UNICAH

2022

Seguridad y gestion de riesgo

3 de Abril de 2022

GESTION DE RIESGO
INSTITUTO EDUCATIVO MODELO

Analisis de evaluación de riesgo con MAGERIT.

Catedratica:

Ing. Patricia Medina

Integrantes:

Isaak Antúnez – 1503200001376

Gerson Martinez – 1501199901715

Diego Mendoza - 0801200010492

Indice.

Introducción

Este informe se desarrollará un profundo análisis de riesgo que serán aplicados en el laboratorio informático del colegio Modelo el cual está orientado a aplicarse con una metodología MAGERIT que tendrá como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Lo primordial en nuestra aplicación de la metodología magerit es evaluar los riesgos que hay hasta el momento y cuantificar que tan desprotegido se encuentra para una evaluación de riesgos y poder tomar acciones en cómo resolverlos. Esto significa que la seguridad informática es la clave de todo el trabajo ya que se refiere a la protección de la información y así al utilizar la metodología que nos ayudará a saber cuán propensos estamos para evitarse reduciendo su impacto.

Objetivos

Objetivo General

Elaborar un análisis de riesgo completo y detallado basado en las condiciones encontradas en el centro de cómputo del Instituto Educativo Modelo, brindar las recomendaciones pertinentes para mejorar la seguridad informática siguiendo los pasos de la metodología MAGERIT.

Objetivos Específicos

* Instalar/Actualizar antivirus

* Realizar limpieza de computadoras

* Elaborar informe sobre los riesgos encontrados.

* Brindar recomendaciones para mitigar las amenazas encontradas.

Planteamiento del Problema.

La inseguridad informática es un tema que concierne al instituto Educativo Modelo por lo que necesitan ayuda para verificar el estado actual de su sistema dentro del laboratorio de computación. Por lo tanto, con esta tarea en mente, tenemos que realizar un análisis a profundidad de los sistemas de seguridad (si los posee) y verificar las posibles amenazas o vulnerabilidades que pueda tener este. Para la realización de nuestro análisis, se evaluaran los siguientes puntos:

- ¿Se poseen protocolos de seguridad?
- ¿Cuál es el estado de seguridad física del lugar en cuestión?
- ¿Para qué se utilizan las computadoras y que se hace para mantenerlas seguras?
- ¿Se les provee acceso a los estudiantes para realizar cambios dentro de los equipos?
- ¿Qué tanto se utiliza el lugar?

Estas interrogantes nos ayudarán a saber con lo que estamos trabajando y facilitaran el trabajo de nuestro equipo para detectar posibles riesgos y/o amenazas, e idear formas de crear un entorno seguro para el uso del laboratorio.

Justificación.

Con la aplicación de la metodología MAGERIT al instituto Educativo Modelo, buscamos mejorar o establecer un sistema de seguridad informática (SGSI) competente y relacionado a las tareas que se realizan dentro del laboratorio informático. Estos sistemas de seguridad son un apartado de suma importancia dentro de cualquier centro de cómputo para responder ante posibles robos, accidentes y ataques físicos y lógicos que pueden poner en riesgo la salud de las instalaciones.

Usualmente las instituciones le prestan muy poca atención a esta parte, en el momento en el que se plantea la creación o implementación de un laboratorio, contratan personal con conocimientos básicos para la instalación y mantenimiento de este, lo cual no es la manera más adecuada de realizar esta tarea. Con estas cosas en mente, es muy importante concientizar a las personas responsables del instituto los riesgos, vulnerabilidades y amenazas a las que están expuestos, la importancia de gestionarlos y brindar métodos para minimizar estos problemas y mantenerlos bajo control.

Marco Conceptual

- **Seguridad Informática.**

  Seguridad informática se basa en la protección integra y la privacidad de la información que esté almacenada en un sistema informático u en la nube como lo son miles de sistemas web. Tiene como objetivo limitar y prevenir la manipulación de datos y sistemas por terceros no autorizados. Esto viene siendo que los sistemas y las personas dentro de la empresa y datos están protegidos contra amenazas y daños no solo se basa en la información en ella sino también los equipos físicos, servicios en la nube el ambiente en donde esté el equipo de mayor vulnerabilidad.

- **SGSI.**

  El Sistema de Seguridad de la Información (SGSI) es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información corporativa en las empresas. El término se denomina en inglés “Information Security Management System” (ISMS).

  Un SGSI es, por tanto, el conjunto de prácticas orientadas a garantizar la seguridad, la integridad y la confidencialidad de estos datos debe implementarse de manera estratégica para que los resultados sean acordes con los objetivos propuestos. Si sólo se aplicara parcialmente, no habría garantías para el resto de información proveniente de aquellas secciones o áreas que han quedado sin cobertura.

- **ISO.**

  Las normas ISO son un conjunto de estándares con reconocimiento internacional que fueron creados con el objetivo de ayudar a las empresas a establecer unos niveles de homogeneidad en relación con la gestión, prestación de servicios y desarrollo de productos en la industria.

  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.

