**Universidad Católica de Honduras**

**“Nuestra Señora Reina de la Paz”**

***Análisis y evaluación de riesgos: Instituto Morazán***

**Clase**: Seguridad informática y gestión de riesgo

**Catedrático:** Lic. Patricia Medina

**Por:**

Aldo Josué Munguía Hernández……………………………. 0607-2001-00897

Jordy Josué Castillo Núñez………………………………… 0601-2002-02272

Jorge Daniel Reyes García…………………………………. 0508-2001-00052

Marco Fabricio Mejía Ordoñez……………………………. 0801-2000-20046

8 de febrero del 2022

**Contenido**

[**Introducción** 3](#_Toc99835353)

[**Objetivos** 4](#_Toc99835354)

[**Planteamiento del problema** 5](#_Toc99835355)

[**Justificación** 6](#_Toc99835356)

[**Marco conceptual** 7](#_Toc99835357)

[**Marco Teórico** 13](#_Toc99835358)

[**Capítulo 1 Planificación** 16](#_Toc99835359)

[**1.1.** **Planeación de la seguridad informática en la organización.** 16](#_Toc99835360)

[**1.2.** **Alcance del análisis y evaluación de riesgos del Sistema Informático.** 17](#_Toc99835361)

[**1.3.** **Objetivos del análisis y evaluación de riesgos del Sistema Informático.** 18](#_Toc99835362)

[**Capítulo 2 Análisis de Riesgos** 19](#_Toc99835363)

[**2.1.** **Descripción de los activos o recursos** 19](#_Toc99835365)

[**2.2.** **Valoración de los activos o recursos** 22](#_Toc99835366)

[**2.3.** **Identificación de amenazas y probabilidad** 23](#_Toc99835371)

[**2.4.** **Amenazas clasificadas por su tipo y su nivel de probabilidad** 26](#_Toc99835372)

[**2.5.** **Matriz de impacto potencial** 29](#_Toc99835373)

[**2.6.** **Riesgo Potencial** 31](#_Toc99835374)

[**2.7.** **Número de amenazas por zona de riesgo y tipo de activo** 31](#_Toc99835375)

[**2.8.** **Matriz de riesgo potencial** 32](#_Toc99835376)

[**2.9.** **Salvaguardas o controles existentes** 33](#_Toc99835377)

[**2.9.1.** **Controles implementados según el activo, la amenaza y su nivel de efectividad.** 34](#_Toc99835378)

[**Capítulo 3 Gestión de Riesgos** 47](#_Toc99835381)

[**3.3.** **Comunicación del riesgo y recomendaciones** 47](#_Toc99835387)

[**3.3.1.** **Amenaza por terremotos** 48](#_Toc99835388)

[**3.4.** **Costos en Seguridad Informática** 53](#_Toc99835389)

[**3.5.** **Conclusiones** 54](#_Toc99835390)

[**Bibliografía** 56](#_Toc99835391)

# **Introducción**

La metodología MAGERIT es una que interesa a los que trabajan con sistemas de información para tratar información y prestar servicios.

Implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

MAGERIT persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Sabemos que las empresas dependen de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. Por esta razón una empresa debe de ser de MAGERIT, para la generalización del uso de los medios electrónicos, informáticos y telemáticos que supone un beneficio para los ciudadanos. Pero al mismo tiempo puede conllevar ciertos riesgos que la empresa debe minimizarse con medidas de seguridad para que generen confianza de los medios electrónicos.

En el presente informe se tratarán estos puntos y se logrará capacitar al lector sobre como implementar esta metodología

# **Objetivos**

**Objetivo general:**

* Crear un análisis real de una empresa que posea un departamento de IT.

**Objetivos específicos:**

* Aprender sobre seguridad informática.
* Aprender sobre la metodología MAGERIT.
* Alcance del análisis y evaluación de riesgos del sistema informático.

# **Planteamiento del problema**

¿Qué tema se quiere tomar como eje de la investigación? ¿Por qué y para qué?

Descripción de la propuesta de análisis de riesgo y sistema de seguridad de la empresa.

Actualmente es difícil e imposible, garantizar que se estar 100% seguro, mientras la información del computador tenga acceso directo o indirecto al Internet ya que, a la hora de usar Internet, considerado como la red universal y está, a disposición de todas las personas que posean acceso a la misma, el Internet es una herramienta muy práctica, pero es como una moneda del azar a veces puede ser fácil de manejar, un gran apoyo, y una excelente herramienta para el aprendizaje, en la búsqueda y recopilación de información, no obstante no deja de ser un peligro, para los datos e información personal, de un individuo o empresa, y puede ser filtrado un espía autorizado o no autorizado por el usuario (spyware), y esta puede robar, y usar de forma desagradable, o sin el conocimiento del usuario los datos e información.

Para solventar esta problemática, es necesario diseñar y crear vínculos que ayuden a la actualización de los protectores del ordenador ya sean virtuales o factibles, en donde se puede hacer, preguntas referentes a los problemas que puede presentar los computadores, y así poder prevenir, y minimizar los daños que pueda causar y de esta forma los usuarios y sus PC.

# **Justificación**

Los riesgos a un ciberataque son reales hoy en día. Les ocurre a grandes empresas e incluso a algunas de las organizaciones que parecen más seguras. Por lo tanto, un plan de seguridad informática no es algo de lo que deberías dudar de tener.

Un plan de seguridad informática te permite entender donde puedes tener vulnerabilidades en tus sistemas informáticos, para una vez detectadas, tomar las medidas necesarias para prevenir esos problemas.

# **Marco conceptual**

**Información**

La información es un conjunto de datos que tiene un significado, y cuyo objetivo es ampliar conocimientos, informar o aportar ideas sobre un tema determinado.

En el proceso de información siempre hay un emisor, un canal, y un receptor para que se lleve a cabo de manera eficaz.

La información puede ser motivo de búsqueda. Por ejemplo, a través de internet, donde los usuarios sienten curiosidad a la hora de encontrar datos sobre temas que les interesan. Y, además, son ellos mismos los que realizan las búsquedas entorno a ciertos aspectos actuales o de cualquier temática que consideren.

Asimismo, la información también puede llegar a los usuarios a través de medios como la televisión. A través de ella, reciben las noticias o informaciones referentes a la actualidad a través de un programa determinado.

**Tipo de información:**

* **Información de carácter privilegiado:** Se trata de la información que no se comparte de manera pública, sino que tan solo unos determinados usuarios pueden tener acceso a ella.
* **Información de carácter público:** Se caracteriza por ser una información accesible a todo el mundo.
* **Información de carácter privado:** Este tipo de información está relacionada con la privacidad de los usuarios, y no es accesible para cualquiera, ni tampoco es pública.
* **Información de carácter externo:** Es la información que llega del exterior a determinadas empresas para gestionar algunos temas en concreto.
* **Información de carácter interno:** Se trata de aquella que tan solo conoce un grupo de personas. (Economipedia, 2022)

**Seguridad informática**

Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

**Áreas principales que cubre la seguridad informática**

* **Confidencialidad:** Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
* **Integridad:** Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
* **Disponibilidad:** Los datos deben estar disponibles para los usuarios cuando sea necesario.
* **Autenticación:** Estás realmente comunicándote con los que piensas que te estás comunicando.

**¿Por qué es tan importante la seguridad informática?**

Prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos relacionados con el trabajo, hojas de cálculo, etc. es algo esencial durante las comunicaciones de hoy en día. Muchas de las acciones de nuestro día a día dependen de la seguridad informática a lo largo de toda la ruta que siguen nuestros datos. (Universidad VIU, 2022)



**Vulnerabilidades y Amenazas informáticas**

**Vulnerabilidad**

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño.

**Amenaza**

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos.

**Amenazas de Malware:**

**Virus:** Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento.

**Gusanos:** El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello.

Troyanos: Pasan desapercibidos para el usuario, su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.

**Ransomware:** Consiste en encriptar toda la información de la empresa y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).

