# UNIVERSIDAD CATÓLICA DE HONDURAS
**"NUESTRA SEÑORA REINA DE LA PAZ"**

**II Período**

**Trabajo a presentar:**
Actividad 3 Propuesta Análisis y Evaluación de riesgo Entregable 3

**Asignatura:**
Seguridad Informática y Gestión de Riesgos

**Catedrático:**
Lic. Patricia Medina.

**Presentado por:**

Emerson Guevara (0209199900371)
Elmer Izaac Figueroa (0101200101622)
Kevin Jafet Guzman (0101200003351)
Mario Alberto Cálix Salmeron (0209200100668)

**Fecha de Entrega:**
**31/07/2022**

# Índice

## Analisis Riesgo de Faith Learning Center

En la siguiente empresa llamada “Faith Learning Center” en base a un análisis de riesgo realizado se han encontrado ciertas vulnerabilidades las cuales son principalmente el factor humano los cuales son los estudiantes que tienen un total acceso a el equipo informático de uso personal como lo son computadoras, impresoras etc… Esto produce una brecha de vulnerabilidad ya que al no hacer uso correcto de este equipo pueden abrir la puerta a un pirata informático el cual puede producir un ataque y hacer caer a la empresa. Como segundo factor de vulnerabilidad es que existe una única red en la cual se conectan todos los dispositivos tanto de los estudiantes, docentes y visitas y sabemos que esto puede ser mejorado creando redes separadas para evitar filtración de información. Y como último riesgo considerado es que cualquier persona tiene acceso al centro de datos donde se encuentra el servidor principal de la empresa y algunos nodos de conexión. Sabemos que esto puede afectar negativamente ya que una persona tiene acceso directo a la información y puede generar y hacer cualquier acto de corrupción de los datos en el servidor.

Algunos ataques que podemos recibir como empresa seria “Man in the middle” creando robo de información de los estudiantes y filtración de datos de los mismos porque el pirata se centra entre la computadora del estudiante o usuario y la red engañando al usuario y robando/filtrando la información que es emitida. Otro ataque que puede ser es la descarga de archivos maliciosos, virus, gusanos ya que los alumnos y usuarios no siempre tiene la capacidad de identificar que sus descargas no están seguras. Por último sería un ataque directo al servidor por medio de una USB u otro tipo de dispositivo extraíble debido a la facilidad de acceso al cerebro principal de la institución.

Algunas posibles soluciones serían la separación de la red en tres partes, una para el personal y estudiantes de la empresa, otra para las visitas y por último para la conexión de los dispositivos de hardware de la institución. Por otro lado restringir y proteger más las descargas de los alumnos principalmente haciendo una autenticación de un experto el cual debe ser aprobado por una contraseña que no sea manejada por los alumnos. Por último el centro de datos restringirá su acceso al menos que esté autorizado y su acceso será mediante huella la cual dejará un registro de acceso y salida.

# Proyecto Análisis de Riesgos del Centro de Datos Faith LC

## Introducción

La seguridad informática se caracteriza por ser un tipo de seguridad intangible, la cual solemos relacionar con programas de antivirus o detectores de malware, entre otras herramientas. Sin embargo, la seguridad informática va más allá de programas o detectores de software malicioso, ya que no solo debe salvaguardar la integridad del dispositivo, sino garantizar la privacidad y la información que pueda almacenar, enviar o recibir entre dispositivos.

Teniendo en cuenta la importancia de la misma se llevará a cabo un proyecto sobre el análisis de sistemas de información donde estaremos evaluando la seguridad del centro de cómputo y a partir de esa evaluación poder ver cómo se podría mejorar dicha seguridad para la empresa de Faith Learning Center la cual es una empresa orientada a brindar los servicios de educación.

Para el desarrollo del análisis de este proyecto se utilizará la metodología MAGERIT para poder evaluar y gestionar los riesgos de mejor manera para poder analizar el impacto que puede tener para la empresa la violacion de la seguridad. Considerando que la metodología es útil para las empresas que quieren empezar a gestionar Seguridad de la información.

# Objetivos

## Objetivo general

Realizar un análisis de riesgos de seguridad de la información en la empresa llamada "Faith Learning Center" para poder identificar las posibles vulnerabilidades así mismo poder presentar un plan de mejora que ayudará a reforzar y evitar cualquier tipo de amenaza.

## Objetivos específicos

- Hacer un análisis correcto de la empresa para poder presentar un plan de mejora contra vulnerabilidades más preciso.
- Aprender y hacer buen uso de la metodología MAGERIT para la mejora de seguridad.
- Evaluar y gestionar los riesgos de la mejor manera para poder analizar el impacto.

## Planteamiento del problema

En la empresa Faith Learning Center la cual es una empresa orientada a brindar los servicios de educación y privacidad más altos en el litoral Atlántico con un enfoque en educación y seguridad del alumnado.

El problema que se ha estado presentando en los últimos meses es que la empresa se ha visto afectada debido a que el cuerpo de docentes y cuerpo estudiantil debido a que realizan el 80% de sus estudios académicos en computadores tiene un completo acceso a los navegadores y portales web los cuales lo hacen vulnerables a virus, gusanos y piratas informáticos.

En repetidas ocasiones se han visto varios equipos afectados con virus debido a que acceden a sitios no seguros y hacen descargas de documentos, extensiones, programas que no son certificados y es por esto que terminan comprometiendo no solamente su computadora de uso diario sino la red de área local de la Institución y por ende comprometen todos los dispositivos los cuales están accediendo a la red.

## Justificación

En el siguiente informe haremos una análisis de la empresa FAITH y veremos cuales son sus vulnerabilidades las cuales hemos considerado que es la red, los usuarios y el acceso al centro de datos siendo las principales brechas porque es donde se pueden generar los ataques. Hemos hecho un análisis y hay un 80 por ciento de los alumnos que pasan descargando archivos de internet para fines educativos y descargando aplicaciones que consideran interesantes para el mismo fin de aprendizaje. Por otro lado tenemos que un 50 por ciento de las visitas pide acceso a la red para fines que estime conveniente y por lo menos unas 10 personas acceden al centro de datos con diferentes razones. Vemos que hay una gran variedad de opciones donde se puede irrumpir a la información de la institución de diferentes formas y métodos debido a todas las vulnerabilidades que se presentan. Y es por eso que como anteriormente habíamos mencionado algunas posibles soluciones serían la separación de la red en tres partes, una para el personal y estudiantes de la empresa, otra para las visitas y por último para la conexión de los dispositivos de hardware de la institución. Por otro lado restringir y proteger más las descargas de los alumnos principalmente haciendo una autenticación de un experto el cual debe ser aprobado por una contraseña que no sea manejada por los alumnos. Por último el centro de datos restringirá su acceso al menos que esté autorizado y su acceso será mediante huella la cual dejará un registro de acceso y salida. Porque consideramos estas opciones, pues generan menos acceso a puertas que pueden abrir los usuarios.

