Universidad Católica de Honduras

“Nuestra Señora Reina de la Paz”

Asignatura: Seguridad Informática y Gestión de Riesgo

Docente: Lic. Patricia Medina

Sección: 1501

Fecha: viernes 10 de junio del 2022

Trabajo: Desarrollo de Informe de Seguridad y Gestión de Riesgo

Grupo: 6

Integrantes	Número de cuenta
Khail Yoshef Cruz Zelaya	0801 2001 11435
Jhonatan Fabricio Vargas Morales	0801 1998 13012
Wendy Paola flores Girón	0703-2000-00873
Wilson Ariel Lizardo Sánchez	0801 2001 11999

Índice

Introducción

En este informe se describe la solución a detalle para que la escuela CENG Evangélico Luz y Verdad tenga una mejor seguridad al momento de manejar todas sus máquinas para las actividades diarias que hacen con ellas. Es importante el siempre tener en cuenta de cubrir cada aspecto o situación peligrosa para que el trabajo sea eficiente y así poder asegurar también la vida útil de las computadoras, los router y todo equipo necesario para realizar las actividades de la escuela. Siempre es necesario el mantenimiento y el chequeo de los equipos como una muy buena práctica para lograr los objetivos de mantener óptimos los equipos de trabajo para que puedan mucho más y servir más para la empresa.

Objetivos

Objetivo General

- Conocer los riesgos , vulnerabilidades que se pueden presentar en el laboratorio de cómputo de la escuela CENG Evangélico Luz y Verdad. De lo anterior mencionado se busca crear un plan de seguridad para la prevención y detección de los equipos informáticos en el laboratorio con el fin de evitar daños, amenazas, acciones malintencionadas en el laboratorio.

Objetivos específicos

- Implementar las metodologías MAGERIT explicadas en clase para un desarrollo de un análisis completo de seguridad.
-
- Cuantificar y evaluar los activos con lo que cuenta el laboratorio de la escuela CENG Evangélico Luz y Verdad
-
- Crear planes para contingencias , emergencias para ser implementados y prevenir riesgos

Justificación

El desarrollo de este Sistema de Gestión en Seguridad Informática para el laboratorio de cómputo de la escuela CENG Evangélico Luz y Verdad, permitirá y buscará el mejor de las prácticas para un laboratorio que con los años y con muchos estudiantes por delante seguirá siendo un espacio confiable, protegido y mantenible de la manera más eficaz.

Este sistema contará cómo hacerle frente con ciertas amenazas y vulnerabilidades, porque como es sabido, todo equipo informático necesita de un debido mantenimiento , cuidado , protección ya sean por acciones malintencionadas de usuarios no autorizados, por causas de fenómenos naturales y también con la infraestructura donde están siendo utilizadas todos estos equipos. Es por eso el desarrollo y la necesidad de un manual como este, que ayudará a prevenir todos los escenarios posibles en los que los equipos del laboratorio puedan estar expuestos.

Planteamiento del problema

La seguridad es algo muy importante hoy más que nunca basándose en dispositivos electrónicos por la información que se maneja en ellos que son desde algo básico como documentos de tareas o trabajo, hasta cuentas de correo electrónico, banca en línea entre otros. Por eso es necesario contar con seguridad en los centros de cómputo.

En este este reporte se trabajará con un laboratorio de cómputo de una escuela el cual nos planteamos estimar si se ve comprometida la seguridad de las máquinas ante virus o amenazas, ver cuales pueden ser los posibles riesgos o amenazas que tengan las computadoras o la red, logrando identificar así todos o la mayoría de problemas principales que puedan llegar a afectar la integridad del laboratorio de cómputo.

Marco Conceptual

¿Qué es la información?

La información es un conjunto organizado de datos relevantes para uno o más sujetos que extraen de él un conocimiento. Es decir, es una serie de conocimientos comunicados, compartidos o transmitidos y que constituyen por lo tanto algún tipo de mensaje. Sin embargo, su definición varía según la disciplina o el enfoque desde el cual se la piense.

Por ejemplo, en la biología, se entiende como información al conjunto de estímulos sensoriales que intercambian los seres vivientes, mientras que en el periodismo la información es el conjunto de mensajes intercambiados por los actores de una sociedad determinada. A esto podríamos añadir definiciones provenientes de la informática, la cibernética o la termodinámica.