**Vulnerabilidades del sistema**

* Errores de configuración.
* Errores en la gestión de recursos.
* Errores en los sistemas de validación.
* Errores que permiten el acceso a directorios.
* Errores en la gestión y asignación de permisos (Ambit, 2022)

**SGSI (Sistemas de Gestión de la Seguridad de la Información)**

El sistema de seguridad de la información o SGSI (Information Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa. El SGSI es un elemento fundamental de la norma internacional ISO 27001 (Sistemas de Gestión de la Seguridad de la Información), que persigue asegurar la integridad y confidencialidad de los datos y los sistemas encargados de procesarlos.

Las empresas que obtienen el certificado ISO 27001 se diferencian por su tratamiento seguro y preciso de todos los datos que manejan y garantizan que se utiliza un sistema de seguridad de la información, que es un estándar a nivel internacional para proteger la privacidad e integridad de la información.

**Beneficios de un SGSI:**

* **Reducción de costes:** Se optimizará todo el proceso para evaluar y detectar amenazas descartando aquellos poco eficaces.
* **Integración de la seguridad en el negocio**: Este sistema requiere de la implicación de todos los miembros de la empresa y del cambio de mentalidad.
* **Cumplimiento de la normativa vigente en seguridad:** Las leyes nacionales e internacionales para el tratamiento y protección de datos estarán cubiertas garantizando que se cumplen en todos los niveles o áreas de la empresa.
* **Incremento de la competitividad:** Con este sistema se dispondrá de una prestigiosa certificación ISO de seguridad que será un elemento diferenciador con la competencia. (Ambit, 2022)



**Normas ISO**

Las normas ISO son documentos que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo. Hasta el momento ISO (International Organization for Standardization), ha publicado alrededor de 19.500 normas internacionales.

**¿Para qué sirven las normas ISO?**

El objetivo perseguido por las normas ISO es asegurar que los productos y/o servicios alcanzan la calidad deseada. Para las organizaciones son instrumentos que permiten minimizar los costos, ya que hacen posible la reducción de errores y sobre todo favorecen el incremento de la productividad.

Los estándares internacionales ISO son clave para acceder a mercados nacionales e internacionales y de este modo, estandarizar el comercio en todos los países favoreciendo a los propios organismos públicos.

Para la sociedad, las normas ISO también son importantes. Existen más de 19.500 normas que ayudan a casi todos los aspectos del día a día de una persona, como aquellas destinadas a garantizar la seguridad vial o la seguridad de los juguetes. Si un producto y/o servicio cumple con alguna de estas normativas, la sociedad puede estar segura que son fiables y que cuentan con la calidad exigida a nivel mundial. (IsoTools, 2022)

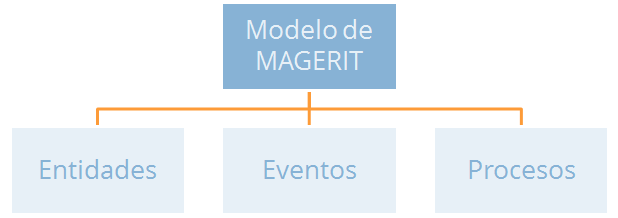


**Metodología MAGERIT**

MAGERIT es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Lo interesante de esta metodología, es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos. Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para una empresa, es decir aquellos relacionados con los sistemas de información. (Weliver Security, 2022)



# **Marco Teórico**

**Instituto Morazán**

El Instituto Morazan con acuerdo presidencial #1063 del 21 de junio de 1995 fue fundado para darle oportunidad a las personas que trabajan y no podían estudiar siendo el primer Instituto de la jornada nocturna en la ciudad de Tegucigalpa logrando así la autorización y funcionamiento en esta capital para hacer estudios de educación secundaria, comercial, primaria y pre- escolar.

El Instituto Morazan logro su funcionamiento impartiendo clases del ciclo común de cultura general, Educación comercial, Bachillerato en ciencias y letras y Bachiller técnico en computación, Bachillerato por madurez, actualmente transformandose tercer ciclo de educación basica, Bachillerato técnico profesional en contaduria y finanzas, BTP en informatica y bachillerato en ciencias y humanidades, Bachillerato en ciencias y humanidades acelarado en un año.

En el año 2019 apertura las modalidades de pre-basica y basica contando con unas matricula de 60 niños.

El Instituto Morazan esta ubicado en el Barrio Villa Adela de comayaguela M.D.C quinta avenida a tres cuadras del estado mayor conjunto de las fuerzas armadas lo cual ayuda a nuestra institución a dar seguridad indirecta a nuestros alumnos y maestros aunque ellos no estén a cargo de la seguridad de la zona.

La institución se proyecta con la comunidad, en el aseo de la áreas circunvecinas, celebrando el día del niño a todos aquellos menores de escasos recursos económicos mediante la donación de juguetes,piñatas etc.

Ubicado en Barrio Villa Adela final quinta avenida, 18 y 19 calle, Comayagüela.

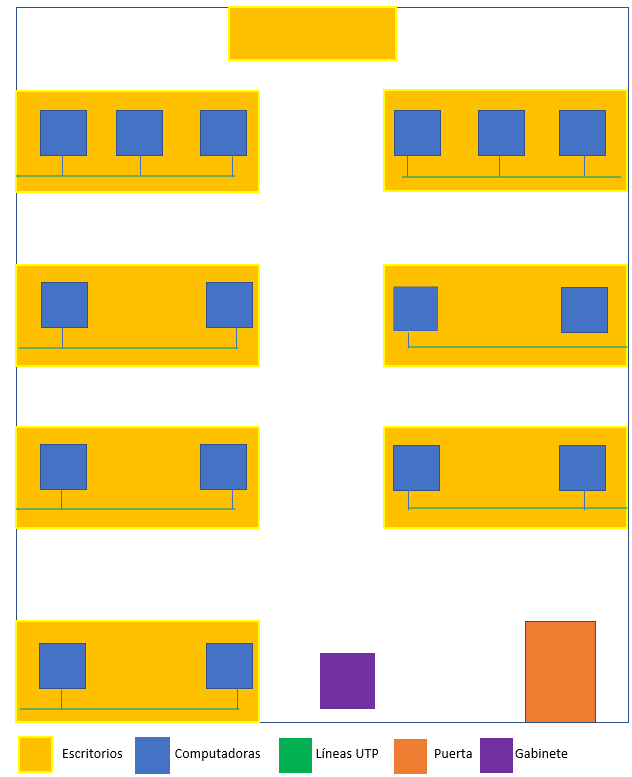
Modalidades: Pre-Básica, Nivel Básica, Nivel Media, Nivel Básica y Media a distancia.

**Fortalezas:**

* Cuenta con un laboratorio de computación con 25 computadoras.
* Publicidad Por Facebook o anuncios de Radio.
* Atención al cliente en el Instituto y por vía WhatsApp.
* Realizan los pagos de matrícula y la mensualidad en bancos o en el Instituto.
* Utilizan Zoom para Impartir clases y dan uso de la herramienta Classroom para envió de tareas y todo lo relacionado.
* Cuentan con una cantidad muy aceptable de alumnos en sus modalidades.

**Debilidades:**

* No dan uso de las demás redes que podrían dar más publicidad como (Instagram, Twitter etc.).
* No cuentan con página web.
* No tienen implementado Chatbots para ayudar a los clientes de una forma instantánea.
* No cuentan con plataforma propia.

**Diagrama de sistema Informático**

# **Capítulo 1 Planificación**

## **Planeación de la seguridad informática en la organización.**

Como cualquier proyecto a realizar es necesario hacer algo tan importante como lo es la planeación del mismo; para que nos pueda servir de guía y de esta manera poder lograr alcanzar los objetivos en la materia de seguridad informática que se han establecido desde un inicio.

Primeramente, se establecerá el alcance que tendrá la investigación, es decir, que se pretende lograr, que se quiere prevenir, en que áreas o departamentos del Instituto Morazán se llevará a cabo y que soluciones ofrecer para evitar que la institución se vea afectada por las distintas amenazas que pueden suceder.

Seguidamente, se procederá a enlistar y describir la serie de elementos informáticos con los que cuenta el Instituto Morazán (así como la ubicación en los que se encuentran), para poder tener el conocimiento de que equipos o recursos se usa y de esta forma analizar cuales son todos aquellos peligros y amenazas a los que se puede enfrentar la empresa por su tecnología actual.

Esto gracias al estudio de las características de los equipos para poder identificar a que tipo de peligro se ven más expuestos y poder evitar esto mediante acciones que vengan a aumentar la seguridad informática del instituto o estar preparados con un plan de acción en caso de que uno de estos eventos llegue a suceder.