## Marco Conceptual

## ¿Qué es seguridad informática?

La seguridad informática se presenta como la mejor aliada de empresas, organizaciones y grupos con presencia online para proteger su información y mantener su prestigio e imagen.

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.

Es por esto que esta disciplina del área de la informática encargada de la protección de la privacidad de datos dentro de los sistemas informáticos se ha convertido en una parte indispensable para los negocios y la operación de las empresas.

Está claro que no existen sistemas 100% infalibles, por lo que las organizaciones que se comunican a través del mundo digital deben buscar los mecanismos oportunos para garantizar la seguridad de sus datos, a través de alguno de los tipos de seguridad informática que existen y que deberían implementar en sus organismos.

## Principales tipos de seguridad informática

Al hablar de seguridad informática es fundamental distinguir algunas de las tipologías que existen, siendo los principales elementos a dar protección el software, la red y el hardware.

## Seguridad de hardware

Este tipo de seguridad se relaciona con la protección de dispositivos que se usan para proteger sistemas y redes —apps y programas de amenazas exteriores—, frente a diversos riesgos. El método más usado es el manejo de sistemas de alimentación ininterrumpida (SAI), servidores proxy, firewall, módulos de seguridad de hardware (HSM) y los data lost prevention

(DLP). Esta seguridad también se refiere a la protección de equipos físicos frente a cualquier daño físico.

## Seguridad de software

Usado para salvaguardar los sistemas frente ataques malintencionados de hackers y otros riesgos relacionados con las vulnerabilidades que pueden presentar los softwares. A través de estos "defectos" los intrusos pueden entrar en los sistemas, por lo que se requiere de soluciones que aporten, entre otros, modelos de autenticación.

## Seguridad de red

Principalmente relacionada con el diseño de actividades para proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal usados. Las principales amenazas en esta área son: virus, troyanos, phishing, programas espía, robo de datos y suplantación de identidad.

## La seguridad informática: un sector en auge y con gran demanda

Para hacer frente a estos problemas de seguridad se precisa contar con especialistas, como son los ingenieros con carreras afines a las tecnologías de la información y comunicación (TIC) —como puede ser la Carrera de Ingeniería Informática — que además posean conocimientos actualizados y especializados.

Para adquirirlos existen estudios especialmente estructuradas como la Maestría en Ciberseguridad de UNIR, un posgrado oficial con estudios 100% online, cuyo objetivo es formar a los alumnos en el uso de las herramientas más vanguardistas del sector, para enfrentarse a los ataques y amenazas cibernéticas que cada día se producen en el entorno digital.

En definitiva, al cada vez más empresas basar sus negocios en acciones digitales, estas se enfrentan a nuevos retos y amenazas, las cuales demandan profesionales capacitados para brindar soluciones, que permitan evitar y minimizar los ataques y riesgos derivados.

## Que es un SGSI?

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información. El término se denomina en Inglés “Information Security Management System” (ISMS).

El término SGSI es utilizado principalmente por la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission.

La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua:

**Plan (planificar):** es una fase de diseño del SGSI de evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

**Do (hacer):** es una fase que envuelve la implantación y operación de los controles.

**Check (controlar):** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

**Act (actuar):** en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

## Normas ISO en seguridad

Las normas ISO de Gestión de la Seguridad de la Información se denominan familia de normas ISO 27000 y son las siguientes:

- ISO 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Es la norma con arreglo a la cual se certifican por auditores externos. Su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Esta norma está publicada en España como UNE-ISO/IEC 27001:2007. Otros países donde también está publicada en español son, por ejemplo, Colombia , Venezuela y Argentina.
- ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.
- ISO 27000: Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de la Seguridad de la Información (SGSI). Generalidades y vocabulario.
- ISO 27003: Sistema de Gestión de la Seguridad de la Información (SGSI). Guía de implantación.

- ISO 27004: Tecnología de la información. Técnicas de Seguridad. Gestión de la Seguridad de la Información. Métricas.
- ISO 27007: Tecnología de la información. Técnicas de Seguridad.Guía de auditoría de un SGSI. Iniciadas las votaciones al DIS (cinco meses).

## Metodología Magerit

Es la metodología de análisis y gestión de riesgos elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro Criptológico Nacional (CCN).

MAGERIT es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización.

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT 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.

## Marco Teórico

En la actualidad las empresas tienen la necesidad de evolucionar y crecer a través de constantes cambios, dentro de los cuales los tecnológicos son los más comunes debido al rápido desarrollo de nuevas tecnologías y componentes, que a su vez rápidamente se ven vulnerados por fallos de seguridad que se extienden en tecnologías conocidas y usadas masivamente , por ello se presenta la importancia de generar medidas de Seguridad de la Información y Seguridad Informática que mitiguen o minimicen los riesgos y que permitan a las empresas asumir riesgos de acuerdo a su apetito de riesgo y que esto les permita ser competitivas y confiables conociendo un estado real de sus recursos y procesos.

Debido a las exigencias de mantener una empresa operativa ante las amenazas y los riesgos existentes, se han desarrollado diferentes metodologías y estándares para la identificación de riesgos, su análisis y su control mediante monitoreo y tratamiento con el fin de mitigar los riesgos.