- **Amenazas.**

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

- **Riesgos.**

Todo cuanto pueda ser definido como una circunstancia que haga disminuir nuestro beneficio puede ser un riesgo potencial derivado de varios factores como: la falta de control sobre los dispositivos, la falta de control sobre el acceso a la información y su protección ante ajenos, así como cuantos factores puedan atentar contra la estabilidad de la plataforma corporativa de sistemas de información.

Por tanto, la adecuada combinación de medidas de control y restricción de acceso, capaces de supervisar el acceso a la información, la infraestructura hardware y software y las comunicaciones de manera integral en la compañía, será la respuesta que signifique la clave del éxito y minimice las amenazas existentes.

- **Vulnerabilidades.**

  Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

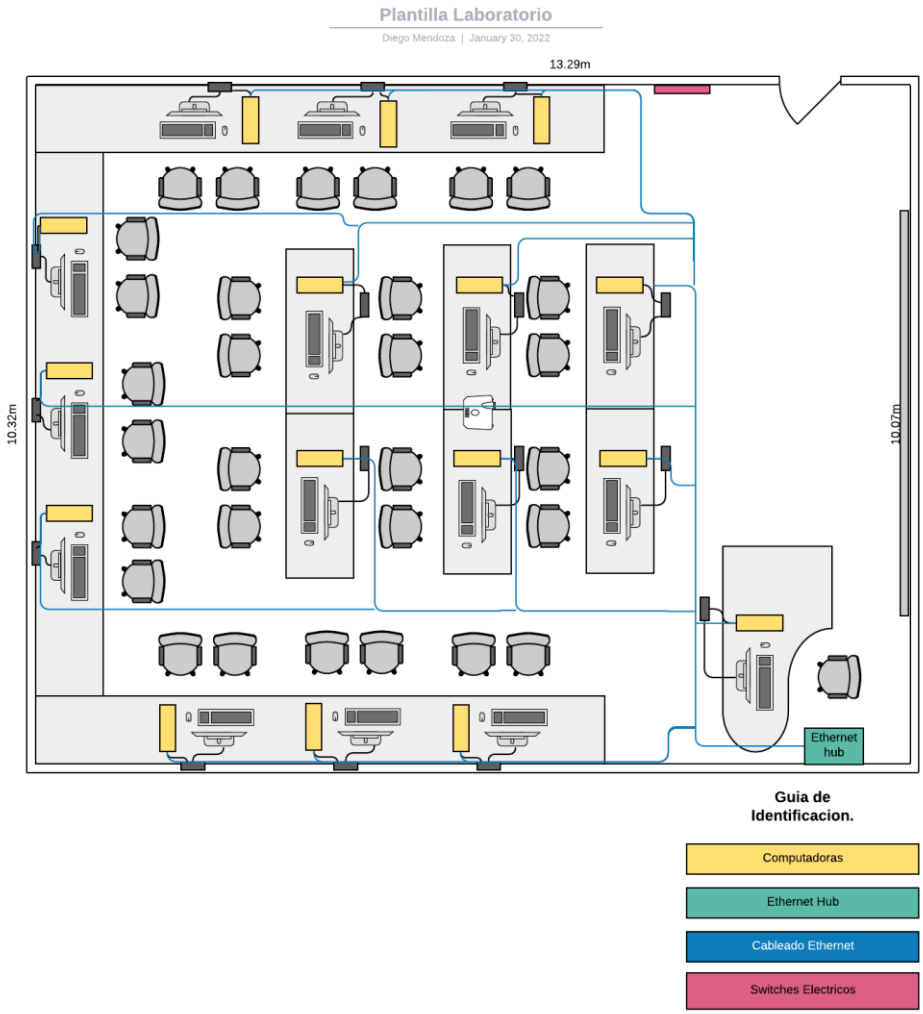
- **Metodología MAGERIT.**

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.

Tiene como objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Diagrama de Sistema Informático.



Planeación de la seguridad informática en la organización

En esta etapa se debe hacer una profunda evaluación del sistema que hay en la institución, así como planear cada método a realizar, como también conocer cada equipo susceptible a daños, pérdidas que comprometan la seguridad e integridad del instituto.

Al tener una evaluación de daños, veremos las vulnerabilidades para tener en detalle lo que se tomará como medida de seguridad en el sistema, al concluir esta parte habrá un proceso de revisión por parte de todo el equipo de seguridad para constar que no dejemos ningún detalle sin evaluar. Para ello se hará un análisis usando la metodología Magerit para aplicarlo al laboratorio del instituto y poder llegar a encontrar los posibles fallos dentro del sistema, con el fin de darle a conocer a los encargados de mantenimiento del laboratorio y sean ellos quienes decidan si aplicar o no las medidas propuestas.

Objetivos del análisis y evaluación de riesgos.

¿Qué es lo que se quiere lograr realizando el análisis y evaluación de riesgos?

- Entender el estado actual en el que se encuentra el sistema en términos de seguridad.
- Evaluar la susceptibilidad del sistema a posibles amenazas externas e internas.
- Analizar los protocolos de seguridad realizados por el personal del laboratorio, si es que los poseen.
- Plantear la idea de mejora del SGSI, dependiendo del resultado del análisis correspondiente y tomando en cuenta las posibilidades del instituto para realizar las mejoras.
- Planificar un estimado de tiempo y recursos necesarios para la revisión y proposición de actividades contra los problemas encontrados.
- Concientizar a las partes encargadas de la importancia de la seguridad informática.
- Exponer al equipo a cargo de las salvaguardas y posibles métodos utilizables para lograr una seguridad informática exitosa.