Tipos de información

La información puede clasificarse de maneras muy distintas, conforme a numerosos criterios. Uno de los más comunes tiene que ver con la relación establecida entre los emisores de la información y sus eventuales o posibles receptores, de la siguiente manera:

- Información confidencial o clasificada. Aquella a la que sólo puede acceder un pequeño conjunto de personas, dada la naturaleza secreta, peligrosa, delicada o privada de los datos contenidos en ella.
- Información pública. Aquella que, por el contrario, permite el acceso general de cualquiera a su contenido, sin requerir permisos especiales y sin tener ningún grado de privacidad.
- Información personal. Aquella que le pertenece a cada persona, es decir, que emana de un individuo concreto, el cual puede decidir con quién compartirla o a quién ofrecérsela.
- Información externa. Aquella que emana de un organismo, institución o empresa, y cuyos destinatarios son instancias o personas externas a la misma.

- Información interna. Aquella, por el contrario, que emana de un organismo, institución o empresa, con el fin de ser consumida de manera interna, sin salir al exterior de la organización.

¿Qué es seguridad informática?

La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndo así en información privilegiada.

¿Para qué sirve?

El objetivo de la seguridad informática es mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computadora. Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Las cuatro áreas principales que cubre la seguridad informática

1. Confidencialidad: Violaciones de seguridad informática que vulneran la confidencialidad.
2. Integridad: Violaciones de seguridad informática que afecta la integridad de la información.
3. Disponibilidad: Violaciones de seguridad informática que afecta la disponibilidad.

4. Autenticidad: Violaciones de seguridad informática que afecta la autenticidad.

¿Por qué es importante la seguridad informática en las empresas?

Porque ayudan a evitar:

- Consecuencias económicas
- Riesgos legales
- Compromisos de seguridad con los usuarios

Tipos de Vulnerabilidades y Amenazas informáticas en la empresa

Son muchas las vulnerabilidades y amenazas informáticas a las que están expuestas las empresas en la actualidad. Por eso la inversión en ciberseguridad y sistema de protección ha experimentado un gran aumento en los últimos años, siendo los profesionales en ciberseguridad uno de los perfiles más buscados en el sector de la informática.

A continuación, veremos las principales amenazas y vulnerabilidades a las que se exponen las empresas hoy en día:

Amenazas de Malware

Los programas maliciosos son una de las mayores ciberamenazas a la que se exponen las empresas. Dentro del malware existen distintos tipos de amenazas, siendo las principales.

- Virus. Los virus informáticos son un software que se instala en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).
- Gusanos. Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles

utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.

- Troyanos. Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.
- Ransomware. El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).
- Keyloggers. Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Vulnerabilidades del sistema

Los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos. Las principales vulnerabilidades suelen producirse en:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos.

Amenazas de ataques de denegación de servicio

Un ataque de denegación de servicio distribuido (DDoS) se produce cuando un servidor recibe muchas peticiones de acceso, sobrecargando el sistema y haciendo que el

servidor caiga o funcione de forma incorrecta (acceso lento o rebotando mensajes de errores). Para realizar este tipo de ataques se utilizan muchos ordenadores (bots) que de forma automatizada hacen peticiones a ese servidor.

Los ataques DDoS son muy habituales contra servidores o servidores web de empresas, por lo que es muy importante disponer de medidas protectoras contra esta peligrosa amenaza que puede dejar fuera de servicio la actividad de una empresa.

Vulnerabilidades producidas por contraseñas

Con el teletrabajo y el cloud computing la gestión de contraseñas se ha convertido en uno de los puntos más importantes en ciberseguridad. Para acceder a las plataformas de trabajo de las empresas es necesario utilizar un usuario y contraseña. Utilizar contraseñas poco seguras genera vulnerabilidades en los sistemas, pues si son fácilmente descifrables pueden generar incursiones de terceros no autorizados que pueden robar, modificar o eliminar información, cambiar configuraciones si disponen de los privilegios apropiados, o incluso apagar equipos.

La generación de contraseñas seguras es una de las claves para incrementar el nivel de ciberseguridad de las empresas.

Vulnerabilidades producidas por usuarios

Una de las principales causas de los ataques informáticos está relacionada con un uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa.

El error humano es otra causa de riesgos en ciberseguridad. El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en ciberseguridad se tiende a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano.

Las malas prácticas o la falta de formación en ciberseguridad también generan vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza a sufrir ataques como el phishing (suplantación de identidad) o similares.

SGSI

El SGSI es un sistema de fácil implantación tanto para grandes empresas como para pymes. Es una herramienta para conocer y gestionar los riesgos a los que se enfrenta el negocio al manejar su información en el día a día. Al implementar SGSI se podrá eliminar esos riesgos o establecer los mecanismos necesarios para mitigar sus consecuencias.