Es importante mencionar, que, aunque toda esta planeación sea efectiva para lograr con los objetivos anteriormente propuestos, estos no se alcanzarán si no se tiene el apoyo total de parte de la administración del Instituto Morazán, así como también, el hecho de asignar personal capacitado en temas de seguridad informática para que pueda estar evaluado cualquier tipo de eventualidad que puedan sufrir los equipos del Instituto, y que sepa cómo actuar antes estos posibles ataques o amenazas, para poder reducir en la medida de lo posible los daños causados por estas contingencias.

## **Alcance del análisis y evaluación de riesgos del Sistema Informático.**

El alcance del análisis y evaluación de riesgos de nuestra actividad tiene como finalidad principal ayudar a la institución a mejorar la seguridad en el laboratorio identificando vulnerabilidades y amenazas que pueden llegar a afectar la integridad de los datos y la imagen del instituto Morazán, brindando las mejores prácticas y políticas de seguridad informática. Se tienen en cuenta también los riesgos de seguridad que se corren en el instituto y el impacto que podrían causar.

En el análisis se realiza con el objetivo de corregir y prevenir, es decir, brindarle una solución a la institución ante los problemas de seguridad que tienen y además de eso, proveerles un plan de contingencia en caso de que ocurran problemas a futuro, ya sean problemas esperados o inesperados.

Destacar que la realización de este análisis y evaluación de riesgos se realiza mediante la metodología MAGERTI en el cual es de mucha ayuda al momento de identificar la importancia de los activos, amenazas, vulnerabilidades y riesgos que se tienen en el laboratorio de informática de la institución.

## **Objetivos del análisis y evaluación de riesgos del Sistema Informático.**

* Ayudar a que el Instituto Morazán pueda mejorar las políticas de seguridad que actualmente aplican en su laboratorio de informática.
* Evitar que el instituto se vea afectado por una amenaza o contingencia que pueda afectar grandemente al mismo.
* Definir las distintas vulnerabilidades a las que actualmente el laboratorio de informática este expuesto para estar al tanto de ellas.
* Proporcionar un plan de acción en caso de que una de estas amenazas se haga realidad, para poder evitar el mayor daño posible.
* Reducir en la medida de lo posible el daño que todas estas amenazas puedan causar al Instituto Morazán en caso de que se concreten.
* Exponer todos los dispositivos o recursos informáticos con los que actualmente cuenta el laboratorio de informática.

# **Capítulo 2 Análisis de Riesgos**



## **Descripción de los activos o recursos**

|  |  |
| --- | --- |
| Activo | Descripción |
| -Computadoras | Herramientas de trabajo utilizadas por parte de los estudiantes del Instituto, y está destinado para un fin educativo. |
| -Servidores | Equipo de cómputo de alto rendimiento, destinado para el alojamiento de los servicios críticos dentro del Instituto. |
| -Enrutadores | Dispositivo físico de red que facilita y establece una conexión entre una red local e Internet pasando información a y desde las redes de conmutación de paquetes. |
| -Conmutadores | Equipo de comunicaciones que enlaza las computadoras que se encuentran de la misma subred |
| -Puntos de Acceso | Dispositivo que crea una red de área local inalámbrica |
| -Elementos de cableado Estructurado | se define como el conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones |
| -Escritorios y Armarios | Elemento de soporte para las computadoras y demás artefactos necesarios. |

|  |  |  |
| --- | --- | --- |
| **Principio de seguridad** | **Clasificación** | **Definición** |
| Confidencialidad | **Publico (1)** | Esta información es considerada de carácter público y puede ser divulgada a cualquier persona o entidad interna o externa al instituto |
| **Interna (2)** | Esta información es utilizada por las autoridades como ser docentes del instituto para la ejecución de sus labores y no puede ser conocida por terceros sin autorización del responsable activo de información. |
| **Confidencial (3)** | Está información es altamente sensible y es utilizada solo por un grupo limitado de empleados, como ser la administración del colegio y no puede ser conocida por otro empleado del instituto sin autorización de la parte directiva. |
| Integridad | **No sensitiva (1)** | La pérdida o modificación no autorizada de esta información podría causar un dalo leve o ningún daño al instituto. |
| **Sensitiva (2)** | La pérdida o modificación no autorizada de esta información podría causar un daño que genere prejuicios importantes que afecten al instituto, pero que puede ser absorbido o asumido por éste (ejemplo: falsos testimonios sobre el colegio, prejuicios económicos etc.). |
| **Altamente sensitiva (3)** | La pérdida o modificación no autorizada de esta información podría causar un daño grave que genere prejuicios que afecten significativamente al instituto Morazán y que difícilmente podría ser asumidos. |
| Disponibilidad | **No crítico (1)** | La información puede no estar disponible por un periodo de tiempo extendido, sin afectar el funcionamiento del instituto. |
| **Importante (2)** | La no disponibilidad de esta información afectaría operaciones y servicios que ofrece el instituto. |
| **Misión crítica (3)** | La ausencia de está información afectaría significativamente las operaciones y servicios que ofrece el instituto Morazán. |

**Clasificación de activos**

**Características de dispositivos**

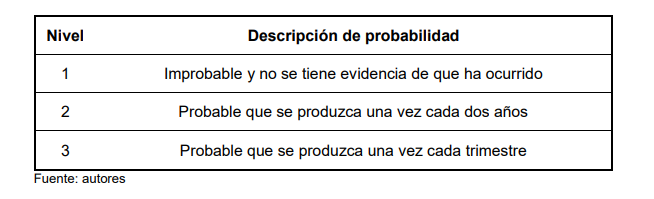
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No. Item** | **Tipo** | **Nombre** | **Encargado** | **Caracteristicas** | **Cantidad** | **C** | **I** | **D** | **Valor Final** |
| 1 | Computadoras | Computadora | Docente Informatica | 256 GB SSD, 12 RAM, 512 GB HHD | 16 | 2 | 2 | 2 | 2 |
| 2 | Software | Sistema Operativo | Docente Informatica | Windows 10 | 16 | 2 | 2 | 1 | 2 |
| 3 | Software | Herramientas de Microsoft | Docente Informatica | Microsoft Office | 16 | 2 | 2 | 1 | 2 |
| 4 | Software | Administrador de Server | Docente Informatica | Windows Server 2016 | 1 | 2 | 1 | 2 | 2 |
| 5 | Servidores | Servidor | Docente Informatica | Dell,64 GB,  512 GB HHD | 1 | 2 | 2 | 2 | 2 |
| 6 | Enrutadores | Enrutador | Docente Informatica | Cisco 4200, 2 puertos Gigabit Ethernet | 1 | 2 | 2 | 2 | 2 |
| 7 | Conmutadores | Conmutador | Docente Informatica | TP-link | 1 | 2 | 2 | 2 | 2 |

## **Valoración de los activos o recursos**

|  |  |  |  |
| --- | --- | --- | --- |
| Valor: |  |  | Criterio: |
| 10 | Muy Alto | MA | Daño muy grave a la organización |
| 7-9 | Alto | A | Daño grave a la organización |
| 4-6 | Medio | M | Daño importante a la organización |
| 1-3 | Bajo | B | Daño menor a la organización |
| 0 | Despreciable | D | Irrelevante a efectos prácticos |



