ENTREGABLE 3

Seguridad Informática y Gestión de Riesgo

Universidad Católica de Honduras

Integrantes:

David Mendoza 0601-1998-00243
Hader Méndez 0615-1998-00403
Jonathan Alemán 0101-1998-04248
Will Mejía 0209-2001-00104

Grupo 7

Campus Global

Introducción

El presente informe se desarrolla una evaluación de la seguridad informática aplicada a una empresa del rubro estudiantil por medio de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). MAGERIT nace de la necesidad de que el mundo cada día avanza tecnológicamente la cual presenta grandes beneficios para todo el mundo en general, pero a su vez genera algunos riesgos de seguridad de la persona. Su causa es que todos los que hacemos uso de algún tipo de tecnología conozcamos los riesgos y que hay manera de gestionarlos para minimizar su impacto de riesgo. En este análisis de evaluación de riesgos se realizará un estudio de los posibles riesgos en lo que puede verse afectada la Institución con el fin de reducir la probabilidad de verse afectados por un problema mayor.

Objetivos

Objetivo General

- Realizar un análisis de riesgo mediante la información tecnológica proporcionada por la institución haciendo uso de la metodología MAGERIT.

Objetivos específicos

- Utilizar la metodología MAGERIT para reducir los riesgos de un centro educativo.
- Desarrollar una propuesta de mejora de la seguridad informática.
- Evaluar el nivel de seguridad informática actual del centro educativo.

Planteamiento del problema

El objetivo de este análisis es realizar una estimación de que tan afectada esta la red escolar de la Institución New Hope para comprender su situación actual y tomar en cuenta cuales pueden ser sus puntos de riesgo. De esta forma podremos identificar los problemas principales y saber que los está causando.

Justificación

El presente problema que intentaremos solucionar es sobre la arquitectura de RED que se maneja en K.S.B.S – N.H.H.S en la cual cualquier usuario que mantenga acceso al WIFI tiene un acceso completo a la RED sin ningún tipo de restricción. Por lo que se planteará una posible solución al fallo de seguridad informático que se está presentando actualmente. En la actualidad toda empresa debe de contar con una seguridad informática de alto nivel si manipulan información privada de clientes los cuales son los estudiantes mismos. Esta situación nos lleva a atacar el problema con urgencia para que sus sistemas sean más seguros y no exista algún tipo de riesgo en un futuro. La presenta investigación es de alta viabilidad, ya que dispone disponemos con los recursos necesarios proporcionados por el instituto para llevarla a cabo. Este trabajo a realizar beneficia a todos los posibles clientes que den acceso a sus datos privados, así mismo a los empleados de la institución que cuentan con datos privados en los sistemas de la institución.

New Hope

La organización que hemos analizado para la implementación de la seguridad informática tiene como nombre “New Hope” siendo esta una escuela. Información básica:

- ✓ Directora de la institución: Marilia Antúnez
- ✓ Dirección: Barrio Independencia, Ave. Morazán a la par de FedEx Express
- ✓ Atención: de 8 am a 5 pm

El rubro en el que se enfoca la organización es en el aprendizaje y servicio a la educación, teniendo clases de aprendizaje desde Primer grado hasta 11vo, contando también con la carrera de humanidades, Cuenta con las debidas herramientas de hardware (computadoras, acceso a internet, impresoras, fotocopiadoras, cortadores).

Redes disponibles en la empresa (wifi)

Actualmente la escuela “New Hope” cuenta con 1 red wifi con su respectivo uso, por lo que el internet que se puede llegar a tener en el área puede llegar a ser bastante limitada cuando se acceden desde diferentes dispositivos, siendo una de las razones por las cuales estamos implementando esta estrategia de seguridad informática. También teniendo en cuenta que el uso de la red wifi dentro de la institución debe ser únicamente para el uso de las herramientas educativas que sean asignadas por un catedrático, por eso, con esto poder limitar que los alumnos puedan acceder a páginas que sean solo autorizadas por el encargado del área de redes.

Análisis realizado

Es necesario tener un control, administración y uso debido de las redes del área, es por eso que implementando debidas normas de uso, el uso exclusivo de las aplicaciones y páginas posibles acceder, no solo se garantiza que los equipos consuman mucho más recurso de lo necesario y retrasan el proceso de las otras máquinas del área, además que hemos analizado que los alumnos tendrán un mejor rendimiento, porque no tendrán manera de distraerse en páginas web, juegos u otra cosa que no sea relacionado con el aprendizaje.

Principales Tipos de Seguridad Informática

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.

Seguridad de hardware

Este tipo de seguridad se relaciona con la protección de dispositivos que se usan para proteger sistemas, 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.

Planeación de la seguridad informática en la organización.

Para cumplir con una buena planificación, debemos tener en cuenta muchos aspectos a seguir, comenzando por una formulación de la seguridad informática que consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que puede causar serias perturbaciones para el normal desarrollo de las actividades de la institución. De igual manera también tenemos que tener presente un alcance ya que este nos llevará a ver más allá de lo que queremos lograr, en nuestro caso implementaremos un análisis utilizando la metodología Magerit para dedicarlo al laboratorio de computación y poder encontrar las posibles fallas en el laboratorio para que la institución actúe de tal manera que pueda solucionarlas.