Los principales beneficios que obtiene una empresa al implantar un sistema SGSI para la seguridad de sus datos son:

- Reducción de riesgos. Se identificarán los riesgos y amenazas gracias a controles, protocolos, políticas y monitorización de procesos logrando reducir el número de amenazas de forma notable. En caso de que se produzca un incidente relacionado con los datos, el negocio estará preparado para actuar de forma inmediata minimizando su impacto.
- Reducción de costes. Se optimizará todo el proceso para evaluar y detectar amenazas descartando aquellos poco eficaces. Con un uso racional de los recursos se conseguirá un ahorro de costes en seguridad.
- Integración de la seguridad en el negocio. Este sistema requiere de la implicación de todos los miembros de la empresa y del cambio de mentalidad, pasando a ser la seguridad uno de los componentes más importantes en cualquier proceso o actividad del negocio.
- Cumplimiento de la normativa vigente en seguridad. Las leyes nacionales e internacionales para el tratamiento y protección de datos estarán cubiertas garantizando que se cumplen en todos los niveles o áreas de la empresa.
- Incremento de la competitividad. Con este sistema se dispondrá de una prestigiosa certificación ISO de seguridad que será un elemento diferenciador con la competencia. Los clientes se sentirán más confiados y seguros de compartir sus

datos personales, bancarios, gustos, y similares al saber que la empresa utiliza las mejores prácticas para garantizar que estén seguros.

RFC 2196

Es un memorándum publicado por el Internet Engineering Task Force para el desarrollo de políticas y procedimientos de seguridad para sistemas de información conectados a Internet; proporciona una amplia y general visión de la seguridad de la información incluyendo la seguridad de la red, respuesta a incidentes o las políticas de seguridad. El documento es muy práctico y centrado en el día a día de las operaciones.

ISM3

ISM3 es un modelo de madurez para seguridad con cinco niveles que facilita la mejora y alineación entre las necesidades del negocio y los de la gestión de la seguridad dirigido a organizaciones de cualquier tipo y tamaño. Fue creado por un consorcio creado en marzo de 2007 y formado por las empresas ESTEC Systems (Canadá), First Legion Consulting y Valiant Technologies (India), Seltika (Colombia), Global 4 Ingeniería (España) y M3 Security (Estados Unidos), con el objetivo de llevar los principios de la gestión de calidad ISO9001 o Six Sigma a los sistemas de gestión de seguridad de la información. Sabemos que alcanzar un grado de madurez en ciberseguridad toma mucho tiempo para algunas organizaciones. Razón por la cual ISM3 se adapta perfectamente a este escenario brindando la oportunidad a la organización de desarrollar planes a corto, mediano y largo plazo, medible, adaptable y 100% integrado al negocio que permita poco a poco alcanzar ese nivel de seguridad óptimo esperado.

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.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.
Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

Metodología Magerit

La metodología Magerit está elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. Magerit ofrece una aplicación para el análisis y gestión de riesgos de un Sistema de la Información. 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. 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.

Esta metodología facilita lograr los siguientes puntos:

- El análisis de riesgo en cualquier tipo de Sistema de Seguridad de la Información (SSI), así como todos sus elementos, obteniendo un índice único en el que se realicen las estimaciones de su vulnerabilidad ante todas las posibles amenazas y el impacto que puede generar en la empresa.
- La gestión de riesgos, se basa en todos los resultados obtenidos durante el análisis que hemos hecho anteriormente, se seleccionan medidas de seguridad adecuadas para poder conocer, prevenir, impedir, reducir o controlar todos los riesgos que se han identificado, pudiendo de este modo reducir al mínimo la potencialidad del riesgo.