## **Identificación de amenazas y probabilidad**



Se realiza la identificación de amenazas, se establece un código para las mismas y se clasifican de acuerdo a la probabilidad de ocurrencia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Amenaza | Descripción | NP | Razón de la calificación |
| A1 | **Inundaciones** | -Lluvias o fuga de agua en áreas que normalmente están secas del Instituto. | **1** | La zona es de bajo riesgo, en todos los años en servicio del Instituto no se tienen registros de ocurrencia. |
| A2 | **Terremotos** | -Es el movimiento brusco de la Tierra y puede dejar inservible completamente el Instituto | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento y podría afectar porque el Instituto es de 3 pisos. |
| A3 | **Incendios** | -Un incendio puede dejar todo el Instituto prácticamente inservible. | **1** | La zona es de bajo riesgo, en todos los años en servicio del Instituto no se tienen registros de ocurrencia y cuentan con un buen control de seguridad. |
| A4 | **Virus informaticos** | -Son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se de cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento. Y dañen archivos o roben información del Instituto delicada. |
| A5 | **Problemas de alta temperatura** | -Puede afectar de maneras distintas el rendimiento de los equipos informáticos del Instituto, uno de los puntos sensibles es sin duda alguna, el CPU del equipo, ya que presenta altas temperaturas de trabajo, que si se suma a altas temperaturas del ambiente podría evitar que se enfríen los dispositivos de trabajo, como el procesador. | **3** | Se han presentado eventos que generan daños o apagado del equipo, traduciéndose en pérdidas de datos y costos en reparaciones. |
| A6 | **Fuga de información** | -Es el incidente que pone en poder de una persona ajena a la Institución, información confidencial y que sólo debería estar disponible para integrantes de la misma (tanto todos como un grupo reducido). | **2** | No se han presentado este tipo de problema, pero podría ocurrir ya que algún empleado del Instituto podría ingresar al sistema de matricula y manipularlo para obtener información. |
| A7 | **Problemas con contraseñas débiles** | -Problema importante, ya que permite a los intrusos acceder a la red, a nuestras cuentas y, en definitiva, comprometer nuestra privacidad. Es algo que debemos cuidar al máximo en todo momento. | **2** | No se han presentado eventos en el laboratorio, sin embargo, existe la probabilidad que ocurra en algún momento ya que algún usuario no puede tener la combinación de una manera tan segura. |
| A8 | **Antivirus que generan conflictos** | -Existen Ajustes que cambian con las actualizaciones y afectan al Instituto ,como también no poseer el antivirus adecuado o Contar con mas de 1 Antivirus | **3** | Se ha presentado que se instalan 2 o más programas de este tipo y se bloquean entre sí, provocando que ninguno cumpla su función, como también no instalar el que cumpla sus necesidades. |
| A9 | **Errores humanos** | -Son las acciones involuntarias -o la falta de acción de los empleados y usuarios que provocan, propagan o permiten que se produzca una violación de la seguridad. | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento. |
| A10 | **Fallas en la red** | -Se sufren Conflictos con direcciones IP,  pueden ocurrir Fallas en switches o Routers, Se Conectan equipos desordenadamentee,  Insuficiente Ancho de Banda. | **3** | Se han presentado eventos que se asigna direcciones IP no validas y esto ocasiona problemas con la Red/Internet, como la incapacidad del dispositivo para conectarse a la Red / Internet. |

## **Amenazas clasificadas por su tipo y su nivel de probabilidad**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Amenaza | Descripción | NP | Razón de la calificación |
| A1 | **Inundaciones** | -Lluvias o fuga de agua en áreas que normalmente están secas del Instituto. | **1** | La zona es de bajo riesgo, en todos los años en servicio del Instituto no se tienen registros de ocurrencia. |
| A2 | **Terremotos** | -Es el movimiento brusco de la Tierra y puede dejar inservible completamente el Instituto | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento y podría afectar porque el Instituto es de 3 pisos. |
| A3 | **Incendios** | -Un incendio puede dejar todo el Instituto prácticamente inservible. | **1** | La zona es de bajo riesgo, en todos los años en servicio del Instituto no se tienen registros de ocurrencia y cuentan con un buen control de seguridad. |
| A4 | **Virus informaticos** | -Son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se de cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento. Y dañen archivos o roben información del Instituto delicada. |
| A5 | **Problemas de alta temperatura** | -Puede afectar de maneras distintas el rendimiento de los equipos informáticos del Instituto, uno de los puntos sensibles es sin duda alguna, el CPU del equipo, ya que presenta altas temperaturas de trabajo, que si se suma a altas temperaturas del ambiente podría evitar que se enfríen los dispositivos de trabajo, como el procesador. | **3** | Se han presentado eventos que generan daños o apagado del equipo, traduciéndose en pérdidas de datos y costos en reparaciones. |
| A6 | **Fuga de información** | -Es el incidente que pone en poder de una persona ajena a la Institución, información confidencial y que sólo debería estar disponible para integrantes de la misma (tanto todos como un grupo reducido). | **2** | No se han presentado este tipo de problema, pero podría ocurrir ya que algún empleado del Instituto podría ingresar al sistema de matricula y manipularlo para obtener información. |
| A7 | **Problemas con contraseñas débiles** | -Problema importante, ya que permite a los intrusos acceder a la red, a nuestras cuentas y, en definitiva, comprometer nuestra privacidad. Es algo que debemos cuidar al máximo en todo momento. | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento ya que algún usuario no puede tener la combinación de una manera tan segura. |
| A8 | **Antivirus que generan conflictos** | -Existen Ajustes que cambian con las actualizaciones y afectan al Instituto ,como también no poseer el antivirus adecuado o Contar con mas de 1 Antivirus | **3** | Se ha presentado que se instalan 2 o más programas de este tipo y se bloquean entre sí, provocando que ninguno cumpla su función, como también no instalar el que cumpla sus necesidades. |
| A9 | **Errores humanos** | -Son las acciones involuntarias -o la falta de acción de los empleados y usuarios que provocan, propagan o permiten que se produzca una violación de la seguridad. | **2** | No se han presentado eventos en el laboratorio, sin embargo existe la probabilidad que ocurra en algún momento. |
| A10 | **Fallas en la red** | -Se sufren Conflictos con direcciones IP,  pueden ocurrir Fallas en switches o Routers, Se Conectan equipos desordenadamentee,  Insuficiente Ancho de Banda. | **3** | Se han presentado eventos que se asigna direcciones IP no validas y esto ocasiona problemas con la Red/Internet, como la incapacidad del dispositivo para conectarse a la Red / Internet. |

## **Matriz de impacto potencial**

Se incluye una escala donde se dio un valor al impacto causado por la materialización de alguna de las amenazas.

|  |  |  |  |
| --- | --- | --- | --- |
| TIPO DE ACTIVO: | CODIGO DE AMENAZA: | AMENAZA: | IMPACTO: |
| Hardware | **A1** | **Inundaciones** | 5 |
| A2 | **Terremotos** | 5 |
| A3 | **Incendios** | 5 |
| A4 | **Virus informáticos** | 4 |
| A5 | **Problemas de alta temperatura** | 3 |
| A6 | **Fuga de información** | 5 |
| A7 | **Problemas con contraseñas débiles** | 4 |
| A8 | **Antivirus que generan conflictos** | 3 |
| A9 | **Errores humanos** | 3 |
| A10 | **Fallas en la red** | 3 |
| Software | **A1** | **Inundaciones** | 5 |
| A2 | **Terremotos** | 5 |
| A3 | **Incendios** | 5 |
| A4 | **Virus informáticos** | 4 |
| A5 | **Problemas de alta temperatura** | 4 |
| A6 | **Fuga de información** | 5 |
| A7 | **Problemas con contraseñas débiles** | 5 |
| A8 | **Antivirus que generan conflictos** | 4 |
| A9 | **Errores humanos** | 3 |
| A10 | **Fallas en la red** | 3 |
| Información | **A1** | **Inundaciones** | 5 |
| A2 | **Terremotos** | 5 |
| A3 | **Incendios** | 5 |
| A4 | **Virus informáticos** | 5 |
| A5 | **Problemas de alta temperatura** | 3 |
| A6 | **Fuga de información** | 5 |
| A7 | **Problemas con contraseñas débiles** | 5 |
| A8 | **Antivirus que generan conflictos** | 4 |
| A9 | **Errores humanos** | 3 |
| A10 | **Fallas en la red** | 4 |

## **Riesgo Potencial**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Probabilidad** | **Impacto** | | | | |
| **Insignificante (1)** | **Menor (2)** | **Moderado (3)** | **Mayor (4)** | **Catastrófico (5)** |
| **1** | ZB(1) | ZB(2) | ZB(3) | ZB(4) | ZM(5) |
| **2** | ZB(2) | ZB(4) | ZM(6) | ZA(8) | ZE(10) |
| **3** | ZB(3) | ZM(6) | ZA(9) | ZE(12) | ZE(15) |
|  | ZB: Zona de riesgo baja: Asumir riesgo. (1 - 4) | | | | |
|  | ZM: Zona de riesgo media: Asumir riesgo, reducir el riesgo. (5 - 7) | | | | |
|  | ZA: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir (8 - 9) | | | | |
|  | ZE: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir (10 - 15) | | | | |