Alcance del análisis y evaluación de riesgos del Sistema Informático.

Aplicamos el alcance del análisis y gestión de riesgos basado en el método Magerit para poder reparar muchos de los daños previstos en los laboratorios de cómputo institucionales, tanto en partes de equipos como en ciertas partes de infraestructura. Como cableado dañado, así como enrutadores, interruptores y algunos equipos en mal estado. Si se llevan a cabo dichas reparaciones, se requiere un mantenimiento continuo del laboratorio, ya que esto evitará que se repitan incidentes futuros del mismo problema.

Objetivos del análisis y evaluación de riesgos del Sistema Informático.

- Rehabilita tu laboratorio de manera rápida y segura para que todas las funciones e infraestructura estén en perfectas condiciones para su correcto uso.
- Verificar el funcionamiento de cada dispositivo para que sea perfecto para el uso normal en la institución.
- Realice reparaciones en la infraestructura, como edificios y cableado, para mantener el equipo en un lugar seguro y funcionando de manera óptima.
- Reemplace el equipo que esté en malas condiciones y repare el equipo que aún tenga reparaciones.
- Haga una lista de los daños encontrados en los laboratorios institucionales para ilustrar qué partes se deben mantener de forma continua para evitar estos problemas.
- Proporciona instrucciones sobre cómo mantener el equipo que estará en el laboratorio de computación.

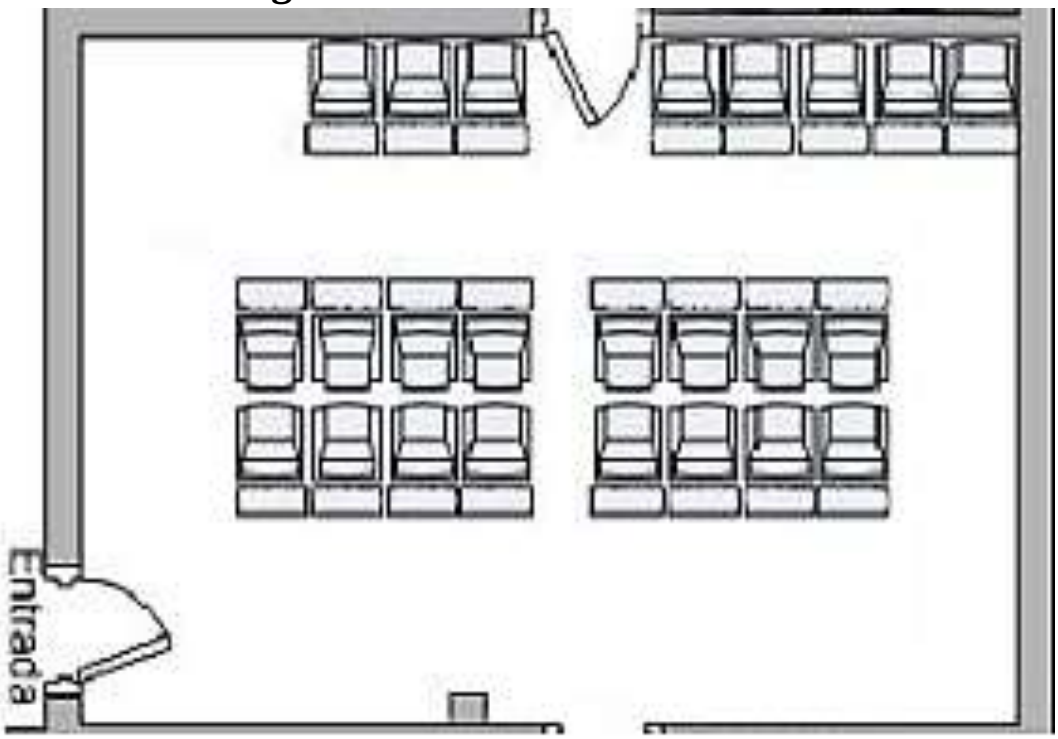
¿Qué es un SGSI?

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de Política de Gestión de la Información. esta palabra se llama en inglés "Sistema de Gestión de la Seguridad de la Información" (SGSI). El término ISMS es utilizado principalmente por ISO/IEC 27001, que es un estándar octubre de 2005 por International Estandarizado y aprobado por la Comisión Electrotécnica Internacional. ISO/IEC 27001 especifica el establecimiento, implementación, Mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) Según el famoso "Ciclo de Deming": PDCA, un acrónimo de Plan, Do, Check, Act (planificar, ejecutar, comprobar, actuar).