Identificacion de los activos.

Activos Hardware

ID	Clave	Nombre	Tipo	Cantidad
A_1	ETH_H	Ethernet	Hardware	1
A_2	PRY_W	Proyector Wireless	Hardware	1
A_3	PC_S	Computadora Servidor	Hardware	1
A_4 A_19	PC_1 – PC_15	Computadoras Cliente	Hardware	15

Activos Software

ID	Clave	Nombre	Tipo	Cantidad
A_20	OFF_L	Licencia Office	Software	1
A_21	VS_L	Licencia de Visual Studio	Software	1

Activos de Informacion.

La empresa no cuenta con informacion crucial o confidencial dentro del laboratorio.

Descripción de los activos o recursos.

Activo	Descripción
Computadoras.	Instrumento que los estudiantes, así como el maestro, utilizan para aprendizaje educativo a través de herramientas de software ofimático y de programación.
Ethernet HUB o switch.	Interconectar los ordenadores creando una red LAN, manteniendo comunicación entre todos los ordenadores y haciendo que uno de ellos sea quien se encargue de la administración de la red.
Sillas y escritorios.	Utensilios para sostener los componentes computacionales y que los estudiantes/maestros puedan usar las computadoras adecuada y cómodamente.
Perifericos	Utencilios dedicados a la manipulacion y control de una computadora como por ejemplo, teclado, mouse, etc.
Recursos	**Descripcion**
Recursos Humanos	Se refiere al personal encargado del funcionamiento del laboratorio y los clientes, siendo estos los alumnos que utilizan las computadoras.
Recursos Tecnologicos	Todas las herramientas de aspecto tecnico que posee el laboratorio.

Valoracion de los Activos.

Se valoraran los activos del laboratorio en base a el daño que ocasiona en el avance dentro de los procesos cruciales del mismo, siguiendo esta rubrica:

Se puede considerar daño muy grave [10] a:

- Daños que puedan causar un incidente serio de seguridad y dificulte la investigacion de los mismos.
- Daños que pueden causar serias perdidas economicas.
- Daños que impidan seriamente la continuidad de los procesos mas importantes del laboratorio o impidan el uso completo de este.

Se puede considerer daño grave [7-9] a:

- Daños que causen la interrupcion de actividades realizadas en el laboratorio.
- Daños que afecten la seguridad fisica de los equipos utilizables por los estudiantes y el maestro.

Se puede considerar daño importante [4-6] a:

- Daños que afecten la eficacia de los equipos del laboratorio.
- Daños que involucren la utilizacion del laboratorio por parte de terceros y cause impedimentos en el uso del mismo.

Se puede considerar daño menor [1-3] a:

- Daños que afecten a un individuo que utilice alguno de los equipos.

Se puede considerar daño despreciable [0] a:

- Daños que no afectan a las actividades propias del laboratorio.

Graficamente expresado de la siguiente manera:

Valoracion de los Activos.			
Valor			**Descripcion**
10	Muy Grave	MG	Daño muy grave al laboratorio.
7-9	Grave	G	Daño grave al laboratorio.
4-6	Importante	I	Daño importante al laboratorio.
1-3	Menor	M	Daño menor al laboratorio.
0	Despreciable	D	Daño despreciable al laboratorio.

Clasificacion de Activos.

Principio de Seguridad	Clasificacion	Definicion
Confidencialidad	**Publico**	Esta informacion es considerada de carácter publico y puede ser divulgada a cualquier persona o entidad interna o externa del Instituto, sin ninguna restriccion.
	Interno	Esta informacion es utilizada por el encargado del laboratorio para la ejecucion de sus labores, no puede ser conocida por terceros sin autorizacion del responsable del activo de informacion o directivas de la institucion.
	Confidencial	Esta informacion se considera altamente sensible y es utilizada solo por un grupo limitado de funcionarios o areas para la ejecucion de labores y no puede ser conocida por otros funcionarios de la institucion o terceros externos.
Integridad	**No sensitiva**	La perdida o modificacion no autorizada podria causar un daño leve o nulo para la Institucion.
	Sensitiva	La perdida o modificacion no autorizada, podria causar un daño que genere perjuicios importantes que afectan a la Institucion, pero que puede ser absorbido o asumido por este.
	Altamente sensitiva	La perdida o modificaion no autorizada, podria causar un daño grave que genere perjuicios que afectan significativamente a la Institucion y que dificilmente podrian ser asumidos por este.
Disponibilidad	**No critico**	Puede no estar disponible por un periodo de tiempo extendido, sin afectar la operación de la Institucion Educativa.
	Importante	La no disponibilidad afectaria operaciones, y servicios del encargado del laboratorio de la Institucion.
	Critico	La no disponibilidad afectaria significativamente las operaciones, servicios del laboratorio y acceso a la informacion.