Las zonas de riesgo derivan del producto de los valores de impacto y probabilidad

## **Número de amenazas por zona de riesgo y tipo de activo**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Zona de riesgo** | **Hardware** | **Información** | **Software** | **Total general** |
| **Zona de riesgo baja** | **0** | **0** | **0** | **0** |
| A1 - A10 | 0 | 0 | 0 | 0 |
| Zona de riesgo media | 3 | 3 | 3 | 9 |
| A1 | 1 | 1 | 1 | 3 |
| A3 | 1 | 1 | 1 | 3 |
| A9 | 1 | 1 | 1 | 3 |
| Zona de riesgo Alta | 5 | 1 | 2 | 8 |
| A4 | 1 | 0 | 1 | 2 |
| A5 | 1 | 1 | 0 | 2 |
| A7 | 1 | 0 | 0 | 1 |
| A8 | 1 | 0 | 0 | 1 |
| A10 | 1 | 0 | 1 | 2 |
| Zona de riesgo extrema | 2 | 6 | 5 | 13 |
| A2 | 1 | 1 | 1 | 3 |
| A4 | 0 | 1 | 0 | 1 |
| A5 | 0 | 0 | 1 | 1 |
| A6 | 1 | 1 | 1 | 3 |
| A7 | 0 | 1 | 1 | 2 |
| A8 | 0 | 1 | 1 | 2 |
| A10 | 0 | 1 | 0 | 1 |
| **Total general** | **10** | **10** | **10** | **30** |

## **Matriz de riesgo potencial**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tipo de activo** | **Código de amenaza** | **Amenaza** | **Impacto** | **Nivel de probabilidad** | **Riesgo potencial** | **Zona de riesgo** |
| **Hardware** | A1 | Inundaciones | 5 | 1 | 5 | ZM |
| A2 | Terremotos | 5 | 2 | 10 | ZE |
| A3 | Incendios | 5 | 1 | 5 | ZM |
| A4 | Virus informáticos | 4 | 2 | 8 | ZA |
| A5 | Problemas de alta temperatura | 3 | 3 | 9 | ZA |
| A6 | Fuga de información | 5 | 2 | 10 | ZE |
| A7 | Problemas con contraseñas débiles | 4 | 2 | 8 | ZA |
| A8 | Antivirus que generan conflictos | 3 | 3 | 9 | ZA |
| A9 | Errores humanos | 3 | 2 | 6 | ZM |
| A10 | Fallas en la red | 3 | 3 | 9 | ZA |
| **Software** | A1 | Inundaciones | 5 | 1 | 5 | ZM |
| A2 | Terremotos | 5 | 2 | 10 | ZE |
| A3 | Incendios | 5 | 1 | 5 | ZM |
| A4 | Virus informáticos | 4 | 2 | 8 | ZA |
| A5 | Problemas de alta temperatura | 4 | 3 | 12 | ZE |
| A6 | Fuga de información | 5 | 2 | 10 | ZE |
| A7 | Problemas con contraseñas débiles | 5 | 2 | 10 | ZE |
| A8 | Antivirus que generan conflictos | 4 | 3 | 12 | ZE |
| A9 | Errores humanos | 3 | 2 | 6 | ZM |
| A10 | Fallas en la red | 3 | 3 | 9 | ZA |
| **Información** | A1 | Inundaciones | 5 | 1 | 5 | ZM |
| A2 | Terremotos | 5 | 2 | 10 | ZE |
| A3 | Incendios | 5 | 1 | 5 | ZM |
| A4 | Virus informáticos | 5 | 2 | 10 | ZE |
| A5 | Problemas de alta temperatura | 3 | 3 | 9 | ZA |
| A6 | Fuga de información | 5 | 2 | 10 | ZE |
| A7 | Problemas con contraseñas débiles | 5 | 2 | 10 | ZE |
| A8 | Antivirus que generan conflictos | 4 | 3 | 12 | ZE |
| A9 | Errores humanos | 3 | 2 | 6 | ZM |
| A10 | Fallas en la red | 4 | 3 | 12 | ZE |

## **Salvaguardas o controles existentes**

|  |  |
| --- | --- |
| ***Nivel*** | ***Descripción de la Efectividad a la utilización del control*** |
| I | Es muy probable que el control aplicado falle en caso de que ocurra la amenaza, o simplemente no existe un control para la misma |
|  |
| II | El control aplicado es medianamente eficaz, podría funcionar la mayor parte en el caso que ocurra la amenaza |  |
|  |
| III | El control aplicado nos garantiza que funcionará eficazmente en caso que ocurra esta amenaza |  |
|  |

## **Controles implementados según el activo, la amenaza y su nivel de efectividad.**

**Amenaza por inundaciones**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Hardware, Software, Información | Falta de pisos elevados | Se deben implementar medidas para proteger los equipos contra las inundaciones | Minimizador | SI | III | El Instituto lo implementa y da protección a los laboratorios |
| Sistema de drenaje deficiente | Se debe asegurar que en caso de inundaciones, se pueda sobrellevar de manera rápida y efectiva | Minimizador | SI | III | Brinda al Instituto más seguridad |
| Mala calidad en los materiales para la construcción del edificio | La construcción debe de resistir en la medida de lo posible, las inundaciones. | Minimizador | SI | III | El Instituto tiene muchos años de servicio y tiene la misma estructura |
| Ausencia de protocolos en caso de inundaciones | Se debe de establecer pasos a seguir en caso de una situación de inundación para poder mitigar el daño | Minimizador | NO | I | No cuentan con un protocolo en caso de que ocurra una Inundación |
| Ubicado en una zona propensa a inundaciones | Los recursos informáticos no deben de estar localizados en una zona propensa a inundaciones | Minimizador | SI | II | Se encuentra en una zona que no sufre de ese problema |
| Falta de un backup en un lugar alterno | Se debe tener al menos una copia de seguridad en un lugar diferente en caso de que ocurra este incidente | Prevención | SI | III | El dueño del Instituto tiene acceso a todo desde su casa, Cuenta con su copia |

**Amenaza por terremotos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Hardware, Software, Información | Ubicado en una zona de alto nivel sísmico | Se deben implementar medidas para proteger los equipos contra los terremotos | Minimizador | Si | III | El Instituto tiene una ubicación idónea |
| Mala calidad en los materiales para la construcción del edificio | Se debe asegurar que en caso de inundaciones, se pueda sobrellevar de manera rápida y efectiva | Minimizador | SI | III | El Instituto tiene muchos años de servicio y tiene la misma estructura |
| Ausencia de protocolos en caso de terremotos | Se debe de establecer pasos a seguir en caso de una situación de inundación para poder mitigar el daño | Minimizador | SI | II | Cuentan con bastantes mensajes en el Instituto en caso que ocurra. |
| Falta de un backup en una lugar alterno | Se debe tener al menos una copia de seguridad en un lugar diferente en caso de que ocurra este incidente | Prevención | SI | III | El dueño del Instituto tiene acceso a todo desde su casa, Cuenta con su copia |