Normas ISO

Las normas ISO son un conjunto de reglas que proporcionan a las empresas una serie de procedimientos para que se produzca una gestión adecuada en todos sus ámbitos. Son establecidas por el Organismo Internacional de Estandarización, y se componen de guías relacionadas con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización. Todo el conjunto de normativa ISO tienen un mismo fin: mejorar los resultados de la empresa, demostrar su liderazgo e innovación y conseguir la diferenciación respecto a sus competidores. La certificación ISO de un producto o servicio funciona como garantía de un estándar de calidad y seguridad imposible de alcanzar de otra manera.

Diagrama de Sistema Informático



Planeación de la seguridad informática en la organización.

Para cumplir con una buena planificación, debemos tener en cuenta muchos aspectos a seguir, comenzando por una formulación de la seguridad informática que consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que puede causar serias perturbaciones para el normal desarrollo de las actividades de la institución. De igual manera también tenemos que tener presente un alcance ya que este nos llevará a ver más allá de lo que queremos lograr, en nuestro caso implementaremos un análisis utilizando la metodología Magerit para dedicarlo al laboratorio de computación y poder encontrar las posibles fallas en el laboratorio para que la institución actúe de tal manera que pueda solucionarlas.

Descripción de los activos o recursos informáticos de la empresa u organización.

Equipo	**Información y servicios que maneja.**
Router	Es responsable de proporcionar conexiones para todos los estudiantes dentro del laboratorio.
Switch	Se utiliza para desarrollar proyectos web donde los estudiantes pueden conectarse y probar sus componentes web.
Cableado en general	Este consiste en cables de red conectados por estudiantes y cables de alimentación utilizados en equipos de cómputo.
Computadoras	Son los dispositivos que utilizan los estudiantes para llevar a cabo sus actividades diarias.
Aires acondicionados	Se utiliza para mantener la temperatura dentro del laboratorio de trabajo.
Muebles	Consta de pupitres para ordenadores, sillas para alumnos y archivadores para expedientes de profesores.
Canaletas para cable de red	Se encargan de proteger y ocultar los cables de red para que no se desvíen.
Suministro eléctrico	Es responsable de proporcionar electricidad de calidad a todos
Componentes eléctricos	Dispositivos electrónicos que componen el sistema de información de una empresa.

Identificación de activos

Tipo de Servicio	Características
Hardware	• Network IDS • Firewall Físico Red
Red	• Router • Punto de acceso • 2 Swicth 48 puertos
Software	• Windows 10 • Microsoft Office • CorelDRAW • Adobe
Instalación	• Cableado estructurado • Conexiones eléctricas

Valoración de los activos o recursos.

Valoración de Activos		
Valor		**Criterio**
7-10	Alto	Daño grave en el laboratorio de computo
4-6	Medio	Daño importante en el laboratorio de computo
1-3	Bajo	Daño menor en el laboratorio de computo

Clasificación de los activos

Principio de seguridad	Clasificación	Definición
Confidencialidad	Público (1)	Puede ser divulgada a cualquier persona o entidad interna o externa sin restricción alguna y está contemplada en las leyes de transparencia de datos.
	Interna (2)	Esta información se utiliza para llevar a cabo su misión y no debe ser conocida por terceros sin la autorización del responsable de la información o de la instrucción del colegio.
	Confidencial (3)	Esta información se considera altamente sensible y solo es utilizada por un grupo limitado de personas o áreas para realizar tareas y no puede ser conocida por otras personas o terceros. No autorizado específicamente por el Oficial de Información o la Junta del Colegio.
Integridad	No sensitiva (1)	pérdida o modificación no autorizada de este La información puede causar poco o ningún daño en el colegio
	Sensitiva (2)	pérdida o modificación no autorizada de este La información puede causar daño, resultando en un daño significativo que afecte al colegio, pero puede ser absorbida o asumida.
	Altamente Sensitiva (3)	pérdida o modificación no autorizada de esta información podría causar lesiones graves, resultando en Los daños que tendrían un impacto significativo en la escuela son casi imposibles de asumir.
Disponibilidad	No crítico (1)	Esta información puede no estar disponible por un período prolongado de tiempo sin afectar las operaciones.
	Importante (2)	La no disponibilidad de esta información afectará Operaciones y servicios escolares.

Identificación de amenazas y probabilidad

Nivel	Descripción de amenazas
1	No hay evidencia de que haya ocurrido
2	Probable que se produzca una vez cada dos años
3	Probabilidad de que se dé una vez cada trimestre

Amenazas clasificadas por su tipo y su nivel de probabilidad

	Amenazas	Descripción	NP	Razón de clasificación
A1	Desastres Naturales	Huracanes, terremotos, humedad que pueda dañar los equipos	2	Los huracanes son probables que se produzcan cada uno o dos años, los terremotos no son descartables en cualquier tiempo
A2	Errores humanos	Daños causados por falta de información de manejo causando interrupciones en las actividades	3	Los errores pueden ocurrir en cualquier momento dentro de plazos cortos
A3	Amenazas legales	Cambios en las regulaciones y lineamientos del gobierno	1	No se tiene evidencia que haya ocurrido, pero puede ocurrir
A4	Falla en las redes	Fallas en las infraestructuras de cableado de red afectando la comunicación	2	La falta de mantenimiento a los equipos de red ha traído problemas tanto de comunicación como del objetivo principal que es la enseñanza
A5	Mal uso de los equipos	El uso de software sin licencia o autorización ya sea por cualquier usuario	3	Es uno de los problemas más presentados el uso de equipos sin autorización o piratas, siendo frecuente
A6	Robos	Robo de información y de hardware	1	No se tiene evidencia que haya ocurrido, pero no se descarta