Activos de tipo Software

Informacion del Activo					Informacion proceso	Clasificacion de activos de informacion			
ID	**Nombre**	**Tipo**	**Propietario**	**Localizacion**	**Proceso**	**C**	**I**	**D**	**Valor Final**
A_20	Office Profesional	Ofimatica	Laboratorio	Laboratorio	Enseñanza de propiedades basicas de los programas ofimaticos	1	2	2	**5/9**
A_21	Visual Studio 2019	Programacion	Laboratorio	Laboratorio	Enseñanza de programacion basica para los estudiantes.	1	2	2	**5/9**

Activos de Hardware.

Informacion del Activo					Informacion proceso	Clasificacion de activos de informacion			
ID	**Nombre**	**Tipo**	**Sistema Operativo**	**Direccion IP**	**Proceso**	**C**	**I**	**D**	**Valor Final**
A_1	Ethernet HUB	Switch	Cisco	192.168.1.254	Crear una red lan para las computadoras.	3	3	3	**9/9**
A_2	Proyector Wireless	Proyector	Android	192.168.1.100	Mostrar contenido educativo y entretenimiento en una gran pantalla.	1	1	2	**4/9**
A_3	PC_S	Computadora	Windows 10	192.168.1.101	Controlar las computadoras cliente y gestionar la red.	2	2	3	**7/9**
A_4 A_19	PC_1 – PC_15	Computadora	Windows 7	192.168.1.102 192.168.1.17	Brindar los recursos necesarios para el aprendizaje de los clientes	1	1	3	**5/9**

Identificacion de las Amenazas.

ID	Descripcion
AM_1	Averias en el equipo por fallas en el fluido electrico.
AM_2	Falta de cumplimiento de la regla que prohibe el ingreso de alimentos y bebidas al laboratorio.
AM_3	Uso de pendrives infectados.
AM_4	Falta de mantenimiento en los equipos.
AM_5	Robo de perifericos o componentes de uso escencial para las computadoras del laboratorio.
AM_6	Destruccion de la informacion publica o perteneciente a estudiantes.
AM_7	Plagas en el laboratorio.
AM_8	Acceso a sitios no relacionados a las actividades educativas.
AM_9	Incendio.
AM_10	Desastres naturales.
AM_11	Daños al aire acondicionado.
AM_12	Descargar de archivos maliciosos o dañinos.
AM_13	Colpaso de la estructura de las instalaciones.
AM_14	Problemas por Contraseñas débiles o por defecto.
AM_15	Softwares desactualizados.
AM_16	Conflicto con direcciones IP.
AM_18	Modificacion o alteracion de archivos.
AM_19	Mal uso de software.

Probabilidad

Estimacion de la probabilidad		
Nivel	**Valor**	**Descripcion**
1	**Improbable**	La probabilidad de que ocurra es demasiado baja, casi nula.
2	**Posible**	La probabilidad de que ocurra es baja, aunque puede presentarse.
3	**Ocasional**	La amenaza puede materializarse en cualquier momento.
4	**Moderado**	La materializacion de la amenaza es alta, de hecho, puede presentarse.
5	**Constante**	Es muy alta la probabilidad de que se presente esta amenaza.

Amenazas clasificadas por su tipo y su nivel de probabilidad.

Clasificacion por nivel de probabilidad		
ID	**Nombre**	**NP**
AM_1	Averias en el equipo por fallas en el fluido electrico.	3
AM_2	Falta de cumplimiento de la regla que prohibe el ingreso de alimentos y bebidas al laboratorio.	4
AM_3	Uso de pendrives infectados.	2
AM_4	Falta de mantenimiento en los equipos.	3
AM_5	Robo de perifericos o componentes de uso escencial para las computadoras del laboratorio.	1
AM_6	Destruccion de la informacion publica o perteneciente a estudiantes.	2
AM_7	Plagas en el laboratorio.	1
AM_8	Acceso a sitios no relacionados a las actividades educativas.	3
AM_9	Incendio.	2
AM_10	Desastres naturales.	1
AM_11	Daños al aire acondicionado.	3
AM_12	Descargar de archivos maliciosos o dañinos.	3
AM_13	Colpaso de la estructura de las instalaciones.	1
AM_14	Problemas por Contraseñas débiles o por defecto.	2
AM_15	Softwares desactualizados.	3
AM_16	Conflicto con direcciones IP.	2
AM_18	Modificacion o alteracion de archivos.	4
AM_19	Mal uso de software.	5

Matriz de impacto potencial.