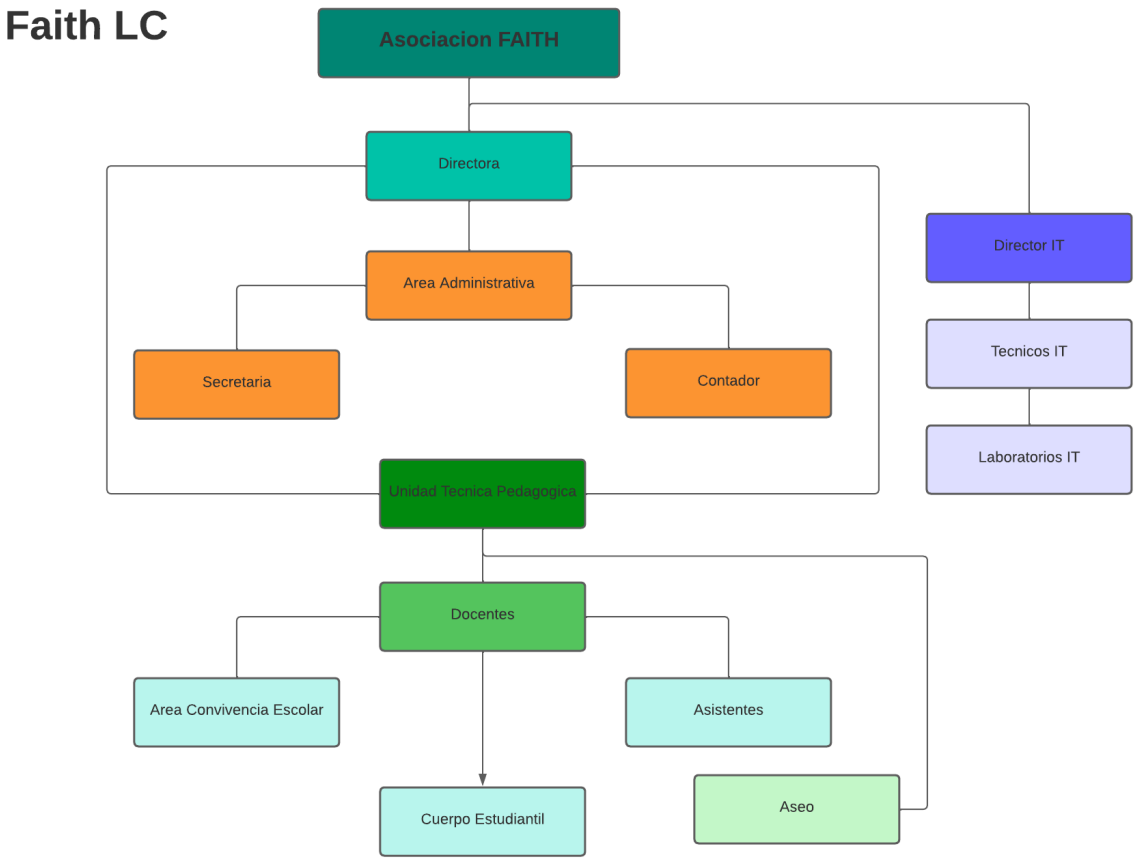
De acuerdo con las metodologías seleccionadas “Octave S”, “Magerit”, “DAFP” e “ISO 31000”, se realizó un primer acercamiento con personal de tecnología de la compañía con el fin de identificar la infraestructura y los componentes tecnológicos (descubrimiento de las oportunidades). Posteriormente con el jefe de área y con la gerencia de Faith Learning Center se hace la definición de expectativas y programación de actividades. Una vez finalizada la fase de recolección de información se procede con el análisis de riesgos, aprobación de la información y entrega de informe. Con el fin de cumplir con un Plan de acción para realizar el análisis de riesgos a Faith Learning Center

Definición del alcance Para definir el alcance se tomaron en consideración las siguientes premisas:

- Al no contar con un ejercicio previo de análisis de riesgos, el informe se construye como un insumo orientado a tener un panorama inicial y no maduro de análisis.

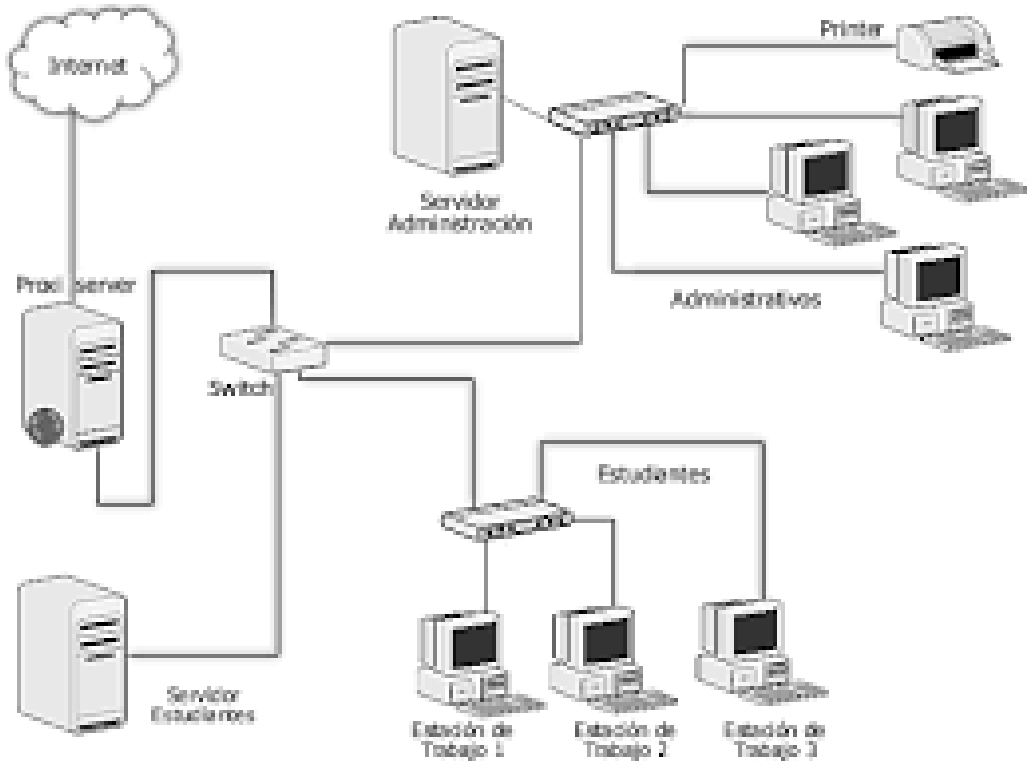
- La información no debe contar con supuestos, el análisis se construye únicamente con la información que Faith Learning Center entrega.
- En este aspecto es importante resaltar que contar con información completa, fiable, detallada y concisa permitirá ser más certero al realizar el análisis.
- El alcance se define basado en las definiciones que sean funcionales a la compañía y que estén en la capacidad de ser soportadas por los ejecutores.

## Organigrama de la empresa



## ¿Qué es 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.



# Planificación

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

El propósito de este plan es garantizar el uso y manejo seguro de todos los datos, sistemas informáticos y equipos informáticos de la escuela Faith Learning Center por parte de los estudiantes y empleados que se presenten en la escuela.

