interno	Aplicar un test de penetración debido a que es recomendable realizar pruebas de penetración internas y externas regulares para identificar y ayudar a abordar las vulnerabilidades.

Alta	Gestión de Incidentes y Vulnerabilidades	Establecer los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información, ya sea notificada por la ARCOTEL, o que corresponda a los casos detectados por los prestadores de servicios de telecomunicaciones, será respaldada de manera que se garantice la confidencialidad, integridad y disponibilidad de la misma.
Alta	Informe de Remediación Externo	El objetivo fundamental de la auditoría de seguridad informática externa es obtener información eficaz del estado de los sistemas computacionales para generar un documento final donde se plasmen qué vulnerabilidades, problemas de configuración han sido detectados, y la criticidad de dichos fallos de seguridad, así como lo respectivos procedimientos para realizar correcciones, o al menos mitigar los fallos.
Alta	Informe de Remediación Interno	El principal objetivo del servicio de remediación de las vulnerabilidades encontradas en el Ethical Hacking, es realizar la identificación, seguimiento, control, la atención de vulnerabilidades sobre los sistemas y equipos informáticos administrados por la institución con la finalidad de mantener un nivel seguro y adecuado de las plataformas y mitigar los riesgos que se asocian.
Media	Gestión de Tratamiento de la Información	Clasificar la información, para poder etiquetar según la criticidad de la misma, además de conocer quién puede acceder y quien no tiene los permisos suficientes.
Media	Control de Acceso Físico	Implementar accesos a biométricos a los Data Center y a las oficinas.

Media	Plan de Concientización	Capacitar de manera periódica al personal de la empresa, sobre la seguridad de la información.
Media	Gestión de Equipos Informáticos	Realizar mantenimiento de manera periódica a todos los equipos informáticos de la empresa.
Media	Gestión de Respaldo de la Información	Realizar una adecuada gestión del respaldo de la información, con la finalidad de que la información no se pierda.
Baja	Gestión de Inventarios de Activos	Tener un control eficiente de los activos críticos de software y de hardware.

Fuente: Elaboración Propia

3.2.5 Fase 5: Aprobar el plan de ciberseguridad

En la presente fase no se especifica debido a que no se encuentra estipulado en el alcance del proyecto investigativo.

3.2.6 Fase 6: Implementar el plan de ciberseguridad

En la presente fase no se especifica debido a que no se encuentra estipulado en el alcance del proyecto investigativo.

CONCLUSIONES Y TRABAJO FUTURO

Actualmente el cibercrimen es un gran negocio, debido a que la idea de un hacker trabajando solo por diversión del desafío ha quedado en el pasado digital. Es por ello que, los ataques cibernéticos de hoy en día a menudo son complejos y están respaldados por un nivel asombroso de recursos, que incluyen hardware y software avanzado y una amplia red de ciberdelincuentes altamente calificados.

Por consiguiente, cuando se realiza correctamente una estrategia de ciberseguridad se debe alinear con los objetivos empresariales para que todo funcione de forma integral para hacer que la empresa sea más eficiente.

En razón a lo antes expuesto se indican las siguientes conclusiones referentes a los objetivos planteados en el presente trabajo de investigación:

- La ausencia de disponibilidad del servicio de Internet provocadas por ciberataques a la empresa IN-PLANET S.A. de la ciudad de Milagro, es por motivo de las diferentes vulnerabilidades encontradas mediante el test de intrusión realizado con la finalidad de identificar, enumerar y describir las vulnerabilidades y de esta manera clasificarlas por su severidad. Se encontraron diferentes tipos de vulnerabilidades tales como: versiones de servicios desactualizadas, versiones de cifrado débiles, versiones desactualizadas de sistemas operativos de dispositivos de conexión, configuraciones sujetas a revisión en sistemas de cifrado, uso de cifrados obsoletos, entre otras.
- Las mejores prácticas para la gestión de los riesgos e incidentes en la empresa IN-PLANET S.A. de la ciudad de Milagro, son de vital importancia debido a que se tiene un protocolo a seguir ante cualquier percance que llegase a suceder. Es por esto, que los trabajadores deben tener una capacitación adecuada y de la misma manera la empresa debe

brindar un plan de concientización sobre el tema de seguridad de la información.