Matriz de impacto potencial

Valor	Descriptor	Descripción del impacto
1	Insignificante	Los impactos a tener en cuenta casi no tendrán afecto en las labores
2	Menor	El impacto seria bajo
3	Moderado	Si el hecho se llegara a presentar tendría impactos moderados
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias
5	Catastrófico	Si el hecho se llegara a presentar, tendría consecuencias catastróficas

Tipo de activo	Código de amenaza	Amenaza	Impacto
HARDWARE	A1	Desastres naturales	5
	A2	Errores humanos	2
	A3	Amenazas legales	3
	A4	Fallas en las redes	2
	A5	Mal uso de los equipos	2
	A6	Robos	5
Software	A1	Desastres naturales	5
	A2	Errores humanos	4
	A3	Amenazas legales	4
	A4	Falla en las redes	3
	A5	Mal uso de los equipos	4
	A6	Robos	5
Información	A1	Desastres naturales	5
	A2	Errores humanos	4
	A3	Amenazas legales	2
	A4	Falla en las redes	2
	A5	Mal uso de los equipos	2
	A6	Robos	5

Riesgo potencial

Riesgo Potencial					
Probabilidad	Impacto				
1 2 3	Insignificante	Menor	Moderado	Mayor	Catastrofico
	H (1)	W (2)	D (2)	D (2)	K (2)
	H (2)	W (3)	D (3)	D (3)	D (3)
	W (1)	D (1)	W (1)	K (1)	D (1)
	H: Zona de riesgo baja: Asumir el riesgo (1-4)				
	W: Zona de riesgo moderada: asumir el riesgo, reducir el riesgo (57)				
	D: Zona de riesgo alta: Reducir el riesgo, evitar, compartir o transferir (8-9)				
	K: Zona de riesgo extrema: Reduce el riesgo, evitar, compartir o transferir (10-15)				

Número de amenazas por zona de riesgo y tipo activo

Zona de riesgo	Hardware	Información	Software	Total, General
Zona H				
Componentes dañados	5	0	0	5
Computadoras sin contraseñas	1	1	1	3
Advertencias de seguridad	1	1	1	3
Protección contra USB	1	2	1	4
	8	4	3	15
Zona W				
Desastres naturales	2	0	0	2

Errores humanos	1	3	1	5
Fuego	4	0	0	4
Daños por agua o inundaciones	4	0	0	4
	11	3	1	15
Zona D				
Exposición de contraseñas	0	4	1	5
Robo de componentes	5	0	0	5
Mal uso del software	2	2	1	5
Sabotaje de los cables de red	3	2	0	5
	10	8	2	20
Zona K				
Fallas en la infraestructura	2	0	1	3
Intrusiones en la red	0	4	1	5
Sabotaje de los routers	3	1	1	5
Fallas en la red	1	4	3	8
	6	9	6	21
Total	35	24	12	71

Matriz de riesgo potencial

Tipo de activo	Código de amenaza	Amenazas	Impacto	Nivel de probabilidad	Riesgo Potencial	Zona de riesgo
Hardware	A1	Computadoras sin contraseñas	3	1	3	H
	A2	Protección contra USB	4	2	8	H
	A3	Desastres naturales	2	2	4	W
	A4	Fuego	4	3	12	W
	A5	Daños por agua o inundaciones	4	1	4	W
	A6	Exposición de contraseñas	5	1	5	D
	A7	Mal uso del software	5	2	10	D
	A8	Sabotaje de los cables de red	5	3	15	D
	A9	Fallas en la infraestructura	3	3	9	K
	A10	Sabotaje de los routers	5	2	10	K
Software	A1	Computadoras sin contraseñas	3	1	3	H
	A2	Protección contra USB	4	3	12	H
	A3	Desastres naturales	2	3	6	W
	A4	Fuego	4	1	4	W
	A5	Daños por agua o inundaciones	4	3	12	W
	A6	Exposición de contraseñas	5	2	10	D
	A7	Mal uso del software	5	2	10	D
	A8	Sabotaje de los cables de red	5	3	15	D
	A9	Fallas en la infraestructura	3	3	9	K
	A10	Sabotaje de los routers	5	3	15	K
Informacion	A1	Computadoras sin contraseñas	3	1	3	H
	A2	Protección contra USB	4	1	4	H
	A3	Desastres naturales	2	3	6	W
	A4	Fuego	4	1	4	W
	A5	Daños por agua o inundaciones	4	2	8	W
	A6	Exposición de contraseñas	5	2	10	D
	A7	Mal uso del software	5	2	10	D
	A8	Sabotaje de los cables de red	5	3	15	D
	A9	Fallas en la infraestructura	3	3	9	K
	A10	Sabotaje de los routers	5	3	15	K

Salvaguardas o controles existentes

Nivel	Descripción de la efectividad del control
1	El control tiene probabilidades de fallar o no existe un control contra esta amenaza.
2	El control es eficaz de forma parcial, podría funcionar en caso de amenazas.
3	El control es óptimo por lo que garantiza el funcionamiento en caso de amenaza.