Descripción de la Organización

Empresa: CENG Evangelico Luz y Verdad

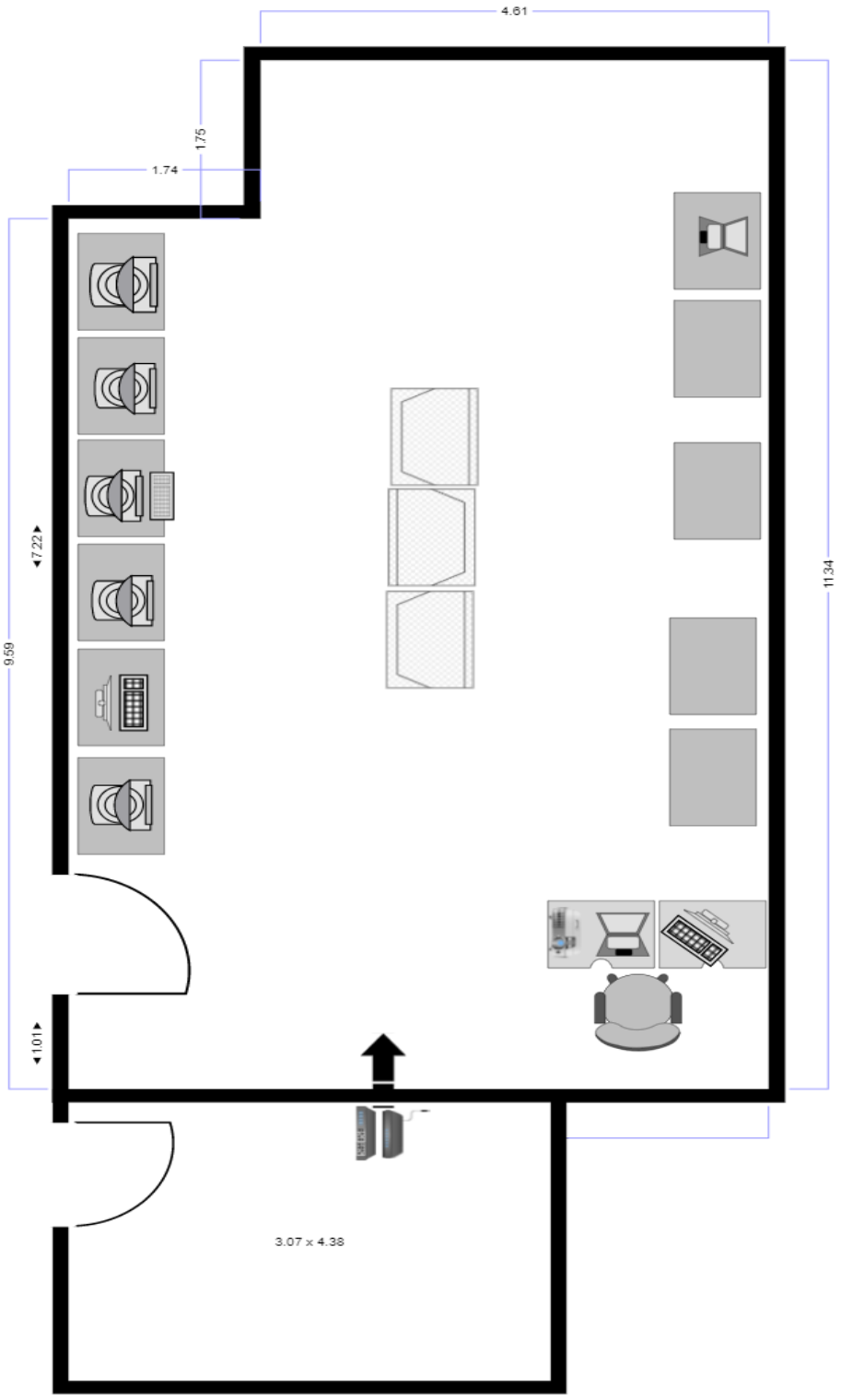
Dirección: 3ra entrada Kennedy, cerca de instituto Jesús milla selva atas de posta policial y correo nacional

Misión: Somos una institución en Educación, ofrecemos enseñanza y servicios de calidad y excelencia, plenamente respaldados con avanzada tecnología y procesos de mejora continua, un recurso humano altamente calificado y con mucho sentido de responsabilidad social.

Visión: Seremos una institución modelo a nivel local en el sistema enseñanza-aprendizaje y ocupar el primer lugar en la forma de alumnos y alumnas con excelencia académica, principios cristianos y humanitarios a nivel nacional

Lugar a analizar: Laboratorio de cómputo, segundo piso

Diagrama Físico y distribución de los activos



Análisis de Riesgos

2.1 Descripción de los activos o recursos informáticos

Activo	Descripción
Computadoras	Equipo informático que es utilizado principalmente por los estudiantes en las áreas del laboratorio en horas de recibir sus clases correspondientes a la informática , haciendo uso también de los diferentes software o programas para su enseñanza.
Proyector	Permite a los docentes ampliar que lo que están haciendo en sus computadoras y sean más visible por los alumnos
Switches	Encargados de conectar muchos equipos directamente a una misma red
Routers	Guían los diferentes paquetes a sus respectiva red de destino , y permite la interconexión y comunicación entre distintas redes
Periféricos	Variedad de teclados y mouse.
Gabinete de red	Es donde se encuentran los equipos de red más sofisticados para la escuela como ser router y switch
Extensiones eléctricas	Elementos con el fin de llevar fuente de energía a equipo que no están cerca de una toma de corriente
Información	Todos aquellos programas de software utilizados en el centro de cómputo, trabajos de clase, como también otro tipo de información de índole personal o profesional