El plan es respaldar sistemas, procesos y procedimientos de red seguros, y proteger toda la información confidencial o de identificación personal que se almacena, en papel o digitalmente, en las instalaciones de Faith Learning o en servidores, computadoras y redes mantenidos por la escuela. Este plan apoya los esfuerzos para mitigar las amenazas que pueden causar daño a los equipos informáticos, sus estudiantes o sus empleados.

Se espera que todas las personas a las que se les otorga acceso a la red de la escuela y otros recursos tecnológicos sean cuidadosas y conscientes de las comunicaciones sospechosas y el uso no autorizado de los dispositivos del distrito y la red(recordando que son personas con poco conocimiento, se les otorgara clases de capacitaciones para aprender a manejar estos temas de ciberseguridad). Cuando un empleado u otro usuario se entera de una actividad sospechosa, debe comunicarse de inmediato con la parte responsable para compartir la información relevante.

Este plan y procedimiento también cubre a los proveedores/contratistas externos que albergan o tienen acceso a información de identificación personal de la escuela. Se requerirá que todas las entidades de terceros firmen el Acuerdo de Restricción en el Uso de Información Confidencial o de Identificación Personal antes de acceder a los sistemas o recibir información.

El desarrollo profesional para el personal y los estudiantes con respecto a la importancia de la seguridad de la red y las mejores prácticas se incluyen en los procedimientos. Los procedimientos asociados con este plan son consistentes con las pautas proporcionadas por profesionales de seguridad cibernética en todo el mundo. La implementación y las mejoras continuas de un sólido sistema de seguridad de hardware y software que está diseñado para proteger los datos, los usuarios y los activos electrónicos de Faith Learning Center.

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

El alcance específico del análisis es la capacidad de evaluar el nivel de seguridad que opera Laboratorios Fleming ubicados en Tegucigalpa, nos enfocaremos en identificar las diversas vulnerabilidades de seguridad de la empresa. Así como analizar el nivel de seguridad de la información. Relación comercial. , acceso al sistema así como acceso a la instalación, entre otras cosas.

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

- Identificar todos los riesgos que amenacen nuestros activos así brindar métodos de protección.
- Determinar el nivel de seguridad dependiendo el análisis y así presentar las posibles mejoras según las vulnerabilidades que se encuentren.
- Protección e integridad de la información de la empresa.
- Capacitar al personal para que cumplan con los estándares de seguridad de la información
- Fortalecer los procedimientos de seguridad de la empresa.
- Minimizar o eliminar el daño que las amenazas encontradas pueden causar.

## Análisis de Riesgos

### 2.1 Descripción de los activos o recursos informáticos de la empresa o organización.

| Tipo de Servicio | Especificaciones |
|---|---|
| **Servidor** | ● Intel Xeon, o AMD Opteron 2 núcleos Memoria RAM 8GB 2 discos duros de 1TB 2 tarjetas Ethernet |
| **Red LAN** | ● Puntos de Acceso EEROS<br>● Switches<br>● Routers |
| **Equipo de trabajo** | ● Lenovo Chromebooks(4 Ram, Intel I3,500Gb HDD) |
| **Equipo de Respaldo** | ● Equipo de alta gama (PC Gamers, Apple Macbooks, Ipads) |
| **Utilidades Fisicas** | ● Impresoras(Espson L355) |
| **Software** | ● Ofimatica, Licencias, Windows 10 |

## 2.2 Valoración de los activos o recursos.

| Principio de Seguridad | Clasificación | Definicion |
|---|---|---|
| Confidencialidad | Publico(1) | Este activo es considerado de carácter público y puede ser divulgado a cualquier persona o entidad interna o externa a la empresa. |
| Confidencialidad | Interno(2) | Este activo es utilizado por los funcionarios autorizados de la empresa para la ejecución de sus labores, y no puede ser conocida por terceros sin autorización del responsable del activo de información o directivas de la empresa. |
| Confidencialidad | Confidencial(3) | Este activo se considera altamente sensible y es utilizada por solo un grupo limitado de funcionarios o áreas para la ejecución de labores y no puede ser conocida por otros funcionarios de la empresa o terceros externos sin autorización especial del responsable de la información o directivas de la empresa. |
| Integridad | No sensitiva(1) | La pérdida o modificación no autorizada de este activo podría causar un daño leve o nulo para la empresa. |
| Integridad | Sensitiva(2) | La pérdida o modificación de este activo podría causar un daño que genera perjuicios importantes que afecten a la empresa, pero puede ser absorbido o asumido por este. |
| Integridad | Altamente Sensitiva(3) | La pérdida o modificación de |

| | | |
|---|---|---|
| | | este activo podría causar un daño grave que genere perjuicios que afecten significativamente a la empresa y que difícilmente podrían ser asumidos por ésta. |
| Disponibilidad | No critico(1) | El activo puede no estar disponible por un periodo de tiempo extendido, sin afectar la operación de la empresa. |
| Disponibilidad | Importante(2) | La no disponibilidad de este activo afectaría operaciones y servicios de los funcionarios |
| Disponibilidad | Mision Critica(3) | La no disponibilidad de este activo afectaría significativamente las operaciones, servicios de la empresa y el acceso a la información |

**Valoración / Confidencialidad de Activos**

| Activo | Valor | Descripción | C | I | D | Valor Final |
|---|---|---|---|---|---|---|
| **Servidor** | 1 | Esencial para el desempeño de la empresa | 3 | 3 | 3 | 3 |
| **Hardware de Red** | 10 | Esencial para el desempeño de la empresa | 2 | 2 | 3 | 3 |
| **Chromebooks** | 20 | Esencial para el desempeño de la empresa | 1 | 1 | 2 | 2 |
| **Macbooks** | 5 | Muy importante para la empresa | 2 | 1 | 1 | 2 |
| **Gamers** | 3 | Muy importante para la empresa | 2 | 1 | 1 | 2 |
| **Impresoras** | 3 | Importancia menor de la empresa | 1 | 1 | 1 | 1 |

## 2.3 Identificación de Amenazas y Probabilidades

| Nivel | Descripción de Probabilidad |
|---|---|
| 1 | No hay posibilidad de que suceda o haya ocurrido. |
| 2 | Posibilidad de que suceda cada cierto periodo. (6 meses a 1 año) |
| 3 | Posibilidad de que suceda cada trimestre. |