Tipo de Activo	Codigo de Amenaza	Amenaza	Impacto
Hardware	AM_1	Averias en el equipo por fallas en el fluido electrico.	3
	AM_2	Falta de cumplimiento de la regla que prohibre el ingreso de alimentos y bebidas al laboratorio.	3
	AM_4	Falta de mantenimiento en los equipos.	4
	AM_5	Robo de perifericos o componentes de uso escencial para las computadoras del laboratorio.	3
	AM_7	Plagas en el laboratorio.	2
	AM_9	Incendios	5
	AM_10	Desastres naturales	5
	AM_11	Daños al aire acondicionado.	3
	AM_13	Colapso de la estructura de las instalaciones.	5
Software	AM_1	Averias en el equipo por fallas en el fluido electrico.	3
	AM_4	Falta de mantenimiento en los equipos.	4
	AM_10	Desastres naturales	5
	AM_19	Mal uso de software.	3
	AM_3	Uso de pendrives infectados.	3
	AM_15	Software desactualizados.	4
	AM_16	Conflictos con direcciones IP.	5
	AM_12	Descargas de archivos maliciosos o dañinos.	2
	AM_8	Acceso a sitios web maliciosos.	2
Informacion	AM_6	Destruccion de la informacion publica o perteneciente a estudiantes.	2
	AM_18	Modificacion o alteracion de archivos.	2
	AM_3	Uso de pendrives infectados.	3
	AM_14	Problemas por contraseñas debiles o por defecto.	3

Zona de Riesgo

Probabilidad	Impacto				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrofico(5)
1	B(1)	B(2)	B(4)	M(5)	M(7)
2	B(2)	B(3)	M(5)	M(6)	A(11)
3	B(3)	M(5)	M(7)	A(9)	A(12)
4	B(4)	M(6)	M(8)	A(11)	A(13)
5	M(6)	M(7)	A(10)	A(12)	A(14)
	B: Zona de riesgo baja: Asumir el riesgo. (1-4)				
	M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo. (5-8)				
	A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir. (9-14)				

Zona de riesgo	Hardware	Software	Informacion	Total General
Zona B	2	2	2	6
Desastres Naturales	1	0	0	1
Plagas en el laboratorio	1	0	0	1
Mal uso de software	0	1	0	1
Acceso a sitios web maliciosos	0	1	0	1
Destruccion de la informacion publica o perteneciente a estudiantes.	0	0	1	1
Modificacion o alteracion de archivos.	0	0	1	1
Zona M	5	5	2	12
Desastres Naturales	0	1	0	1
Averias en los equipos por fallas en el fluido electrico	1	1	0	2
Falta de cumplimiento de la regla que prohibe el ingreso de alimentos y bebidas al laboratorio.	1	0	0	1
Robo de perifericos o componentes de uso escencial para las computadoras del laboratorio.	1	0	0	1
Daños al aire acondicionado	1	0	0	1
Colapso de la estructura de las instalaciones.	1	0	0	1
Uso de pendrives infectados.	0	1	1	2
Conflictos con direcciones IP	0	1	0	1
Contraseñas debiles o por defecto.	0	0	1	1
Descargas de archivos maliciosos o dañinos	0	1	0	1
Zona A	2	2	0	4
Falta de mantenimiento en los equipos.	1	1	0	2
Incendio	1	0	0	1
Software desactualizados	0	1	0	1
Total	9	9	4	22

Riesgo Potencial

Tipo de activo	Codigo de Amenaza	Amenaza	Impacto	Nivel de probabilidad	Riesgo Potencial	Zona de Riesgo
Hardware	AM_1	Averias en el equipo por fallas en el fluido electrico.	3	3	7	M
	AM_2	Falta de cumplimiento de la regla que prohibre el ingreso de alimentos y bebidas al laboratorio.	3	4	8	M
	AM_4	Falta de mantenimiento en los equipos.	4	3	9	A
	AM_5	Robo de perifericos o componentes de uso escencial para las computadoras del laboratorio.	3	1	5	M
	AM_7	Plagas en el laboratorio.	2	1	2	B
	AM_9	Incendios	5	2	11	A
	AM_10	Desastres naturales	5	1	7	B
	AM_11	Daños al aire acondicionado.	3	3	7	M
	AM_13	Colapso de la estructura de las instalaciones.	5	1	7	M
Software	AM_1	Averias en el equipo por fallas en el fluido electrico.	3	3	7	M
	AM_4	Falta de mantenimiento en los equipos.	4	3	9	A
	AM_10	Desastres naturales	5	1	11	A
	AM_19	Mal uso de software.	3	5	4	B
	AM_3	Uso de pendrives infectados.	3	2	5	M
	AM_15	Software desactualizados.	4	3	9	A
	AM_16	Conflictos con direcciones IP.	5	2	11	A
	AM_12	Descargas de archivos maliciosos o dañinos.	2	3	5	M
	AM_8	Acceso a sitios web maliciosos.	2	3	5	M

Tipo de activo	Codigo de Amenaza	Amenaza	Impacto	Nivel de probabilidad	Riesgo Potencial	Zona de Riesgo
Informacion	AM_6	Destruccion de la informacion publica o perteneciente a estudiantes.	2	2	3	B
	AM_18	Modificacion o alteracion de archivos.	2	4	6	M
	AM_3	Uso de pendrives infectados.	3	2	5	M
	AM_14	Problemas por contraseñas debiles o por defecto.	3	2	5	M

Salvaguardas o Controles existentes.