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

Desastres naturales

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Control implementado	Efectividad del control	Comentarios
Hardware, software, información	Zona propensa a inundaciones	Los laboratorios que contienen equipo de cómputo no deberían de estar en zonas que son propensas a inundaciones	Minimizador	Si	3	El laboratorio se encuentra localizado en una zona fuera del alcance de las inundaciones.
	Incapacidad para absorber rayos	Sistema para rayos y polo a tierra	Minimizador	No	1	No existe un sistema contra rayos por lo que todo el laboratorio está expuesto.
	Sistema de drenaje débil	Se debe implementar protección contra inundaciones	Minimizador	Si	2	Existe un sistema de drenaje que funciona en la mayoría de los casos, pero está expuesto en caso de tormentas demasiado prolongadas.
	Ausencia de backup en un lugar diferente o lugar alterno.	Tener un sitio que almacene la información de forma alterna a la principal.	Recuperación	No	1	No existe un backup de información.
	Ausencia de control de humedad	Sistema de monitoreo para humedad	Minimizador	No	1	No existe un sistema que permita monitorizar la humedad dentro del laboratorio.

Errores humanos

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Control implementado	Efectividad del control	Comentarios
Hardware, información	Insuficiente definición de roles y responsabilidades de seguridad de la información	Las funciones y responsabilidades de los empleados y terceros deben ser definidas y documentadas por las medidas de seguridad.	Administración	Si	2	Muchos de los empleados y terceros hacen caso omiso sobre las medidas de seguridad que se deben de tener por seguridad.
	Perdida de información	Los discos duros que presenten advertencias de "reparación automática están expuestos a fallar dentro de poco tiempo.	Recuperación	Si	2	Hay partes del personal que está capacitado para el uso del equipo de cómputo, pero a su vez hay partes que no están capacitados.

Errores humanos

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Control implementado	Efectividad del control	Comentarios
Hardware, información	Insuficiente definición de de seguridad de la información	Las funciones y responsabilidades de los empleados y terceros roles y deben ser definidas y responsabilidades documentadas por las medidas de de seguridad de seguridad.	Administración	Si	2	Muchos de los empleados y terceros hacen caso omiso sobre las medidas de seguridad que se deben de tener por seguridad.
	Perdida de información	Los discos duros que presenten advertencias de "reparación automática están expuestos a fallar dentro de poco tiempo.	Recuperación	Si	2	Hay partes del personal que está capacitado para el uso del equipo de cómputo, pero a su vez hay partes que no están capacitados.

Amenazas legales

Activos afectados	Vulnerabilidad	Controles control	Tipo de	Control implementado	Efectividad del control	Comentarios
Software, información	Protección insuficiente de los registros de la institución	Se deberían de proteger los registros importantes de la institución para asegurar el cumplimiento de las restricciones legales sobre el uso del material protegido por derechos de propiedad y sobre el uso de productos de software propietario.	Administración	No	1	La información de la institución esta guardada de forma optima por lo que está expuesta de muchas maneras.
	Insuficiente protección de los registros de la institución	La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación legal. Se debería de implementar una política de protección de datos.	Administración	No	1	No existe un sistema contra rayos por lo que todo el laboratorio está expuesto.
	Reglamento de los controles criptográficos	Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.	Prevención	No	1	No existe ninguna implementación sobre esto.

Fallas en la red

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Control implementado	Efectividad del control	Comentarios
Hardware, Software, información	Ausencia de procesos de autorización	Debería establecerse un proceso de autorización cuando se va a realizar una instalación de un nuevo recurso.	Administración	Si	3	Existe un proceso de autorización por parte de la administración en caso de necesitar una nueva instalación.
	Sistemas sobrecargados de la capacidad inadecuada	Se monitoriza y ajusta el uso de recurso, con el propósito de mejorar las capacidades en un futuro de ser necesario.	Administración / Monitorización	Si	3	Se tiene implementado un control formal para monitorear el uso de los recursos para mejorar la infraestructura de ser necesario.
	Reglamento de los controles criptográficos	Los controles criptográficos deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones.	Prevención	No	1	No existe ninguna implementación sobre esto.
Software	Instalaciones y controles de servicio	Se debe asegurar que todas las configuraciones tengan una defectuosa instalación optima.	Prevención	Si	3	Los servicios que se ofrecen en el laboratorio operan con total normalidad en el día a día en caso de presentar un fallo se aborda de inmediato.
Hardware	Baja calidad en entidad para información o	Establecer requerimientos de la los equipos de nuevos sistemas de hardware para mejorar los ya existentes, que especifiquen los controles de seguridad	Administración	Si	3	Todo producto de baja calidad o que no ofrezca un rendimiento optimo es retirado con la finalidad de que los usuarios tengan la mejor experiencia
	Uso de periféricos y repuestos incompatibles	requeridos.		Si	3	Todos los equipos utilizados son compatibles entre sí.
	Ausencia de equipos adecuados para la protección de fallas de energía	Se deberían de proteger los equipos contra fallos de energía u otro tipo de falla eléctrica	Prevención	Parcial	2	Se cuenta con equipo de protección para el equipo en caso de algún tipo de fallo en la energía, pero solo para los equipos de principal relevancia.
	Ausencia de control de humedad	Sistema de monitoreo para humedad	Minimizador	No	1	No existe un sistema que permita monitorizar la humedad dentro del laboratorio.
	Ausencia de mantenimiento periódico	Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.	Prevención	Si	3	Se hace un mantenimiento al equipo de cómputo cada 4 meses debido a su alto uso.