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

| ID Amenaza | Amenazas | Descripción de Probabilidad | NP | Motivo de Clasificación |
|---|---|---|---|---|
| **A1** | **Energia Electrica** | Fallas en caída o corte de la energía ya que frecuentemente suele pasar en la zona. | **3** | Es un incidente que suele suceder en repetidas ocasiones y la forma de combatirlo es mediante UPS. |
| **A2** | **Robos** | Nunca se puede descartar un robo ya que son frecuentados en nuestro país. | **1** | No nos ha sucedido pero puede darse el caso ya que la seguridad de acceso al edificio no es la mejor. |
| **A3** | **Errores Humanos** | Los humanos somos perfeccionistas en cometer fallas de uso, de acceso y de muchos tipos. | **2** | Se suele frecuentar que por medio de descargar entren virus al equipo |
| **A4** | **Acceso al Data Center** | El fácil acceso por el personal de la empresa es | **3** | El data center debe ser restringido el |

| | | | | |
|---|---|---|---|---|
| | | una debilidad producida para el datacenter | | acceso aunque sea personal de la empresa pero la información dentro de ella es de uso privado |
| **A5** | **Derrame de Alimentos en Equipo** | Puede darse mayormente en el equipo de uso diario como son las PC | **2** | Nos ha sucedido en ocasiones que cuentan con bebidas y se les derrama en su equipo |
| **A6** | **Mal Uso del Sistema** | Pueden producir un daño al sistemas por el mal uso o descargas de sitio no seguros y generar un virus en el equipo y dañarlo. | **2** | En la navegación y descargas suele filtrarse virus en alguna ocasiones |
| **A7** | **Caida de RED** | No se descarta esta opción ya que puede fallar uno de los puntos de acceso por el tiempo de uso | **1** | Aún no nos ha sucedido pero al pasar el tiempo nunca se descarta la opción ya que no hay redundancia en la red |
| **A8** | **Cyberseguridad** | Ataques informáticos son posibles en todo lugar que existan redes informáticas | **1** | No hay mucha información valiosa que se quiera proteger pero no se descarta la posibilidad |
| **A9** | **Daños Naturales** | Un tormenta, la caída de un árbol entre otros siempre pueden | **2** | Lluvias y caídas de árboles no dependen de nosotros así que |

| | | | | |
|---|---|---|---|---|
| | | suceder | | existe la posibilidad de que el agua perfore el edificio de una u otra forma. |
| **A10** | **Falsificación** | Suele darse que por curiosidad falsifican usuarios para ver información | **2** | Se han tomado las medidas necesarias pero siempre se han dado más casos ya que el descuido viene del mismo usuario y sus credenciales |

## 2.5 Matriz de impacto potencial

| Valor | Descriptor | Descripción del impacto |
|---|---|---|
| 1 | Insignificante | Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad. |
| 2 | Menor | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad. |
| 3 | Moderado | Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad |
| 4 | Mayor | Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad |
| 5 | Catastrófico | Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad. |

Fuente: autores

| TIPO DE ACTIVO: | CODIGO DE AMENAZA: | AMENAZA: | IMPACTO: |
|---|---|---|---|
| **Hardware** | **A1** | **Energia Electrica** | **4** |
| | **A2** | **Robos** | **5** |
| | **A3** | **Errores Humanos** | **5** |
| | **A4** | **Acceso al Data Center** | **4** |
| | **A5** | **Derrame de Alimentos en equipo** | **4** |
| | **A6** | **Mal uso del sistema** | **4** |
| | **A7** | **Caida de Red** | **3** |

| | | | |
|---|---|---|---|
| | A8 | Cyberseguridad | 4 |
| | A9 | Daños Naturales | 5 |
| | A10 | Falsificación | 5 |
| Software | A1 | Energia Electrica | 4 |
| | A2 | Robos | 5 |
| | A3 | Errores Humanos | 5 |
| | A4 | Acceso al Data Center | 4 |
| | A5 | Derrame de Alimentos en equipo | 4 |
| | A6 | Mal uso del sistema | 5 |
| | A7 | Caida de Red | 5 |
| | A8 | Cyberseguridad | 4 |
| | A9 | Daños Naturales | 3 |
| | A10 | Falsificación | 5 |
| Información | A1 | Energia Electrica | 5 |
| | A2 | Robos | 5 |

| | | | |
|---|---|---|---|
| | **A3** | **Errores Humanos** | **5** |
| | **A4** | **Acceso al Data Center** | **5** |
| | **A5** | **Derrame de Alimentos en equipo** | **3** |
| | **A6** | **Mal uso del sistema** | **5** |
| | **A7** | **Caida de Red** | **5** |
| | **A8** | **Cyberseguridad** | **4** |
| | **A9** | **Daños Naturales** | **5** |
| | **A10** | **Falsificación** | **5** |

## 2.6 Riesgo Potencial

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

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

A continuación se mostrará una tabla donde se encontrarán los riesgos que enfrenta cada activo de la empresa.

| Zona de Riesgo | Hardware | Software | Informacion | Total General |
|---|---|---|---|---|
| **Zona B** | | | | |
| **Advertencias de seguridad** | 2 | 1 | 1 | **4** |
| **PC sin contraseñas** | 1 | 1 | 1 | **3** |
| **Componentes dañados** | 0 | 0 | 0 | **0** |
| **Zona M** | | | | |
| **Energia Electrica** | 1 | 1 | 1 | **3** |
| **Errores Humanos** | 0 | 0 | 0 | **0** |
| **Fuego** | 0 | 0 | 0 | **0** |
| **Zona A** | | | | |
| **Acceso al Data center** | 2 | 2 | 1 | **5** |
| **Derrame de alimentos en equipo** | 0 | 0 | 0 | **0** |
| **Caida de Red** | 0 | 0 | 0 | **0** |
| **Mal uso del sistema** | 1 | 1 | 1 | **3** |

| Zona E | | | | |
|---|---|---|---|---|
| **Desastres naturales** | 3 | 0 | 0 | **3** |
| **Intrusiones en la red** | 0 | 0 | 0 | **0** |
| **Falsificación** | 0 | 1 | 1 | **2** |
| **Total** | **10** | **7** | **6** | **21** |