Salvaguardas	
ID	**Descripcion**
SG_1	Adicion de un sistema anti incendios.
SG_2	Antivirus de windows actualizado y funcional en todo momento.
SG_3	Protocolo de mantenimiento de equipos cada semana.
SG_4	Camaras dentro del laboratorio.
SG_5	Monitorizacion de las paginas y bloqueo de paginas que pueden ser distraccion para los estudiantes.
SG_6	Renovacion de las instalaciones y fortificacion de la estructura de la misma.
SG_7	Mantenimiento mensual del aire acondicionado.
SG_8	Comprobacion de actualizaciones diarias, y automaticas para las computadoras.
SG_9	Denegar los permisos para acciones que puedan perjudicar a otros alumnos o los equipos.
SG_10	El maestro imparte las reglas y condiciones de uso de las computadoras, igualmente los cuidados a tomar en cuenta.
SG_11	Fumigaciones cada 3 meses y limpieza diaria del laboratorio.
SG_12	Adicion de un extintor en el laboratorio.
SG_13	UPS que ayuden a la alimentacion de energia electrica a los equipos, y los protejan de anomalias en la misma.
SG_14	Establecimiento estricto de las normas del laboratorio, y revisiones por alumno para evitar el ingreso de comestibles y bebidas.

Controles

Tipo de activo	Codigo de amenaza	Vulnerabilidad	Controles	Tipo de control	¿Control implementado?	Eficacia del control
Hardware	AM_1	Falta de protectores de voltaje	Se necesita la instalacion de dispositivos para la proteccion de los dispositivos.	Prevencion	Si	3
	AM_2	Esquemas no tan rigurosos para las reglas.	Revisiones antes del ingreso al laboratorio.	Prevencion	No	2
	AM_4	No hay protocolos de mantenimiento.	Protocolos semanales de mantenimiento.	Monitorizacion	No	3
	AM_5	Falta de un sistema apropiado de seguridad.	Sistema de camaras.	Monitorizacion	No	2
	AM_7	No se realizan protocolos de higiene.	Fumigaciones mensuales y limpieza diaria.	Prevencion	Si	3
	AM_9	Falta de sistemas contra incendios.	Implementacion de detectores de humo y extintor.	Minimizadoras	No	2
	AM_10	El local no presenta los sistemas necesarios para minimizar el impacto de los desastres naturales.	Implementar pisos elevados, proteccion contra inundaciones y monitoreo de temperatura.	Minimizadoras	Si	2

	AM_11	Falta de cuidados y uso excesivo del A/C	Control en el uso y mantenimiento mensual del A/C	Prevencion	Si	3
	AM_13	Infraestructura debil contra posibles daños.	Fortificacion de la estructura de las instalaciones	Prevencion	Si	3
Software	AM_1	Falta de protectores de voltaje	Se necesita la instalacion de dispositivos para la proteccion de los dispositivos.	Prevencion	Si	3
	AM_4	No hay protocolos de mantenimiento.	Protocolos semanales de mantenimiento.	Monitorizacion	No	3
	AM_10	El local no presenta los sistemas necesarios para minimizar el impacto de los desastres naturales.	Implementar pisos elevados, proteccion contra inundaciones y monitoreo de temperatura.	Minimizadoras	Si	2
	AM_19	Falta de instrucciones para el correcto uso del software.	El maestro imparte instrucciones para el uso del software.	Concienciacion.	Si	1
	AM_3	Falta de seguridad contra malware en los equipos.	Constante proteccion de los equipos gracias al mantenimiento del antivirus.	Monitorizacion	Si	2
	AM_15	Falta de atencion a las actualizaciones de software.	Monitoreo diario de posibles actualizaciones.	Monitorizacion.	Si	3
	AM_16	Posibles problemas en la red, o conexion con el servidor.	Uso de DHCP para asignacion automatica de direcciones IP	Prevencion	Si	3

	AM_12	Infeccion de los equipos por descarga de archivos maliciosos.	Control del acceso a la red y descarga de archivos.	Prevencion	Si	2
	AM_8	Distracciones para los alumnos con acceso a la web	Restricciones a webs no autorizadas.	Minimizadoras	No	2
Informacion	AM_6	Destruccion de la informacion publica.	Restriccion de la eliminacion de archivos en las computadoras.	Prevencion	Si	2
	AM_18	Modificacion o alteracion de la informacion publica.	Restriccion de la modifiacion de archivos en las computadoras.	Prevencion	No	2
	AM_3	Falta de seguridad contra malware en los equipos.	Constante proteccion de los equipos gracias al mantenimiento del antivirus.	Monitorizacion	Si	2
	AM_14	Contraseñas debiles e inseguras.	Uso de contraseñas seguras y cambio regular de las mismas.	Administrativas	No	2