**Amenaza por incendios**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Hardware, Software, Información | Cercanía a plantas o empresas que trabajan con materiales inflamables (Gasolina, químicos, gas) | Los recursos deben estar a una distancia adecuada de cualquier lugar que contenga materiales inflamables | Minimizador | NO | I | El Instituto no esta cerca de materiales que brinden mas riesgos de lo normal |
| Cercanía a lugares de almacenamiento de materiales inflamables | I |
| Materiales inflamables utilizados para la construcción | Utilizar materiales que no sean inflamables, o que no puedan incendiarse tan fácilmente | Minimizador | SI | III | El Instituto no cuenta con materiales inflamables |
| Equipos y circuitos eléctricos de mala calidad | Se debe de elegir a personas capaces para estas instalaciones, que sepa elegir productos de buena calidad | Minimizador | SI | III | No han teneido problemas de electricidad |
| Carencia de un sistema de detección de incendios | Se debe de contar con un sistema que pueda alertar en caso que este sucediendo un incendio | Minimizador | No | I | No se cuenta con un sistema en el Instituto |
| Ausencia de equipo contra incendios | Se debe de colocar equipo contra incendios en lugares estratégicos | Minimizador | SI | III | Cuentan con extintores en el Instituto |
| Permitir fumar dentro de las instalaciones | Se debe de limitar las actividades que se pueden hacer en donde están los recursos informáticos | Minimizador | NO | I | Es prohibido fumar en el Instituto |
| Falta de un mecanismo automático para mitigar el incendio | Se debe de contar con un sistema que pueda mitigar de manera automática el incendio una vez este ultimo a sido detectado | Minimizador | NO | I | No se cuenta con un sistema de este tipo pero seria muy útil contal con el |
| Ausencia de protocolos en caso de incendios | Se debe de establecer pasos a seguir en caso de una situación de incendio para poder mitigar el daño | Minimizador | SI | II | Cuenta con mensajes en todo el Instituto |
| Falta de un backup en una lugar alterno | Se debe tener al menos una copia de seguridad en un lugar diferente en caso de que ocurra este incidente | Prevención | SI | III | El dueño del Instituto tiene acceso a todo desde su casa, Cuenta con su copia |

**Virus Informáticos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Software, Información | Mala configuración del sistema | Se debe de configurar adecuadamente el sistema en cuanto a la seguridad para evitar el acceso de virus informáticos | Minimizador | SI | III | El Instituto nunca a tenido este tipo de problemas |
| Deficiencias en las gestión de los recursos | Se debe de definir detalladamente que usuarios tienen acceso a que recursos, para asegurar la protección de estos | Prevención | SI | III | Solo el encargado de los laboratorios y el dueño tienen acceso |
| Errores en las validaciones de seguridad | Se deben de analizar constantemente las validaciones de seguridad que se tengan, para identificar si alguna de ellas llega a fallar. | Prevención | NO | I | El encargado hace las validaciones solo al iniciar un año escolar |
| Utilización de antivirus piratas o de mala calidad | Se debe de hacer un análisis para elegir que antivirus utilizar |  | SI | III | Cuentan con los Antivirus adecuados |
| Ausencia de normas para los usuarios | Se debe dejar en claro lo que deben y no deben de hacer los usuarios, para evitar la propagación de algún virus informático | Minimizador | SI | III | Tienen normas de lugares que no pueden visitar |
| Ausencia de protocolos en caso de propagación de virus informáticos | Se debe de establecer pasos a seguir en caso de una situación de una propagación de algún virus informático para poder mitigar el daño | Minimizador | NO | I | Al no tener ese tipo de problemas no cuentan con un plan |
| Falta de un backup en una lugar alterno | Se debe tener al menos una copia de seguridad en un lugar diferente en caso de que ocurra este incidente | Prevención | SI | III | El dueño del Instituto tiene acceso a todo desde su casa, Cuenta con su copia |

**Problemas de altas temperaturas**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Hardware, Software, Información | Las instalaciones están ubicadas en un lugar donde el sol es más intenso | Se debe de procurar que las instalaciones están resguardadas por sombras, para reducir la intensidad del sol | Minimizador | SI | II | El Instituto es de 3 pisos y totalmente techado en todas sus áreas |
| Falta de aires acondicionados en donde están los recursos informáticos | Es importante tener a una temperatura adecuada los equipos para evitar el calentamiento de estos | Minimizador | SI | III | Cuentan con la ventilación adecuada |
| Ausencia de mecanismos de enfriamiento en cada recurso | Es crucial tener sistemas de enfriamiento en cada recurso, para evitar su sobrecalentamiento | Minimizador | NO | I | No cuentan en el Instituto con sistemas de enfriamiento y serian muy útiles |
| Ausencia de protocolos en caso de sobrecalentamientos de los equipos | Se debe de establecer pasos a seguir en caso de una un sobrecalentamiento de un equipo. | Minimizador | SI | II | Al solo ser una persona esa persona pasa pendiente |
| Falta de un backup en una lugar alterno | Se debe tener al menos una copia de seguridad en un lugar diferente en caso de que ocurra este incidente | Prevención | SI | III | El dueño del Instituto tiene acceso a todo desde su casa, Cuenta con su copia |
| Equipos comprados de baja calidad | Se deben de hacer las compras pertinentes, para poder asegurar la compra de equipo de alta calidad | Minimizador | SI | III | El Instituto ya lleva bastante tiempo con el mismo equipo solo compran lo necesario |

**Fuga de información**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Software, Información | Ausencia de protección física | Los lugares donde están los recursos informáticos deben tener controles que garanticen solo el acceso a persona autorizado | Minimizador | SI | III | En el laboratorio solo pueden ingresar con llaves |
| Ausencia de supervisión a trabajos del persona externo | Se deben de establecer mecanismos para garantizar la seguridad de la información del personal externo | Minimizador | SI | III | No permiten el ingreso de otras personas que no sean del Instituto |
| Falta de procedimientos para el manejo de información | Se debe de establecer de manera clara, la metodología a utilizar para el manejo de información | Minimizador | SI | II | La persona encargada tiene todo en orden |
| La documentación de los sistemas debe estar protegida a personal no autorizado | Minimizador | SI | III | Cuentan con buena seguridad en sus sistemas de matriculas y demás sistemas. |
| Se deben de crear contratos, para que los empleados entiendan la gravedad en caso de filtrarse la información | Minimizador | SI | II | Todo esta bien ordenado al momento que contratan algún profesor |
| Carencia de normas de seguridad para el resguardo de la información | Se deben de establecer procedimientos para poder garantiza la seguridad de la información. | Minimizador | SI | III | Es muy necesario contar con todas las medidas de seguridad |
| Ausencia de procedimientos para la clasificación de la información | Todos los recursos deben de estar clasificas e identificados de acuerdo a su importancia | Minimizador | NO | I | Sus recursos no están clasificados |
| Todos los recursos deben de contar con una persona que se pueda hacer responsable de ellos y de su información | Minimizador | SI | III | si lo hacen pero solo es una persona la encargada |
| Inadecuado procedimiento al momento de quitar acceso al sistema a un empleado despedido | Se debe de ser minuciosos con las personas que tienen acceso al sistema, para poder evitar que un empleado que ya no trabaje ahí, pueda divulgar información | Minimizador | SI | III | Solo el personal autorizado y con sus credenciales pueden ingresar |
| Ausencia de protocolos en caso de fuga de información | Se deben de establecer políticas en caso de una fuga de información | Minimizador | NO | I | No tienen políticas porque no a ocurrido un problema de ese tipo |

**Problemas con contraseñas débiles**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Software, Información | Falta de políticas de contraseñas | Se deben de establecer criterios a seguir para poder elegir una contraseña adecuada | Minimizador | SI | III | Tienen sus propias palabras claves para contraseñas |
| No dar a conocer la importancia que tienen las contraseñas | Se les debe de hacer saber a los usuarios la importancia de establecer una contraseña segura. | Minimizador | SI | II | Se les recuerda poner contraseñas seguras y no compartirlas |
| Establecimiento de contraseñas débiles en recursos cruciales | En los equipos más vitales se deben de establecer contraseñas aún mas seguras que para un equipo ordinario. | Minimizador | SI | III | Cuentan con diferentes contraseñas en cada equipo |

**Antivirus que generan conflictos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Software, Información | Mala configuración del antivirus | Se establecen normas que no son necesarias y hacen que el rendimiento del ordenador sea menor | Minimizador | NO | I | No cuentan con normas |
| Se debe de hacer un análisis minucioso para saber que normas establecer en el antivirus | Minimizador | NO | I | No hacen un análisis adecuado que debería de realizarse |
| Utilización de 2 o mas antivirus en un mismo ordenador | Se debe de tener solo 1 antivirus en cada ordenador (después de análisis de cual nos beneficia mas) | Minimizador | SI | III | Solo cuentan con un Antivirus en cada ordenador y el encargado esta en sus actualizaciones |
| Utilizar antivirus piratas | Se debe de contar con las licencias originales de el antivirus utilizado | Minimizador | NO | I | Los Antivirus los descargan de Internet sin licencias algunos |