## 2.8 Matriz de riesgo potencial

Esta tabla está relacionada con la tabla de riesgo potencial y la matriz de impacto potencial ya que en la anterior se muestra el código de amenaza y la descripción de la amenaza, así mismo tomamos en cuenta el nivel de impacto , nivel de probabilidad y la zona de riesgo

| Tipo de activo | Código de amenaza | Amenaza | Impacto | Nivel de probabilidad | Riesgo potencial | Zona de riesgo |
|---|---|---|---|---|---|---|
| **Hardware** | A1 | **Energia Electrica** | 4 | 3 | **12** | **E** |
| | A2 | **Robos** | 5 | 1 | **5** | **A** |
| | A3 | **Errores Humanos** | 5 | 2 | **10** | **E** |
| | A4 | **Acceso al Data Center** | 4 | 3 | **12** | **E** |
| | A5 | **Derrame de Alimentos en equipo** | 4 | 2 | **8** | **A** |
| | A6 | **Mal uso del sistema** | 4 | 2 | **8** | **A** |
| | A7 | **Caida de Red** | 3 | 1 | **3** | **B** |
| | A8 | **Cyberseguridad** | 4 | 1 | **4** | **B** |
| | A9 | **Daños Naturales** | 5 | 2 | **10** | **E** |
| | A10 | **Falsificación** | 5 | 3 | **15** | **E** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Software** | A1 | **Energia Electrica** | 5 | 3 | **15** | **E** |
| | A2 | **Robos** | 4 | 1 | **4** | **B** |
| | A3 | **Errores Humanos** | 4 | 2 | **8** | **A** |
| | A4 | **Acceso al Data Center** | 5 | 3 | **15** | **E** |
| | A5 | **Derrame de Alimentos en equipo** | 4 | 2 | **8** | **A** |
| | A6 | **Mal uso del sistema** | 5 | 2 | **10** | **E** |
| | A7 | **Caida de Red** | 5 | 1 | **5** | **M** |
| | A8 | **Cyberseguridad** | 4 | 1 | **4** | **B** |
| | A9 | **Daños Naturales** | 3 | 2 | **6** | **M** |
| | A10 | **Falsificación** | 5 | 3 | **15** | **E** |
| **Informaci ón** | A1 | **Energia Electrica** | 5 | 3 | **15** | **E** |
| | A2 | **Robos** | 5 | 1 | **5** | **M** |
| | A3 | **Errores Humanos** | 5 | 2 | **10** | **E** |
| | A4 | **Acceso al Data Center** | 5 | 3 | **15** | **E** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | A5 | **Derrame de Alimentos en equipo** | 3 | 2 | **6** | **M** |
| | A6 | **Mal uso del sistema** | 5 | 2 | **10** | **E** |
| | A7 | **Caida de Red** | 5 | 1 | **5** | **M** |
| | A8 | **Cyberseguridad** | 4 | 1 | **4** | **B** |
| | A9 | **Daños Naturales** | 5 | 2 | **10** | **E** |
| | A10 | **Falsificación** | 5 | 3 | **15** | **E** |

## 2.9 Salvaguardas o controles existentes

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjugan simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal. En este caso presentamos una tabla con dos columnas donde en una de ellas nos muestra los niveles de efectividad (entre menor escala es, menor es su efectividad) y en la otra columna presentamos la descripción de la efectividad del control.

| Nivel | Descripción de la efectividad del control |
|---|---|
| **1** | Probabilidad de fallos ante amenazas |
| **2** | Ocasionalmente bueno, funciona la mayor parte del tiempo |
| **3** | Garantiza su funcionamiento de una forma eficaz durante la presencia de amenazas |

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

En esta tabla presentamos los controles de los activos que se implementan en el laboratorio de Faith Learning Center, donde hablamos de las amenazas y su nivel de efectividad. Es recomendable realizar este tipo de tabla ya que nos ayuda a llevar un seguimiento resumido de lo que sucede dentro del laboratorio.

| Activos | Amenazas | Controles | Tipo de control | Nivel de efectividad del control |
|---|---|---|---|---|
| Hardware | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | 2 |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | 2 |
| | **Errores Humanos** | Personal capacitado | Prevención | 2 |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | 2 |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | 2 |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | 2 |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | 2 |
| | **Cyberseguridad** | Personal capacitado para ataques | Prevención | 2 |

| | | | | |
|---|---|---|---|---|
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | 1 |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | 2 |
| Software | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | 2 |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | 2 |
| | **Errores Humanos** | Personal capacitado | Prevención | 2 |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | 2 |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | 2 |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | 2 |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | 2 |
| | **Cyberseguridad** | Personal capacitado para ataques | Prevención | 2 |
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | 1 |

| | | | | |
|---|---|---|---|---|
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | 2 |
| Informacion | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | 2 |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | 2 |
| | **Errores Humanos** | Personal capacitado | Prevención | 2 |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | 2 |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | 2 |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | 2 |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | 2 |
| | **Cyberseguridad** | Personal capacitado para ataques | Prevención | 2 |
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | 1 |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | 2 |

## Gestión de Riesgos

## 3.1 Impacto residual

| Activos | Amenazas | Controles | Tipo de control | Control Implementado? | Nivel de efectividad del control | Impacto potencial | Impacto residual |
|---|---|---|---|---|---|---|---|
| Hardware | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | Si | 2 | 4 | 2 |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | Si | 2 | 5 | 2.5 |
| | **Errores Humanos** | Personal capacitado | Prevención | Si | 2 | 5 | 2.5 |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | Si | 2 | 4 | 2 |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | Si | 2 | 4 | 2 |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | Si | 2 | 4 | 2 |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | Si | 2 | 3 | 1.5 |
| | **Cybersegu ridad** | Personal capacitado para ataques | Prevención | Si | 2 | 4 | 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | Si | 1 | 5 | 5 |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | Si | 2 | 5 | 2.5 |
| Software | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | Si | 2 | 4 | 2 |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | Si | 2 | 5 | 2.5 |
| | **Errores Humanos** | Personal capacitado | Prevención | Si | 2 | 5 | 2.5 |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | Si | 2 | 4 | 2 |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | Si | 2 | 4 | 2 |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | Si | 2 | 5 | 2.5 |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | Si | 2 | 5 | 2.5 |
| | **Cybersegu ridad** | Personal capacitado para ataques | Prevención | Si | 2 | 4 | 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | Si | 1 | 3 | 3 |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | Si | 2 | 5 | 2.5 |
| Informacion | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | Si | 2 | 5 | 2.5 |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | Si | 2 | 5 | 2.5 |
| | **Errores Humanos** | Personal capacitado | Prevención | Si | 2 | 5 | 2.5 |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | Si | 2 | 5 | 2.5 |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | Si | 2 | 3 | 1.5 |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | Si | 2 | 5 | 2.5 |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | Si | 2 | 5 | 2.5 |
| | **Ciberseguridad** | Personal capacitado para ataques | Prevención | Si | 2 | 4 | 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | Si | 1 | 5 | 5 |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | Si | 2 | 5 | 2.5 |