Impacto Residual

Tipo de activo	Codigo de amenaza	Vulnerabilidad	Control	Impacto potencial	Impacto residual	Riesgo Residual
Hardware	AM_1	Falta de protectores de voltaje	Se necesita la instalacion de dispositivos para la proteccion de los dispositivos.	3	1,7	2
	AM_2	Esquemas no tan rigurosos para las reglas.	Revisiones antes del ingreso al laboratorio.	2	2,2	3
	AM_4	No hay protocolos de mantenimiento.	Protocolos semanales de mantenimiento.	7	1	2
	AM_5	Falta de un sistema apropiado de seguridad.	Sistema de camaras.	6	1	1
	AM_7	No se realizan protocolos de higiene.	Fumigaciones mensuales y limpieza diaria.	4	1,5	2
	AM_9	Falta de sistemas contra incendios.	Implementacion de detectores de humo y extintor.	8	4	4
	AM_10	El local no presenta los sistemas necesarios para minimizar el impacto de los desastres naturales.	Implementar pisos elevados, proteccion contra inundaciones y monitoreo de temperatura.	11	3	3
	AM_11	Falta de cuidados y uso excesivo del A/C	Control en el uso y mantenimiento mensual del A/C	5	1,3	2
	AM_13	Infraestructura debil contra posibles daños.	Fortificacion de la estructura de las instalaciones	11	5	5
Software	AM_1	Falta de protectores de voltaje	Se necesita la instalacion de dispositivos para la proteccion de los equipos.	8	3	3
	AM_4	No hay protocolos de mantenimiento.	Protocolos semanales de mantenimiento.	6	2	1,8

	AM_10	El local no presenta los sistemas necesarios para minimizar el impacto de los desastres naturales.	Implementar pisos elevados, proteccion contra inundaciones y monitoreo de temperatura.	11	3	3
	AM_19	Falta de instrucciones para el correcto uso del software.	El maestro imparte instrucciones para el uso del software.	4	2	1
	AM_3	Falta de seguridad contra malware en los equipos.	Constante proteccion de los equipos gracias al mantenimiento del antivirus.	4	1,5	1
	AM_15	Falta de atencion a las actualizaciones de software.	Monitoreo diario de posibles actualizaciones.	3	1	2
	AM_16	Posibles problemas en la red, o conexion con el servidor.	Uso de DHCP para asignacion automatica de direcciones IP	6	2	1
	AM_12	Infeccion de los equipos por descarga de archivos maliciosos.	Control del acceso a la red y descarga de archivos.	5	1,7	2
	AM_8	Distracciones para los alumnos con acceso a la web	Restricciones a webs no autorizadas.	2	1	1
Informacion	AM_6	Destruccion de la informacion publica.	Restriccion de la eliminacion de archivos en las computadoras.	4	1	1
	AM_18	Modificacion o alteracion de la informacion publica.	Restriccion de la modifiacion de archivos en las computadoras.	4	1	1
	AM_3	Falta de seguridad contra malware en los equipos.	Constante proteccion de los equipos gracias al mantenimiento del antivirus.	5	2	2
	AM_14	Contraseñas debiles e inseguras.	Uso de contraseñas seguras y cambio regular de las mismas.	4	1	2

Comunicación del riesgo y Recomendaciones.

Analizando las zonas de riesgo, nuestro equipo decidio omitir ciertas amenazas y sus respectivos riesgos debido al poco daño que provocarian y su muy rara aparicion en el laboratorio. De igual manera se omitiran las amenazas que ya presentan un metodo de control propio.

Para los riesgos ubicados en las zonas medias (M) y zonas altas (A), se recomienda que se lleve a cabo un tratamiento de inmediato. Las opciones de tratamiento que se sugieren son:

Eliminación: consiste en suprimir uno o varios elementos que intervienen en el riesgo siempre y cuando se empleen otros en su reemplazo y no se afecte el correcto funcionamiento del laboratorio.

Mitigación: consiste en implementar nuevos controles o aumentar la madurez del control existente y por ende la efectividad del mismo, con el objetivo de reducir el impacto o reducir la probabilidad de ocurrencia.

Compartición: hace referencia a la transferencia del riesgo, ya sea parcial o total se puede dar de dos formas: la primera, es tercerizar los servicios o componentes en riesgo, acordando niveles de servicio que garanticen la operatividad de los mismos. La segunda es directamente con una aseguradora, la cual por medio de una cuantía monetaria se hace responsable de las consecuencias a causa de la materialización del riesgo.

Financiación: consiste en un ahorro o ‘fondo de contingencia’ que la institucion aprovisiona para responder a las consecuencias a causa de la materialización del riesgo.

Amenazas	Zona de Riesgo		
	Baja	Media	Alta
Modificacion o alteracion de la informacion publica.	5	--	--
Falta de cumplimiento de la regla que prohibe el ingreso de alimentos y bebidas al laboratorio.	--	3	--
Robo de perifericos o componentes de uso esencial para las computadoras del laboratorio.	--	2	--
Contraseñas debiles o por defecto.	--	8	--
Falta de mantenimiento en los equipos.	--	--	12
Incendios.	--	--	9
Total	5	13	21

Tratamiento de riesgos.