**Errores humanos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Hardware, Software, Información | Mala definición de roles y responsabilidades en el sistema | La funciones y responsabilidades de los usuarios deben estar definidas y previamente analizadas | Minimizador | NO | I | Solo una persona es la encargada |
| La mala capacitación de los usuarios | Es importante que los usuarios sepan que hacer y que no hacer con los recursos informáticos | Minimizador | SI | III | La persona encargada da un buen manejo a los recursos con los que cuentan |
| Utilización de la misma contraseña para múltiples accesos | Se debe de dejar en claro a los usuarios, que no utilices contraseñas que este utilizando para acceder a otros sitios | Minimizador | NO | I | No se deja claro para los usuarios cuando se le asigna un ordenador |
| Deterioro de los equipos por falta de conocimientos | Los usuarios deben de saber las buenas practicas para conservar en buen estado físicamente los equipos |  | SI | III | Se brindan charlas para cuidar el equipo ya que no es mucho |
| Dejar la contraseña expuesta | Se debe de hacer énfasis a los usuarios para que no dejen la contraseña en cualquier lugar visible. | Minimizador | SI | III | Se les dice de ese aspecto para evitar conflictos |

**Fallas en la red**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***Activos Afectados*** | ***Vulnerabilidad*** | ***Controles*** | ***Tipo de Control*** | ***¿Control implementado?*** | ***Eficacia del Control*** | ***Observaciones*** |
| Software, Información | Sistemas sobrecargados por el exceso de trafico | Se debe de monitorear el trafico en los equipos, y así poder determinar si algo esta fallando o se necesita un equipo de mayores capacidades | Minimizador | NO | I | No se realiza monitoreo |
| Debilidades en la administración de los accesos a la red | Se debe de administrar cuidadosamente que personas podrán acceder a la red. |  | SI | III | Se administra de la mejor manera para no tener problemas |
| Inadecuada seguridad de la red | Las redes deben están controladas y configuradas para que estén protegidas de cualquier amenaza |  | NO | I | No estan configuradas pero si seria de gran ayuda y seguridad  para el Instituto |
| Instalación de configuraciones de red defectuosas | Se debe de asegurar que cualquier norma de configurada en la red este funcionando correctamente. | Minimizador | NO | I | No tienen normas configuradas |
| Hardware | Compra de equipos de baja calidad | Las compras deben ser realizadas por alguien que sepa del tema, para que pueda hacer compras de productos de calidad. | Minimizador | SI | III | Cuando compran algo solo van el encargado del laboratorio y el dueño del Instituto |
| Falta de mantenimiento | Se debe de hacer mantenimiento a los equipos relacionados con la red, para postergar el deterioro de los mismos | Minimizador | NO | I | No hacen ese tipo de mantenimiento en la red |



# **Capítulo 3 Gestión de Riesgos**



## **Comunicación del riesgo y recomendaciones**

Luego de un trabajo muy arduo realizado sobre el instituto Morazán donde se analizaron riesgos, amenazas a la que se expone el laboratorio de dicho instituto, una información más formal y detallada sobre los activos y un son números de matriz con información detallada (riesgo potencial, salvaguardas, impactos etc.) con el fin de que dicha información proporcionada sea de utilidad para las autoridades administrativas al momento de tomar decisiones sobre las acciones a tomar en base al análisis de riesgos proporcionado.

Por parte del equipo de la Universidad Católica de Honduras de la clase de seguridad informática y gestión de riesgos se recomienda las diferentes medidas de tratamiento de riesgo en base a la metodología MAGERIT:

Según el análisis realizado en la matriz de riesgo de las amenazas identificadas ninguna está em la zona de riesgo baja, lo que significa que al ocurrir un daño el impacto sería muy grande, entonces para la zona de riesgo media solamente sería darle un seguimiento o vigilancia continua ya que solo están 3 amenazas en dicha zona.

En la zona de riesgo alta y zona de riesgo extrema si se cuentan con más amenazas por lo que el impacto si sería muy fuerte si llegan a ocurrir, en este punto se recomienda:

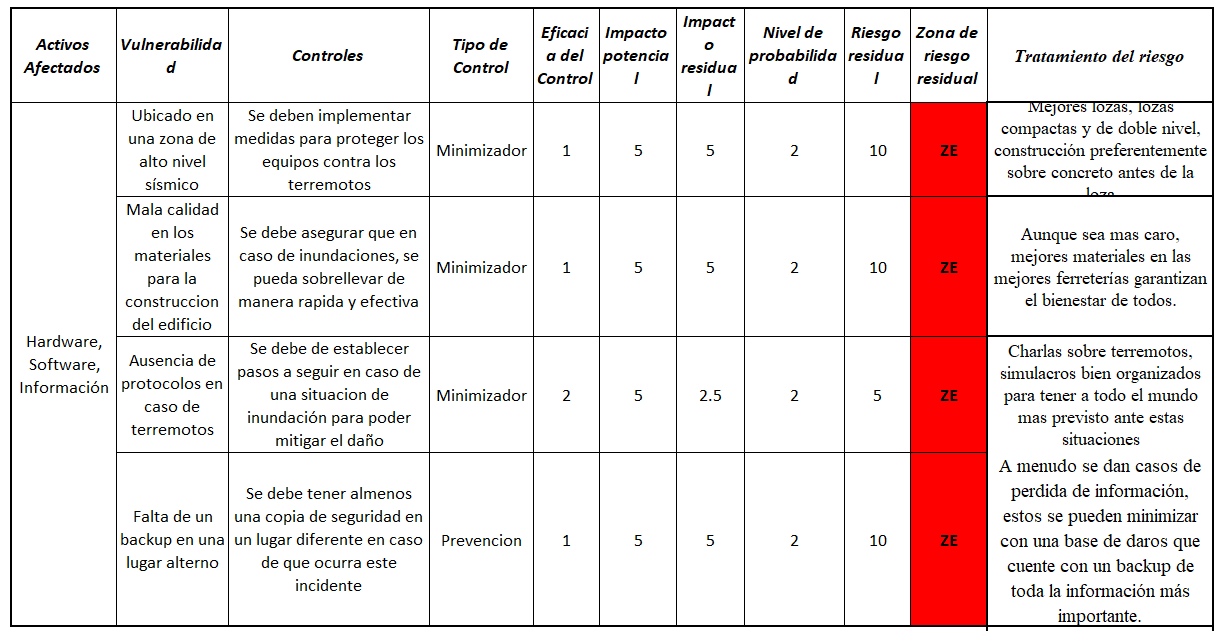
Eliminar varios elementos que intervienen en el riesgo para que no afecten el funcionamiento correcto del Instituto Morazán.

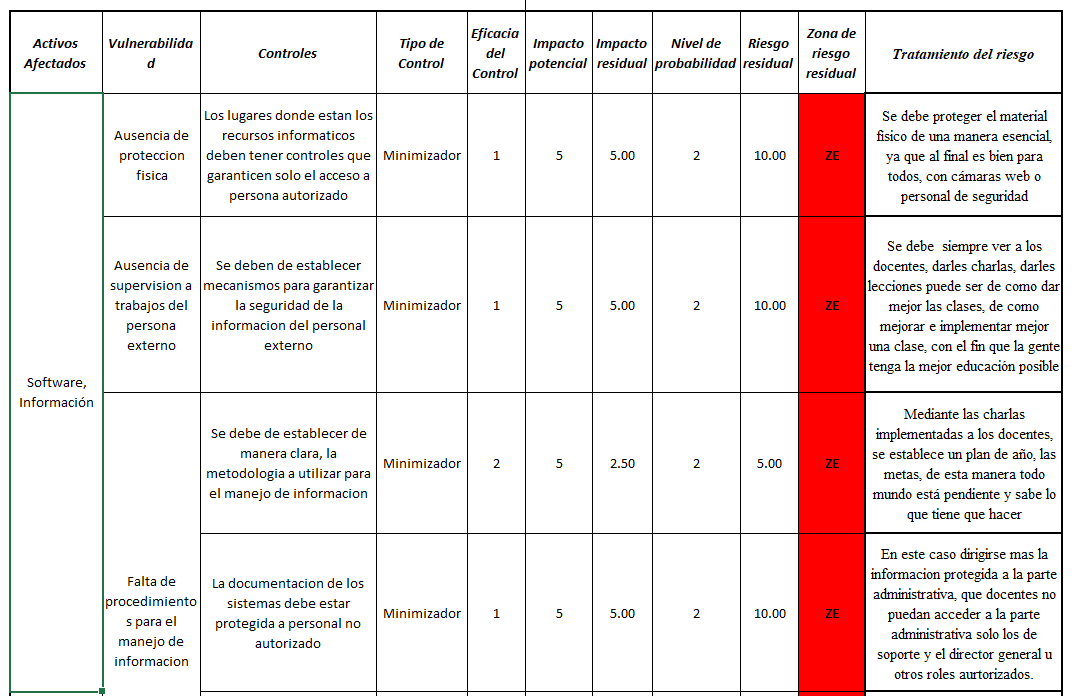
En el laboratorio del instituto implementar nuevos controles de seguridad con el objetivo de reducir el impacto o mejor aún la posibilidad de que dicha amenaza ocurra.