## 3.2 Matriz de impacto residual y riesgo residual

| Activos | Amenazas | Controles | Tipo de control | Control Implementado? | Eficacia del control | Impacto potencial | Impacto residual | Nivel de probabilidad | Riesgo Residual | Zona de riesgo residual |
|---|---|---|---|---|---|---|---|---|---|---|
| Hardware | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | Si | 2 | 4 | 2 | 3 | 6 | **M** |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | Si | 2 | 5 | 2.5 | 1 | 2.5 | **B** |
| | **Errores Humanos** | Personal capacitado | Prevención | Si | 2 | 5 | 2.5 | 2 | 5 | **M** |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | Si | 2 | 4 | 2 | 3 | 6 | **M** |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | Si | 2 | 4 | 2 | 2 | 4 | **B** |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | Si | 2 | 4 | 2 | 2 | 4 | **B** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | Si | 2 | 3 | 1.5 | 1 | 1.5 | **B** |
| | **Cyberseguridad** | Personal capacitado para ataques | Prevención | Si | 2 | 4 | 2 | 1 | 2 | **B** |
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | Si | 1 | 5 | 5 | 2 | 10 | **E** |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | Si | 2 | 5 | 2.5 | 3 | 7.5 | **M** |
| Software | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | Si | 2 | 4 | 2 | 3 | 6 | **M** |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | Si | 2 | 5 | 2.5 | 1 | 2.5 | **B** |
| | **Errores Humanos** | Personal capacitado | Prevención | Si | 2 | 5 | 2.5 | 2 | 5 | **M** |
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | Si | 2 | 4 | 2 | 3 | 6 | **M** |
| | **Derrame de** | No se permite el ingreso de | Administración | Si | 2 | 4 | 2 | 2 | 4 | **B** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Alimentos en equipo** | alimentos | | | | | | | | |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | Si | 2 | 5 | 2.5 | 2 | 5 | **M** |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | Si | 2 | 5 | 2.5 | 1 | 2.5 | **B** |
| | **Cyberseguridad** | Personal capacitado para ataques | Prevención | Si | 2 | 4 | 2 | 1 | 2 | **B** |
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | Si | 1 | 3 | 3 | 2 | 6 | **M** |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | Si | 2 | 5 | 2.5 | 3 | 7.5 | **M** |
| Informacion | **Energia Electrica** | Contar con un constante flujo de energía eléctrica | Prevención | Si | 2 | 5 | 2.5 | 3 | 7.5 | **M** |
| | **Robos** | Infraestructura capacitada para robos | Seguridad | Si | 2 | 5 | 2.5 | 1 | 2.5 | **B** |
| | **Errores Humanos** | Personal capacitado | Prevención | Si | 2 | 5 | 2.5 | 2 | 5 | **M** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Acceso al Data Center** | Seguridad perimetral | Seguridad | Si | 2 | 5 | 2.5 | 3 | 7.5 | **M** |
| | **Derrame de Alimentos en equipo** | No se permite el ingreso de alimentos | Administración | Si | 2 | 3 | 1.5 | 2 | 3 | **B** |
| | **Mal uso del sistema** | Capacitación al personal | Prevención | Si | 2 | 5 | 2.5 | 2 | 5 | **M** |
| | **Caida de Red** | Reducir el tiempo de inactividad de sus servicios | Prevencion | Si | 2 | 5 | 2.5 | 1 | 2.5 | **B** |
| | **Cyberseguridad** | Personal capacitado para ataques | Prevención | Si | 2 | 4 | 2 | 1 | 2 | **B** |
| | **Daños Naturales** | Infraestructura soportable a daños naturales | Seguridad | Si | 1 | 5 | 5 | 2 | 10 | **E** |
| | **Falsificación** | Aseguramiento de protección de datos | Seguridad | Si | 2 | 5 | 2.5 | 3 | 7.5 | **M** |

## 3.3 Comunicación del riesgo y recomendaciones

Los sistemas eléctricos que respaldan los servidores, el almacenamiento y el entorno de la instalación pueden presentar una variedad de riesgos para el personal del centro de datos. Garantizar la seguridad física de los empleados y de las demás personas que hagan uso de estos laboratorios debe ser el objetivo principal en cualquier centro de datos. Comprender cómo evaluar y mitigar el riesgo puede ayudar tanto a los propietarios, personas que hagan uso de estos centros y al personal del centro de datos a mantenerse seguros ahora y en el futuro.

Los centros de datos albergan una variedad de sofisticados sistemas eléctricos y mecánicos de alta potencia que presentan un riesgo significativo de daño físico para el personal y el edificio si no se gestionan adecuadamente. La excelente seguridad del centro de datos significa priorizar la seguridad del personal y la gestión adecuada de los equipos peligrosos por encima de todo.

La naturaleza de los riesgos en las instalaciones de un centro de datos puede variar de una instalación a otra. Algunos de los riesgos que se presentan a continuación tenemos que tomarlos en cuenta para contar con un centro de datos seguro:

- Peligros físicos. Los cables de alimentación y los cables alrededor de los sistemas eléctricos presentan riesgos de tropiezos, y los paneles de piso abiertos en pisos elevados presentan riesgos de caídas.
- Riesgos de altura. El personal de las instalaciones del centro de datos a menudo trabaja a gran altura en racks altos.
- Peligros ambientales. Los factores de riesgo ambientales incluyen calor y frío excesivos , así como ruidos fuertes. El personal que permanece en el sitio durante períodos prolongados se vuelve susceptible a la hiper o hipotermia y la pérdida de audición. Los peligros ambientales cambian según la época del año, el equipo en el que trabaja el personal y el personal particular involucrado, pero un centro de datos debe considerar los riesgos inherentes a estos factores en todo momento.
- Peligros del sistema de seguridad de las instalaciones. Los sistemas de seguridad incluyen sistemas de supresión de incendios, métodos de carga de baterías de UPS , tipos de baterías de respaldo.