Elemento en riesgo	Riesgo	Fortaleza	Debilidad	Impacto	Zona Inicial	Zona Final	Accion
Instalaciones y equipos.	Incendio.	Personal capacitado y sistemas contra incendios.	- No se cuenta con sistemas contra incendios. - Se tendria que capacitar al personal que dirige el laboratorio.	Catastrofico	Alto	Alto	**Compartir:** Capacitaciones. **Compartir:** Compra del equipo necesario para detectar y hacer lo posible para mitigar el fuego.
Equipos	Falta de mantenimiento en los equipos.	Tecnico especialista que se asegure de mantener los equipos en estados optimos.	- Falta de limpieza en los equipos. - Componentes disfuncionales. - Reemplazo de componentes.	Mayor	Alto	Medio	**Reducir:** Contratar a un tecnico que se encargue del estado de los equipos. **Compartir:** Comprar herramientas necesarias para mantener los equipos.
Equipos	Robo de perifericos o componentes para las computadoras del laboratorio.	Sistemas de vigilancia. Estudiantes conocen los riesgos sobre el robo en el laboratorio.	- Falta de componentes necesarios para las computadoras. - Falta de personal de vigilancia y sistema de vigilancia	Moderado	Medio	Bajo	**Evitar:** Instalar un equipo de vigilancia. **Compartir:** Contratar a un vigilante.
Software	Contraseñas debiles o por defecto.	Protocolos mas estrictos para la mantencion de la seguridad en las contraseñas.	- Inseguridad de los equipos. - Personal inexperto en temas de seguridad.	Moderado	Medio	Bajo	**Compartir:** Capacitar al personal sobre los protocolos de seguridad.

Archivos de informacion	Modificacion o alteracion de la informacion publica.	Equipos mas robustos en cuanto a seguridad se refiere.	- Archivos desprotegidos. - No hay limitaciones en los permisos dados a los estudiantes.	Moderado	Medio	Bajo	**Reducir:** Aplicar restricciones a los usuarios utilizados por los estudiantes.
Equipos e instalaciones.	Falta de cumplimiento de la regla que prohibe el ingreso de alimentos y bebidas al laboratorio.	Control sobre posibles accidentes relacionados a liquidos y comestibles ingresados al laboratorio.	- Daños al sistema electrico. - Daños a los equipos del laboratorio.	Moderado	Medio	Bajo	**Compartir:** Concientizar a los estudiantes sobre los daños que podrian ocasionar a los equipos. **Reducir:** Protocolos estrictos de entrada al laboratorio.
Software de los equipos.	Software desactualizados.	Contar con las ultimas actualizaciones y opciones disponibles por los softwares instalados.	- Fallos de seguridad en el sistema operativo. - Mal funcionamiento del equipo. - Uso de software obsoleto.	Mayor	Alto	Bajo	**Reducir:** Verificar posibles actualizaciones semanalmente. **Evitar:** Programar actualizaciones automaticas.

Costos en Seguridad Informatica.

Tipo de Recurso	Descripcion del recurso	Valor mensual	Valor Anual
Recursos Humanos	Tecnico para la revision del estado de los equipos.	L 4,000.00	L 48,000.00
	Personal para supervisar las actividades en el laboratorio.	L 6,000.00	L 72,000.00
	Asesoria sobre seguridad informatica.	L 20,000.00	L 240,000.00
Recursos Tecnologicos	Tapa de tomacorrientes plastica para intemperie.	L 125.00	L 1,500.00
	Circuito cerrado de camaras de vigilancia.	L 7,389.17	L 88,670.00
	Detectores de humo y alarmas contra incendios.	L 141.75	L 1,701.00
	Extintor.	L 56.67	L 680.00
	Herramientas de mantenimiento preventivo (aire comprimido, pasta termica, brochas).	L 298.00	L 3,576.00
	Total	**L 38,010.59**	**L 456,127.00**

Conclusiones

- Terminado el analisis de riesgos y la gestion de los mismos, plasmados ya en el documento presente, lograra la concienciacion del personal del laboratorio del Instituto Educativo Modelo sobre los riesgos, vulnerabilidades y amenazas que podrian generar un impacto negativo en el funcionamiento del laboratorio.

- Gracias a la formulacion de la gestion de riesgo implementada, se le ha podido brindar informacion al instituto, para que siga un camino en busqueda de afianzar la seguridad informatica dentro de sus instalaciones. Gracias a la division de los posibles riesgos, se pueden priorizar las amenazas que representan gran impacto al instituto.

- Nuestro equipo motiva al instituto Educativo Modelo, a continuar trabajando en consolidar firmemente las bases de seguridad informatica ya implementada dentro del instituto, y crear un ambiente seguro para sus empleados y estudiantes.

- Una vez la institucion tenga la iniciativa para invertir en la seguridad informatica del laboratorio, se ha facilitado en nuestro plan de gestion de riesgos, un costo estimado que puede servir de guia para futuras mejoras, si es que desean implementar algunas de las opciones presentadas.

Bibliografia

Guamanga Chilito, C. A., & Perilla Buitrago, C. L. (2015). Análisis de riesgos de seguridad de la información basado en la metodología magerit para el área de datacenter de una entidad promotora de salud. Universidad Piloto de Colombia Facultad de Ingeniería.

Libro 1 - Metodo. (2012). Ministerio de Hacienda y Administraciones Públicas.

Gómez Vieites, A. (2015). Seguridad informatica basico. ECOE Ediciones.

Plan de tratamiento de riesgos seguridad de la informacion. (2018). Tecnológico de Antioquia Institución Universitaria.

Gómez Vieites, A. (2014). Auditoría de seguridad informática (978.a-84.a-9265.a-074-3 ed. ed.). RA-MA, S.A. Editorial y Publicaciones.