Robos

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Control implementado	Efectividad del control	Comentarios
Hardware, Software, información	Falta de protección física	Seguridad física debe ser diseñada y aplicada para oficinas y demás recursos.	Disuasión	Si	3	El acceso a toda área de relevancia está restringido bajo llave y solo tiene acceso una persona en específico.
		Protección física y directrices deben ser diseñadas y aplicadas para trabajar en áreas seguras.	Disuasión	No	1	No se cuentan con gulas o procedimientos para protección física y trabajos en áreas seguras.
		Los usuarios deben garantizar que un equipo no atendido tenga la protección adecuada.	Prevención	Si	3	Se cuenta con intervalos de tiempo de suspensión cortos en caso de dejar un equipo sin uso.
		Las áreas seguras deben estar protegidas apropiadamente por controles que garanticen el acceso a personal autorizado	Prevención	Si	3	En zonas donde se maneja información privada es de acceso solo para personal autoriza (3) para tener la mayor seguridad posible
	No existe una supervisión del trabajo de personal externo o de limpieza.	Establecer mecanismos de control sobre el personal externo y de aseo como: Supervisar el trabajo que están realizando en sus horas laborales.	Disuasión	Si	3	Se supervisa el trabajo de todos los empleados en horas específicas y sorpresa para garantizar la protección de la institución.
	Inadecuada e insegura reutilización o eliminación de los equipos.	El equipo, información o software no debe ser sacado fuera de la Entidad sin autorización.	Prevención	Si	3	No se permite que ningún personal que no esté capacitado toque el equipo, hay Jefe de TI es la única persona autorizada para realizar estas acciones.
	Debería haber procedimientos para la gestión de los medios informáticos removibles		Monitorización	Si	3	Se tiene personal autorizado para realizar este tipo de cambios.
	Se debe disponer en forma segura de los medios ya no se requieran, utilizando procedimientos formales.		Monitorización	Si	3	Una vez que el equipo no sea requerido pasa al inventario de la institución marcado por un código que hace capaz de identificar si esta inactivo o activo.

Mal uso de los equipos

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Control implementado	Efectividad del control	Comentarios
Software, Información	Falta de medidas de restricción contra acceso no autorizado	Se debería dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de este, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	Prevención	Si	3	Se tiene definido que los únicos autorizados para solicitar privilegios de acceso son los administrativos y el personal autorizados.
		Los sistemas sensibles pueden necesitar entornos informáticos dedicados.	Prevención	Si	3	La información esta solo para administrativos y se restringe con contraseña.
	Insuficiente capacitación a los usuarios	Todos los empleados y usuarios terceros deben recibir entrenamiento para obtener el conocimiento del correcto uso del equipo.	Concienciación	Si	3	Se impartió una capacitación al personal por cada nueva tecnología que sea implementada.
	Ausencia de controles para la instalación	Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales.	Administración	Si	3	Se tiene restricciones a los usuarios que no estén autorizados a nivel de privilegios.
	Ausencia de controles para cierre o bloqueo de sesión de usuario o del sistema.	Las sesiones se deberían desactivar tras un periodo definido de inactividad.	Prevención	Si	3	Todos los equipos luego de un periodo de tiempo específico de inactividad se bloquean para mayor seguridad.

Impacto residual

Tipo de activo	Vulnerabilidad	Eficacia del controlador	Impacto potencial	Impacto residual
Hardware	Computadoras con polvo	3	5	1.7
	Computadoras si acceso a red wifi	1	5	5.0
	La zona de alcance del router es mínima	2	5	2.5
	nivel de tinta de la impresora	2	5	2.5
Red	fallas del router	1	5	5.0
	puntos de acceso mal ingresados	1	5	5.0
	puertos del swicth inestables	2	5	2.5
Software	El sistema operativo no recomendado	2	5	2.5
	Microsoft Office no activado	2	5	2.5
	el Adobe no está instalado	2	5	2.5
Instalación	Flautas dañadas	1	5	5.0
	cableado a simple vista	2	5	2.5
	toma corrientes sin protección	3	5	1.7