Por parte de nuestro equipo se recomienda tomar medidas a aquellas amenazas que ponen en mayor peligro el centro de datos de Faith Learning Center, sin olvidar las amenazas mínimas. Primero se debería tomar en cuenta lo que peligra más ya que encontramos varios errores o problemas que podrían ocasionar pérdidas de datos en un futuro. Se recomienda guiarse de la metodología Magerit ya que aquí se encuentran distintas metodologías para llevar a cabo planes de contingencia para la seguridad de un centro de cómputo.

Evaluar los procesos y procedimientos del personal en busca de riesgos para garantizar que el personal permanezca seguro en todo momento. También revisar dichos procedimientos regularmente para asegurarse de que aún cumplan con las pautas y los requisitos de seguridad locales.

La creación de una evaluación de riesgos del personal para los centros de datos requiere aportes del equipo de recursos humanos, el personal en el sitio y el equipo de TI. Cada equipo debe seguir requisitos y pautas específicas e incluirlos en su evaluación para llevar a cabo estas tareas.

La asignación de un líder de seguridad dedicado a que sea responsable de todas las actividades de seguridad puede facilitar la coordinación entre los equipos relevantes. Esta persona supervisa la estrategia de seguridad de alto nivel y establece una comunicación clara al respecto con el personal. Esta persona identifica y desarrolla programas de capacitación en seguridad apropiados para el personal que siguen las pautas establecidas y los procesos internos. El líder de seguridad también monitorea y cumple continuamente con los estándares y prácticas de seguridad cambiantes y realiza auditorías periódicas. El líder de seguridad dedicado debe documentar la estrategia general y coordinar el desarrollo de procesos y procedimientos por parte de las partes relevantes. Sin embargo, el personal TI siempre debe participar también en los esfuerzos de documentación; estas personas conocen los riesgos inherentes a sus trabajos mejor que nadie.

La estrategia, el proceso y los procedimientos de seguridad solo funcionan si el personal los usa. El líder o líderes de seguridad siempre deben documentar la información de seguridad, almacenar esa documentación en algún lugar donde todo el personal pueda acceder a ella, actualizarla según sea necesario y celebrar reuniones y sesiones de capacitación sobre seguridad

con regularidad. El personal de todos los niveles debe conocer los protocolos de seguridad vigentes y sentirse respaldado en su capacidad para rechazar cualquier trabajo que parezca inseguro. El líder de seguridad debe programar todo el entrenamiento de seguridad y asegurarse de que el personal asista. Los gerentes deben colaborar con el líder de seguridad para mantener las medidas de seguridad adecuadas y deben participar en cualquier actividad de actualización de la evaluación de riesgos.

### 3.3.1 Tratamiento del riesgo

Dentro del centro de datos, se han evaluado en varias ocasiones y por varias personas lo que podrían y lo que son las amenazas que afectan esta área. En esta tabla mostramos el elemento en riesgo, el riesgo que esta tiene con sus fortalezas, debilidades y la acción a tomar para manejar estas situaciones.

| **Elemento en riesgo** | **Riesgo** | **Fortaleza** | **Debilidad** | **Accion** |
|---|---|---|---|---|
| Software | Incapacidad de realizar actividades | Está en constante chequeo | No contar con personal adecuado | Capacitación de nuevos empleados |
| Hardware | Problemas de daños físicos | Hardware con tolerancia a fallos | Falta de conocimientos por parte del personal | Crear capacitaciones para el uso adecuado |
| Cuarto Tecnico | Deja sin funcionamiento el centro de datos | Contar con personal de mantenimiento inmediato | No contar con suficiente personal de mantenimiento | Tener a disponibilidad la cantidad necesaria de personal calificado |
| Personal | El personal no esté capacitado | Personal dispuesto a mejorar | Poco personal dentro del centro de datos | Contar con más personas dispuestas a mejorar y dar todo lo mejor |

## 3.3 Costos en Seguridad Informática

| Activos | Controles | Costo Mensual | Costo Anual |
|---|---|---|---|
| Servidor | Implementar servidores seguros de autenticación web | 12,000 lps | 240,000 lps |
| | Recibir capacitaciones para configurar estos errores | 5,000 lps | 60,000 |
| | Activar medidas de seguridad en la configuración | 2000 lps | 24,000 lps |
| Red LAN | Mantenimiento de la Red | 1000 lps | 12,000 lps |
| | Implementar medidas de seguridad | 5,000 lps | 60,000 lps |
| | Verificación de registros correctos | 1,000 lps | 12,000 lps |
| | Implementación de seguridad informática dentro del laboratorio | 1,000 lps | 12,000 lps |
| Equipo de trabajo | Mejora de los equipos para su uso de trabajo | 10,000 lps | 120,000 lps |
| | Asegurar todos los controles de seguridad de los equipos | 10,000 lps | 120,000 |
| Equipo de respaldo | Mejora de los equipos para su uso de trabajo | 20,000 lps | 240,000 lps |
| | Asegurar todos los controles de seguridad | 5,000 lps | 60,000 lps |

| | | | |
|---|---|---|---|
| Utilidades fisicas | Recibir entrenamientos apropiados para la reparación y utilización de estos equipos | 1,000 lps | 12,000 |
| Software | Procedimientos apropiados para la seguridad | 1,000 lps | 12,000 lps |
| | Chequear las licencias cada cierto periodo de tiempo | 5,000 lps | 60,000 lps |

## Conclusiones

Podemos decir que se encuentra en buen estado y con un buen rendimiento ya que cada computadora cuenta con un software y hardware en buen estado con el rendimiento que debe de estar para los estudiantes, además cuenta con personas capacitadas para apoyo de cualquier dificultad en caso de problemas presentados por las computadoras como podrían ser virus espías y falta de quemador de cualquier equipo de ahí concluimos que el centro de cómputo debe de estar y contar con un mantenimiento especializado para la realización de las actividades a trabajar.

## Recomendaciones

Sensibilización y capacitación de empleados. Uno de los principales riesgos para la información de las empresas son las prácticas descuidadas de sus trabajadores al usar Internet. Estas prácticas incluyen abrir correos electrónicos con programas malintencionados, uso de WiFi libre que puede comprometer la transferencia de información e incluso la pérdida de dispositivos de almacenamiento, teléfonos inteligentes o tabletas que contienen información relevante o claves de acceso de la empresa. Por esto es importante sensibilizarlos y capacitarlos sobre buenas prácticas en el uso de Internet y dispositivos.

# 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/