2.1.1 Especificaciones de los activos

Activo	Especificaciones
Switches	TP-LINK TL-SF1024 24 puertos 10/100 Mbps
Routers	MikroTik
Proyector	Epson
Extensiones eléctricas	Aguila

2.2 Valoración de Activos o Recursos

A continuación se presenta la valoración de qué tan graves o peligrosas las situaciones que lleguen a presentarse en el laboratorio

La valoración 5 significa que es un daño muy grave

Estos son daños que pueden causar incidentes fatales en el laboratorio además de pérdida económica y activos

La valoración 4 significa que es un daño grave

Estos daños se limitan a solo ser un problema para la continuación de actividades en el laboratorio y que pueden afectar la seguridad física de las máquinas que utilizan los estudiantes y el encargado

La valoración 3 significa que es un daño importante
Estos daños afectan la eficacia de trabajo de los equipos del laboratorio y daños involucrando terceros utilizando el laboratorio causando impedimentos

La valoración 2 significa que es un daño medio
Estos daños son daños un poco preocupantes y pueden ser causados por accidentes menores que pueden llegar a la máquina principal afectada y a sus alrededores

La valoracion 1 significa que es un daño menor
Estos daños con de rápido arreglo y solo afectan a un individuo que utilice el equipo

La valoración 0 significa que es insignificante
Estos daños no afectan en absoluto en el laboratorio

Gráficamente se expresan de la siguiente manera:

2.2.1 Tabla de Valoración de Activos o Recursos

Tabla de Valoración		
Valor		Descripción
5	Muy Grave	Daños muy graves que afecten demasiado
4	Grave	Daños graves en el laboratorio
3	Importante	Daños importantes que deben ser atendidos rápidamente
2	Medianamente Grave	Daños medianamente graves que pueden solucionarse casi de manera inmediata
1	Poco Grave	Daños que no tienen tanto impacto en el laboratorio
0	Insignificante	Daño que no afecta ningún área del laboratorio

2.3 Identificación de Amenazas y Probabilidad

Nivel	Descripción de probabilidad
1	Probabilidad de suceder de forma anual.
2	Probabilidad de suceder cada 6 meses.
3	Probabilidad de suceder de forma trimestral.
4	Probabilidad de suceder de forma mensual.
5	Probabilidad de suceder de forma muy ocasional.

2.4 Amenazas Clasificadas por su tipo y su nivel de Probabilidad

ID	NOMBRE	NP
AM_1	Uso de pendrives infectados	5
AM_ 2	Falta de mantenimiento en los equipos	3
AM_3	Averías en el equipo por fallas en el fluido eléctrico	4
AM_ 4	Falta de cumplimiento de la regla que prohíbe el ingreso de alimentos	5
AM_5	Destrucción de la información pública o perteneciente a estudiantes	4
AM_6	Robo de periféricos o componentes de uso esencial	2
AM_7	Mal uso de software.	5
AM_8	Descargar de archivos maliciosos o dañinos	4
AM_9	Desastres naturales	1
AM_10	Conflicto con direcciones IP	4
AM_11	Plagas en el laboratorio	1
AM_12	Problemas por Contraseñas débiles o por defecto	3
AM_13	Software desactualizado	3
AM_ 14	Incendios en el laboratorio	1

2.5 Matriz de Impacto Potencial.

ID	Descripción	Descripción de impacto
1	Grado Insignificante	Los impactos tendrán un efecto muy leve o ninguno.
2	Grado Menor	Los impactos son de bajo grado.
3	Grado Moderado	Los impactos tendrían efectos considerables.
4	Grado Mayor	Los impactos tendrían un efecto bastante grave.
5	Grado Catástrofe	Los efectos causarían efectos muy graves, casi terminando con el centro informático.