- Se aplicaron diferentes criterios de buenas prácticas de Ciberseguridad en la empresa IN-PLANET S.A., en donde lo primordial de aquello es la comunicación efectiva con todos los empleados de la institución, de tal manera lograr educarlos sobre posibles amenazas de ciberseguridad y las formas existentes de mitigarlas.

Por lo expuesto en líneas anteriores, un enfoque centrado en la tecnología para la ciberseguridad no es suficiente para garantizar una protección integral, debido a que los ciberataques a menudo utilizan a las personas de la empresa como punto de entrada. Es por eso que es mejor utilizar un enfoque centrado en las personas para mitigar en gran manera los riesgos relacionados con los humanos.

RECOMENDACIONES

En este mundo digitalizado, la gran mayoría de las personas necesitan tener la información que haya almacenado se encuentre segura y disponible en cualquier momento, por lo tanto, la seguridad informática es importante para mantener la información personal protegida, es importante mantener la seguridad informática y su estado general mediante la prevención de virus y malware que podrían afectar el rendimiento de los sistemas informáticos.

En razón al presente trabajo investigativo se recomienda que:

- La ciberseguridad de la empresa cumpla con los protocolos y normas vigentes por la ARCOTEL, con la finalidad de aplicar un plan de concientización a todo el personal de la institución, no es solo un trabajo para el equipo del área de sistemas.
- Antes de tomar cualquier decisión, es importante llevar a cabo un análisis exhaustivo de toda la infraestructura de tecnología de información, en donde se podrá identificar posibles vulnerabilidades y determinar los procesos existentes que están en su lugar.
- El plan estratégico de ciberseguridad que se ha realizado se ponga en marcha, con la finalidad de evitar ciberataques que puedan afectar a la seguridad de la información.
- Se debe actualizar correctamente el firewall con el objetivo de reducir el riesgo de una violación de la red y asimismo detectar el acceso no autorizado a la red.
- Se debe aplicar auditorias informáticas en donde se pueda llevar a cabo para verificar la eficiencia de los diferentes sistemas informáticos de la empresa y detectar cualquier violación en la red. La auditoría informática

es la herramienta que facilita el negocio en lo que respecta al procesamiento de datos, al tiempo que preocupa especialmente a algunas operaciones específicas.

Por lo expuesto en líneas anteriores, se puede indicar que es bueno tener un punto de referencia inicial para trabajar antes de llevar a cabo las mejoras en políticas de seguridad de la información.

BIBLIOGRAFÍA GENERAL

Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). . *Cuadernos de estrategia, (185)*, 19-64.

Almeida, C. A., & Herrera, L. R. (2019). La ciberseguridad en el ecuador, una propuesta de organización. . *Revista de Ciencias de Seguridad y Defensa, IV, 7*, 156-169.

Alvarado, W., & Changoluisa, I. (2019, 07). *ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI*. Retrieved from http://repositorio.utc.edu.ec/bitstream/27000/5323/1/PI-001347.pdf

Álvarez Valenzuela, D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista chilena de derecho y tecnología, 7(1)*, 1-2.

Amancha, W., & Freddy, B. (2020). *PLAN DE CIBERSEGURIDAD PARA ASEGURAR LA CONTINUIDAD DEL NEGOCIO EN LA COOPERATIVA DE AHORRO Y CREDITO SIERRA CENTRO LTDA.* Retrieved from https://dspace.uniandes.edu.ec/bitstream/123456789/11692/1/TUAEXCOMMI%c3%89002-2020.pdf

Artiles, N. G. (2011). Situación dCiberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia, (149)*, 165-214.

Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias, 3(3)*, 200-217.

Borbúa, R. V., Herrera, L. R., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO, Revista latinoamericana de Estudios de Seguridad, (20)*, 31-45.

Cano, J. J. (2020). Retos de seguridad/ciberseguridad en el 2030. . *Revista Sistemas, (154)*, 68-79.

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *bie3: Boletín IEEE, (2)*, 950-966.

Carrillo, J. J., Zambrano, N. A., Cantos, J. S., & Bravo, M. Z. (2019). Ciberseguridad y su aplicación en las Instituciones de Educación Superior. *Revista Ibérica de Sistemas e Tecnologias de Informação, (E20)*, 438-448.