Matriz de impacto residual y riesgo residual

Tipo de activo	Vulnerabilidad	Eficacia del controlador	Impacto potencial	Impacto residual	Nivel de probabilidad	Zona de riesgo residual
Hardware	Computadoras con polvo	3	5	1.7	4	H
	alcance minimo del router	2	5	2.5	2	W
	falta de hojas de papel	3	5	1.7	1	H
	niveles bajos de tinta	2	5	2.5	2	D
	Ram defectuosas	1	5	5.0	1	K
	Swicth inestable	1	5	5.0	1	k
Red	Denegación de servicio	2	5	2.5	1	D
	Problemas de acceso a HTTP	3	5	1.7	2	H
	Conflicto con direcciones IP	3	5	1.7	1	H
	Conflictos en la red	3	5	1.7	2	H
	Ataque por servidor	1	5	5	1	K
	Ataue de bloqueo de dominio	2	5	2.5	1	D
	Suplantacion de DNS	2	5	2.5	1	D
Software	Fuga de información	1	5	5	3	K
	Firmware desactualizado	3	5	1.7	3	W
	Problemas de Configuración	1	5	5	2	K
	Falla de Access Point	3	5	1.7	4	W
	Drivers ausentes	3	5	1.7	5	H
	Infección de malware	1	5	5	3	K
Instalación	Sobrecarga de energia	2	5	2.5	2	D
	Problemas de alta temperatura	1	5	5	4	K
	variacion de voltaje	3	5	1.7	2	W
	toma corrientes sin protección	3	5	1.7	1	H
	Cables enrredados	3	5	1.7	3	H
	Flautas Inestables	2	5	2.5	2	D

Tabla de riesgos y recomendaciones para su solución

Riesgos	Recomendaciones
Conflicto con las direcciones ip	Monitorización continua de sistema de red
Errores de hardware o software	Mantenimiento riguroso de ambos
Robo de información	Mantener un respaldo de la información importante
Incendios	Servicios de Consultoría para la elaboración de un plan de contingencias
Terremotos	Servicios de Consultoría para la elaboración de un plan de contingencias
Caída del router por sobrecarga	Configuración de nuevos equipos de mayor capacidad.
Administración sin atender	Monitorización continua de sistema de red
Inundaciones	Servicios de Consultoría para la elaboración de un plan de contingencias
Problemas de alta temperatura	Revisión de Sistemas de Enfriamiento por los A/C de precisión
Problemas por contraseñas débiles	Utilización contraseñas seguras
Delegar tareas sin poner limites	Configuración de Parámetros de grupos para usuarios en el sistema de gestión de red
Problemas de configuración	Uso de plantillas de configuración
Virus	Antivirus
Perdida de información	Mantener información en la nube

Vulnerabilidad	Eficacia del controlador	Impacto potencial	Impacto residual	Nivel de probabilidad	Zona de riesgo residual
Ram defectuosas	1	5	5	1	K
Swicth inestable	1	5	5	1	k
Ataque por servidor	1	5	5	1	K
Fuga de información	1	5	5	3	K
Problemas de Configuración	1	5	5	2	K
Infección de malware	1	5	5	3	K
Problemas de alta temperatura	1	5	5	4	K

Tipo de activo	Vulnerabilidad	Eficacia del controlador	Impacto potencial	Impacto residual
Hardware	Computadoras con polvo	3	5	1.7
	Computadoras si acceso a red wifi	3	5	1.7
	La zona de alcance del router es minima	2	5	2.5
	nivel de tanta de la impresora	2	5	2.5
Red	fallas del router	1	5	5.0
	puntos de acceso mal ingresados	1	5	5.0
	puertos del swicth inestables	2	5	2.5
Software	El sistema operativo no recomendado	2	5	2.5
	Microsoft Office no activado	2	5	2.5
	el Adobe no está instalado	2	5	2.5
Intalación	Flautas dañadas	1	5	5.0
	cableado a simple vista	2	5	2.5
	toma corrientes sin protección	3	5	1.7