Tipo de activo	Código Amenaza	Amenazas	Impacto
	AM_3	Averías en el equipo por fallas en el fluido eléctrico	3
	AM_ 4	Falta de cumplimiento de la regla que prohíbe el ingreso de alimentos	3
Hardware	AM_ 2	Falta de mantenimiento en los equipos	4
	AM_6	Robo de periféricos o componentes de uso esencial	3
	AM_11	Plagas en el laboratorio	2
	AM_9	Desastres naturales	5
	AM_3	Averías en el equipo por fallas en el fluido eléctrico	3
	AM_ 2	Falta de mantenimiento en los equipos	4
	AM_9	Desastres naturales	5
Software	AM_7	Mal uso de software	3

	AM_3	Averías en el equipo por fallas en el fluido eléctrico	3
	AM_13	Software desactualizado	4
	AM_10	Conflicto con direcciones IP	5
	AM_8	Descargar de archivos maliciosos o dañinos	2
	AM_5	Destrucción de la información pública o perteneciente a estudiantes	2
Informática	AM_12	Problemas por Contraseñas débiles o por defecto	3

2.6 Matriz de Riesgo Potencial

		Muy Bajo	Bajo	Medio	Alto	Muy Alto
PROBABILIDAD	**VALOR**	1	2	3	4	5
Muy alta	5	5	10	15	20	25
Alta	4	4	8	12	16	20
Media	3	3	6	9	12	15
Baja	2	2	5	6	8	10
Muy baja	1	1	2	3	4	5

	Riesgo Grave
	Riesgo importante
	Riesgo Apreciable
	Riesgo Marginal

Tipo de activo	Código Amenazas	Amenazas	Impacto	Nivel Probabilidad	Riesgo potencial	Zona Riesgo
	AM_3	Averías en el equipo por fallas en el fluido eléctrico	3	3	9	R_I
	AM_4	Falta de cumplimiento de la regla que prohíbe el ingreso de alimentos	3	4	12	R_I
Hardware	AM_2	Falta de mantenimiento en los equipos	4	3	12	R_I
	AM_6	Robo de periféricos o componentes de uso esencial	3	1	3	R_A
	AM_11	Plagas en el laboratorio	2	1	2	R_M
	AM_9	Desastres naturales	5	1	5	R_A
	AM_3	Averías en el equipo por fallas en el fluido eléctrico	3	2	6	R_A
	AM_2	Falta de mantenimiento en los equipos	4	3	12	R_I
	AM_9	Desastres naturales	5	1	5	R_A
Software	AM_7	Mal uso de software	3	5	15	R_G
	AM_3	Averías en el equipo por fallas en el fluido eléctrico	3	3	9	R_I

	AM_13	Software desactualizado	4	3	12	R_I
	AM_10	Conflicto con direcciones IP	5	2	10	R_I
	AM_8	Descargar de archivos maliciosos o dañinos	2	3	6	R_A
	AM_5	Destrucción de la información pública o perteneciente a estudiantes	2	2	4	R_A
Informática	AM_12	Problemas por Contraseñas débiles o por defecto	3	2	6	R_A

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

Activo	Riesgo	Total
Riesgos marginales		
Computadora	Desperfectos en el equipo	2
	Robo de información	
Proyector	Desperfectos en el equipo	1
Switch	Desperfectos en el equipo	3
	Daños físicos al equipo	
	Fallas de configuración	
Router	Desperfectos en el equipo	3
	Daños físicos al equipo	
	Fallas de configuración	
Gabinete de red	Daños físicos al equipo	1
Extensiones eléctricas	Desperfectos eléctricos	1
Riesgos apreciables		
Computadora	Virus, gusanos y ransomware	4
	Robo de información	
	Hardware y Software incompatible	
	Sistema operativo no arranca	
Proyector	Mal manejo del equipo	2
	Daños físicos al equipo	
Switch	Fallas de configuración	4
	Daños físicos al equipo	
	Puertos en mal estado o sucios	
	Contraseñas débiles	
Router	Fallas de configuración	4
	Daños físicos al equipo	
	Puertos en mal estado o sucios	
	Contraseñas débiles	
Periféricos	Daños físicos al equipo	1
Gabinete de red	Desperfectos	1
Riesgos Importantes		

Gabinete de red	No asegurar bajo llave	1
Router	No crear usuarios ni contraseñas	1
Switch	No crear usuarios ni contraseñas	1

2.8 Salvaguardas o Controles existentes

Para riesgos siempre hay que tener siempre planes de contingencia para tratar de contrarrestar cualquier situación que pueda poner en peligro tanto el ambiente laboral como los equipos que se utilicen para realizar las actividades. Estos son algunos de los controles y salvaguardas que se encuentran en la instalación en caso de que algún desastre se presente.