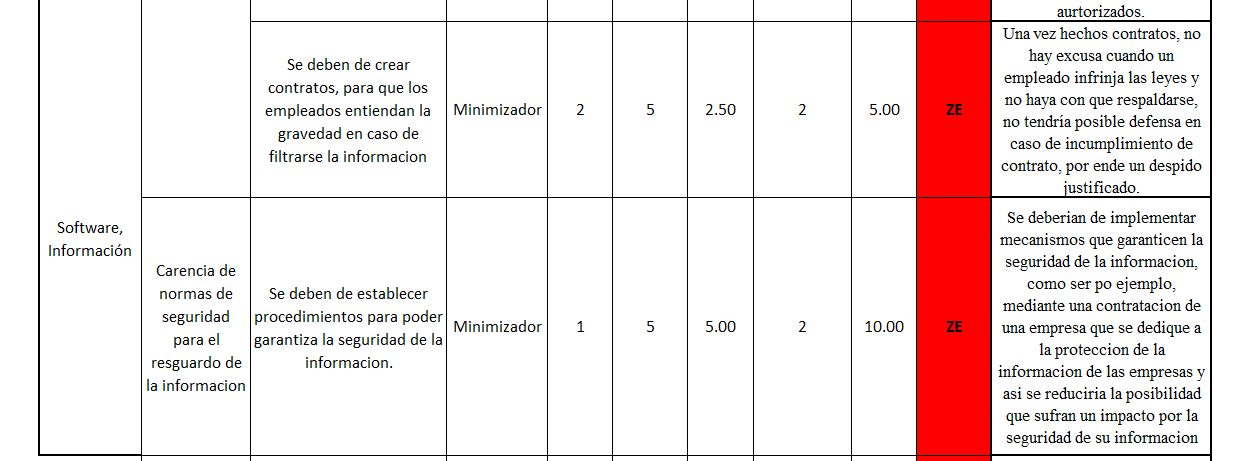
Contar con un fondo de contingencia para responder al impacto una vez se haya dado la amenaza, esto es para poder cubrir daños materiales o de algún soporte de software.

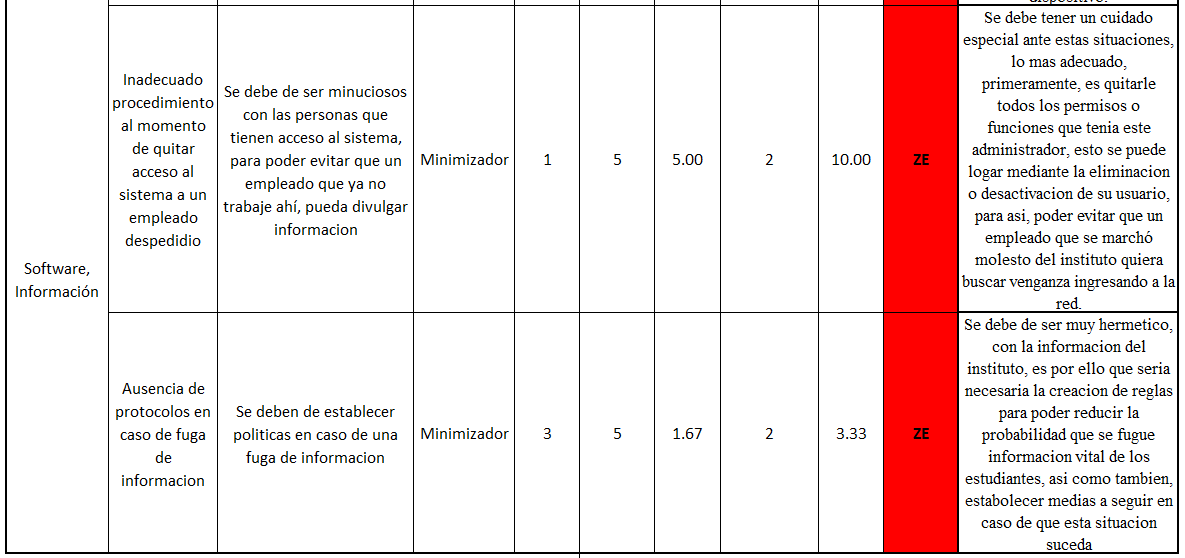
Contare con un sistema de alimentación ininterrumpido (UPS) para que en caso de ausencia de energía el servidor y computadoras sigan funcionando de manera correcta, se recomienda esto ya que en nuestro país la posibilidad de que ocurra un corte de energía es muy grande.

### **Amenaza por terremotos**

**Amenaza por terremotos**

**Fuga de información**





## **Costos en Seguridad Informática**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo de Recurso** | **Descripción del recurso** | **Valor Mensual** | **Valor anual** |
| **Recurso Humano** | Técnico en informática | L 19,000.00 | L 228,000.00 |
|  |
|  |
| **Recurso tecnológico** | Hardware: Computadoras, Servidores, Enrutadores, Conmutadores, Elementos de cableado Estructurado, Escritorios y Armarios | L 25,000.00 | L 300,000.00 |  |
| Software: Windows 10, Microsoft Office, Windows Server 2016 | L 7,400.00 | L 88,800.00 |  |
|  |  |  | L 616,800.00 |  |
|  |  |  |  |

## **Conclusiones**

* Se pudo lograr que el instituto Morazán sea consciente de aquellas vulnerabilidades, amenazas y riesgos que sufren sus recursos informáticos, así como también el impacto que podrían recibir si deciden pasar por alto estos elementos.
* Se logró detallar las amenazas a las que están expuestos los recursos informáticos junto con el nivel de probabilidad de que estas situaciones ocurran, para que el Instituto sea consciente que amenazas son más frecuentes.
* A partir de lo elaborado en dicho informe, el instituto Morazán puede continuar con la metodología MAGERIT, para poder elaborar un informe en donde se plasme como tratar todas estas amenazas a los que los recursos informáticos del instituto estan expuestos, asi como también darle un mejor seguimiento a lo anteriormente dicho y poder evaluar si estos planes de acción están siendo efectivos.
* Se pudieron clasificar los recursos informáticos del instituto Morazán de acuerdo a tres puntos fundamentales en la seguridad informática; como lo es la confidencialidad, integridad y disponibilidad.
* Gracias a la clasificación de los recursos informáticos según su disponibilidad, confidencialidad e integridad, el encargado del recurso ahora se encuentra más informado sobre la importancia que tiene este recurso para el correcto funcionamiento de la organización.
* Se logró detallar las vulnerabilidades a las que están expuestos los recursos informáticos del instituto, así como también los controles de seguridad que se tienen o no para poder hacerles frente a dichas vulnerabilidades.
* Como grupo consideramos que fue un proceso de bastante enseñanza, en donde pudimos aprender la importancia que tiene para una organización la seguridad de sus recursos informáticos, y la importancia que tiene la metodología Magerit para poder exponer todas estas amenazas, vulnerabilidades y riesgos a los que están expuestos el equipo información de una organización.

# **Bibliografía**

*Ambit*. (2022). Obtenido de . https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

*Ambit*. (2022). Obtenido de https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases

*Economipedia*. (2022). Obtenido de https://economipedia.com/definiciones/tipos-de-informacion.html

*IsoTools*. (2022). Obtenido de https://www.isotools.org/normas/

*Universidad VIU*. (2022). Obtenido de https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

*Weliver Security*. (2022). Obtenido de https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/