Tipo de activo	Vulnerabilidad	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Zona de riesgo residual	Controles
Hardware	Ram defectuosas	1	5	5	1	K	Reducir: Incluir en los presupuestos la compra de memorias RAM de respuesta en caso de algún tipo de fallo. Mitigar: Aplicar un cambio inmediato de la memoria defectuosa. Evitar: Hacer test de estres para conocer que memorias estan por sufrir un fallo, para aplicar un mantenimiento preventivo.
	Swicth inestable	1	5	5	1	k	Reducir: Incluir en los presupuestos la compra de switch de respuesta en caso de algún tipo de fallo. Mitigar: Aplicar un cambio inmediato del switch para verificar que está causando problemas.
Red	Ataque por servidor	5	5	5	1	K	No aplica
Software	Fuga de información	1	5	5	3	K	Reducir: Mantener toda la información privada bajo alta seguridad y el acceso restringido al personal administrativo. Mitigar: Solo una persona capacitada puede llevar el control de la seguridad de la información. Evitar: Evaluar a diario el sistema de seguridad integral.
	Problemas de Configuración	1	5	5	2	K	Reducir: Revisar periódicamente la configuración de todo hardware y software implementado. Mitigar: Desactivar cualquier tipo de hardware o software que implique un fallo. Evitar: Verificar que las configuraciones de todo el hardware y software este correcto antes de su implementación.
	Infección de malware	1	5	5	3	K	Reducir: Realizar análisis periodicos para verificar la integridad del SO. Mitigar: Desconectar de la red cualquier equipo en el que se detecte una infección para minimizar su propagación. Evitar: Implementar un antivirus de alta seguridad.
Instalación	Problemas de alta temperatura	1	5	5	4	K	Reducir: Incluir en el presupuesto unos coolers que garanticen la refrigeración del equipo al igual que verificar un buen sistema de refrigeración de la zona. Mitigar: Sacar del uso el equipo que presente problemas de temperaturas para su revisión. Evitar: Realizar mantenimientos periódicos para garantizar una buena refrigeración de los equipos.

Tabla de riesgos y amenazas

Riesgos

Conflicto con las direcciones ip
Errores de hardware o software
Robo de información
Incendios
Terremotos
Caída del router por sobrecarga
Administración sin atender
Inundaciones
Problemas de alta temperatura
Problemas por contraseñas débiles
Delegar tareas sin poner limites
Problemas de configuración
Virus
Perdida de información

Tabla de valoración de riegos y amenazas

Valoración por colores		
Nivel de riego	Categorías	Representación
=6	MUY ALTO	
=5	ALTO	
=4	MODERADO	
=3	BAJO	
=1,2	ACEPTABLE	

Valoración del impacto y probabilidad

Las valoraciones de las probabilidades en los riesgos se clasifican en tres rangos:

• Bajo: La amenaza se materializa a lo sumo una vez cada año

• Medio: La amenaza se materializa a lo sumo una vez cada mes

• Alto: La amenaza se materializa a lo sumo una vez cada semana

Para el caso del impacto que tienen los riesgos también se clasifican en tres rangos:

• Bajo: El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización

• Moderado: El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.

• Alto: El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Categorías y riesgos		Probabilidad			Impacto		
		(1)	(2)	(3)	(1)	(2)	(3)
A1	Conflicto con las direcciones ip	**X**				**X**	
A2	Errores de hardware o software		**X**				**X**
A3	Robo de información	**X**					**X**
A4	Incendios	**X**					**X**
A5	Terremotos	**X**					**X**
A6	Caída del router por sobrecarga		**X**			**X**	
A7	Administración sin atender			**X**			**X**
A8	Inundaciones	**X**					**X**
A9	Problemas de alta temperatura		**X**		**X**		
A10	Problemas por contraseñas débiles		**X**			**X**	
A11	Delegar tareas sin poner limites			**X**			**X**
A12	Problemas de configuración		**X**		**X**		
A13	Virus			**X**		**X**	
A14	Perdida de información		**X**				**X**

Costos estimados en la implantación de las medidas de seguridad en el Sistema Informático.

Tipo de recurso	Descripción del recurso	Valor mensual	Valor anual
Recurso Humano	Técnico en sistemas	L. 13,000.00	L. 156,000.00
	Ing. En sistemas.	L. 25,000.00	L. 300,000.00
Recurso Tecnológico	Hardware: Computadoras, impresora, switches, Routers, cableado eléctrico	L. 20,000.00	L. 240,000.00
	Software: Licencias de office, aplicaciones específicas para los estudiantes, realizar copia de seguridad de toda la información relevante, aplicaciones actualizadas	L. 2,500.00	L. 30,000.00
	Comunicaciones: Firewall, antivirus, tipo de conexión a internet.	L. 1,000.00	L. 12,000.00
			L. 738,000.00

Conclusiones

- La organización en la que se a estado trabajando debe ver con máxima importancia los riesgos mas grandes que tienen para atacarlos de raíz, cortar pequeños problemas que son fáciles de atender.

- Son muchas las medidas rescatables que podemos observar en el informe que desde un mínimo tiempo se pueden resolver contratando al personal adecuado para atacar el punto indicado.

- Influye mucho lo visto en clases en el caso de ser un pequeño laboratorio se pueden hacer un problema de manera grande que ataque la integridad y seguridad de un colegio.

Recomendaciones

- ✓ Tomar en cuenta las normas ISO para tener una guía de la seguridad con la que podrían empezar aplicar dentro del laboratorio de cómputo.

- ✓ Tomar en cuenta que siempre estamos bajo amenaza por más insignificante que sea la información es algo muy delicado hoy en día y la seguridad debe de ser algo muy importante a tener en cuenta que debe de estar protegida.

- ✓ Las siguientes medidas deben de ser una prioridad para dicha empresa no dejar que avance a la continuidad ya que esto pone en riesgo su integridad.

Bibliografía

- https://ceupe.com.ar/blog/tipos-de-seguridad-informatica/