Salvaguardas y Controles	
Código	Descripción
S_1	Extintor localizado cerca de la entrada del laboratorio
S_2	Sistema de detectores de humo instalados en el techo del laboratorio
S_3	Camaras de Seguridad a la entrada del laboratorio y del área del router
C_1	Protocolos de Seguridad contra incendios y terremotos
C_2	Sistema especial de seguridad que mantiene segura las computadoras
C_3	Mantenimiento del aire acondicionado
C_4	Limpiezas diarias en el laboratorio
C_5	Normas establecidas del laboratorio al momento de usarlo para trabajar

2.8.1 Controles Implementados según activos, amenaza y efectividad

Tipo	Código	Vulnerabilidad	Controles	Tipo de Control	Implementación	Eficacia
Hardware	AM_ 2	Falta de Mantenimiento de los equipos	Chequear los equipos a ciertos tiempos	Monitoreo	Si	5
	AM_ 3	Averías en el equipo por falta de fluido eléctrico	Tener un respaldo de electricidad para las máquinas	Prevención	No	2
	AM_ 6	Robo de periféricos o componentes del uso esencial	Contar con respaldos y repuestos de dichos componentes	Prevención	No	3
Software	AM_ 1	Uso de pendrives infectados	Utilizar antivirus en todos los equipos para evitar daños	Prevención	Si	4
	AM_ 7	Mal uso de software	Revisar los datos que se usen o los motivos de uso del software	Minimización	Si	3
	AM_ 8	Descargar archivos maliciosos o dañinos	Contar con un antivirus que analize si el archivo pueda ser peligroso	Prevención	Si	3
	AM_ 13	Software desactualizado	Revisión del software a ver si es necesario un cambio	Monitoreo	Si	4
Información	AM_ 10	Conflicto de Direcciones IP	Chequear las IP de los equipos para identificar mejor las máquinas	Monitoreo	No	1

	AM_ 12	Problemas por contraseñas débiles o por defecto	Hacer uso de contraseñas más largas y complejas por seguridad	Minimización	No	1
Ambiente	AM_ 4	Falta de cumplimiento de normas referentes a comida	Chequear de manera correcta la entrada de los usuarios con sus utensilios	Monitoreo	Si	5
	AM_ 9	Desastres naturales	Hacer uso de protocolos de evacuación para los usuarios del laboratorio	Prevención	Si	4
	AM_ 11	Plagas en el laboratorio	Fumigar el laboratorio para mantener fuera las plagas	Prevención	No	1
	AM_ 14	Incendio en el laboratorio	Tener componentes y utensilios anti incendios para apagar las llamas	Prevención	Si	3

3.1 Impacto Residual

Tipo de Activo	*Amenazas*	*Controles*	*Tipos de Control*	*Control Implementado*	*Eficiencia del Control*	*Impacto Potencial*	*Impacto Residual*
Hardware	Falta de Mantenimiento de los equipos	Chequear los equipos a ciertos tiempos	Monitoreo	Si	5	3	1.7
	Averías en el equipo por falta de fluido eléctrico	Tener un respaldo de electricidad para las máquinas	Prevención	No	2	3	0.7
	Robo de periféricos o componentes del uso esencial	Contar con respaldos y repuestos de dichos componentes	Prevención	No	3	3	1.0
Software	Uso de pendrives infectados	Utilizar antivirus en todos los equipos para evitar daños	Prevención	Si	4	2	2.0
	Mal uso de software	Revisar los datos que se usen o los motivos de uso del software	Minimización	Si	3	3	1.0
	Descargar archivos maliciosos o dañinos	Contar con un antivirus que analize si el archivo pueda ser peligroso	Prevención	Si	3	2	1.5
	Software desactualizado	Revisión del software a ver si es necesario un cambio	Monitoreo	Si	4	4	1.0
Información	Conflicto de Direcciones IP	Chequear las IP de los equipos para identificar mejor las máquinas	Monitoreo	No	1	5	0.2
	Problemas por contraseñas débiles o por defecto	Hacer uso de contraseñas más largas y complejas por seguridad	Minimizador	No	1	3	0.3
Ambiente	Falta de cumplimiento de normas referentes a comida	Chequear de manera correcta la entrada de los usuarios con sus utensilios	Monitoreo	Si	5	4	1.3

	Desastres naturales	Hacer uso de protocolos de evacuación para los usuarios del laboratorio	Prevención	Si	4	3	1.3
	Plagas en el laboratorio	Fumigar el laboratorio para mantener fuera las plagas	Prevención	No	1	1	1.0
	Incendio en el laboratorio	Tener componentes y utensilios anti incendios para apagar las llamas	Prevención	Si	3	5	0.6