CEPAL. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Retrieved from https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. . *Revista Científica General José María Córdova*.

ESCUELA SUPERIOR DE REDES RED CEDIA. (2019). *Gestión del riesgo de las TI NTC 27005.* Retrieved from https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI9.pdf

Fernández Bermejo, D., & Martínez Atienza, G. (2018). Ciberseguridad, ciberespacio y ciberdelincuencia. . *Thomson Reuters Aranzadi*, 1-236.

Fonfría, A., & Duch-Brown, N. (2020). Elementos para una política de ciberseguridad efectiva. . *Análisis del Real Instituto Elcano (ARI).*, 127.

Gamboa, J. (2020). *IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD EN EL MUNDO ACTUAL.* Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

Giant, N. (2016). Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones (Vol. 206). . *Narcea Ediciones.*

Giraldo, Y. (2021, 11). *Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad.* Retrieved from https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5550/Yenifer_Zuly_Giraldo_Montes_2021.pdf?sequence=8&isAllowed=y

Gómez, F., & Valencia, H. (2021). *Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa.* Retrieved from https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5197/FredyHumberto_GomezOrjuela_2021.pdf?sequence=5&isAllowed=y

Hernández, J. C. (2018). Estrategias nacionales de ciberseguridad en América Latina. *Análisis GESI, (8)*, 1.

Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. , . *Revista de Pensamiento Estratégico y Seguridad CISDE, 7(1)*, 69-79.

Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos. *ciberseguridad e insurtech*, 1-311.

Lirios, C. G. (2021). Bioseguridad y ciberseguridad percibidas ante la Covid-19 en México. . *Estudios En Seguridad Y Defensa, 16(31)*, 137-160.

Machin, N., & Gazapo, M. (2016, 10). *LA CIBERSEGURIDAD COMO FACTOR CRÍTICO EN LA SEGURIDAD DE LA UNIÓN EUROPEA.* Retrieved from https://www.ucm.es/data/cont/media/www/pag-89564/UNISCIDP42-2NIEVA-MANUEL.pdf

Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI, (42)*, 47-68.

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. In La violencia del siglo XXI. *Nuevas dimensiones de la guerra. Instituto Español de Estudios Estratégicos.*, 45-76.

Martínez, R. B. (2018). Gobierno de la ciberseguridad. *Economía industrial, (410)*, 61-70.

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. . *Pixel-Bit.*

Morán Blanco, S. (2017). La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. . 195-221.

Morán, N. (2021, 04). *ESTADO DE LA CIBERSEGURIDAD EN LAS EMPRESAS DEL SECTOR PÚBLICO DEL ECUADOR: UNA REVISIÓN SISTEMÁTICA.* Retrieved from https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf: https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf

Moreno, A. H. (2017). Ciberseguridad y confianza en el ámbito digital. *Información Comercial Española, ICE: revista de economía, (897)*, 55-66.

Petrenko, S. (2019). La administración de la ciberseguridad. Industria 4.0. . *University of Oviedo (Spain)*.

PORTAL ADMINISTRACIÓN ELECTRÓNICA. (2012, 10). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Roca, J. (2022, 05 25). *El sector energético espera ataques cibernéticos más extremos.* Retrieved from https://elperiodicodelaenergia.com/sector-energetico-espera-ataques-ciberneticos-mas-extremos/

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier. URVIO. *Revista Latinoamericana de Estudios de Seguridad, (20)*, 8-15.

Segura Serrano, A. (2017). Ciberseguridad y Derecho internacional. *Revista española de derecho internacional, 69(2)*, 291-300.

TECNISEGUROS. (2022, 06 06). *Las ciberamenazas han evolucionado y las organizaciones deben estar preparadas para enfrentarlas.* Retrieved from https://www.tecniseguros.com.ec/ciberamenazas-han-evolucionado/

UNIR. (2020, 05 14). *Claves de las políticas de seguridad informática*. Retrieved from https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

UNIR. (2021). *¿Qué es la seguridad informática y cuáles son sus tipos?* Retrieved from https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Universidad PECB. (2022). *Capacitaciones en Riesgos de Seguridad de la Información ISO/IEC 27005.* Retrieved from https://pecb.com/es/education-and-certification-for-individuals/iso-iec-27005