3.2 Matriz de impacto residual y riesgo residual

Tipo de Activo	*Amenazas*	*Controles*	*Tipos de Control*	*Control Implementado*	*Eficiencia del Control*	*Impacto Potencial*	*Impacto Residual*	Nivel de probabilidad	Riesgo Residual
Hardware	Falta de Mantenimiento de los equipos	Chequear los equipos a ciertos tiempos	Monitoreo	Si	5	3	1.7	3	5.00
	Averías en el equipo por falta de fluido eléctrico	Tener un respaldo de electricidad para las máquinas	Prevención	No	2	3	0.7	4	2.67
	Robo de periféricos o componentes del uso esencial	Contar con respaldos y repuestos de dichos componentes	Prevención	No	3	3	1.0	2	2.00

Software	Uso de pendrives infectados	Utilizar antivirus en todos los equipos para evitar daños	Prevención	Si	4	2	2.0	5	10.00
	Mal uso de software	Revisar los datos que se usen o los motivos de uso del software	Minimización	Si	3	3	1.0	5	5.00
	Descargar archivos maliciosos o dañinos	Contar con un antivirus que analize si el archivo pueda ser peligroso	Prevención	Si	3	2	1.5	4	6.00
	Software desactualizado	Revisión del software a ver si es necesario un cambio	Monitoreo	Si	4	4	1.0	3	3.00
Información	Conflicto de Direcciones IP	Chequear las IP de los equipos para identificar mejor las máquinas	Monitoreo	No	1	5	0.2	4	0.80
	Problemas por contraseñas débiles o por defecto	Hacer uso de contraseñas más largas y complejas por seguridad	Minimizador	No	1	3	0.3	3	1.00
Ambiente	Falta de cumplimiento de normas referentes a comida	Chequear de manera correcta la entrada de los usuarios con sus utensilios	Monitoreo	Si	5	4	1.3	5	6.25
	Desastres naturales	Hacer uso de protocolos de evacuación para los usuarios del laboratorio	Prevención	Si	4	3	1.3	1	1.33
	Plagas en el laboratorio	Fumigar el laboratorio para mantener fuera las plagas	Prevención	No	1	1	1.0	1	1.00
	Incendio en el laboratorio	Tener componentes y	Prevención	Si	3	5	0.6	1	0.60

		utensilios anti incendios para apagar las llamas							

3.3 Comunicación del Riesgo y Recomendaciones

Riegos:

1. Incendios. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones inalámbricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

2. Inundaciones. Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.

3. Sismos. Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan, o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

4. Humedad. Se debe proveer de un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y al área de máquinas en forma exclusiva.

5. Robos. Las computadoras son posesiones valiosas de las empresas, y están expuestas, de la misma forma que están expuestas las piezas de stock e incluso el dinero. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección de la que dan a una máquina de escribir o a una calculadora, y en general a un activo físico.

6. Actos vandálicos. En las empresas existen empleados descontentos que pueden tomar represalias contra los equipos y las instalaciones.

7. Fraude. Cada año millones de dólares son sustraídos de empresas y, en muchas ocasiones las computadoras han sido utilizadas para dichos fines.

8. Sabotaje. Es el peligro más temido en los centros de cómputo. Empresas que han intentado implementar sistemas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros, el saboteador puede ser un empleado o un sujeto ajeno a la empresa.

Recomendaciones:

1. Mantener sistemas operativos actualizados

Si en las computadoras de tu laboratorio se ejecuta software personalizado que requieren de sistemas operativos desactualizados, ten presente que el nivel de vulnerabilidad ante los hackers es altísimo, ya que todo tipo de actualización está impedida.

2. Protegerse del malware

Los diferentes dispositivos de tu laboratorio pueden verse afectados por los agresivos malware, que no son más que códigos maliciosos diseñados para alterar su funcionamiento.

3. Controlar el uso de dispositivos móviles

Los celulares, tablets, portátiles y demás equipos inalámbricos son un gran desafío a la hora de garantizar la seguridad de la información, por ello como laboratorio debes implementar medidas que permitan autenticar, rastrear y proteger de forma remota la información contenida en estos dispositivos.

4. Reforzar la seguridad de alojamiento de la información

El alojamiento de la información dentro de un laboratorio puede hacerse tanto interna como externamente.

5. Implementa un sistema de contraseñas seguras

Si te has dado cuenta, la gran mayoría de los equipos, sitios web, aplicaciones informáticas, etc., te dan la posibilidad de establecer contraseñas de acceso, esto es una gran ventaja para la seguridad de la información.

Establece contraseñas complejas, difíciles de descifrar.

6. Proteger las computadoras con un Firewall

Los Firewall son la primera línea de defensa contra los hackers al evitar el acceso no autorizado a tu ordenador.

3.3.1 Tratamiento del Riesgo

1. Incendios: Tener a mano medidas anti incendios como extintores que sean de fácil acceso y rociadores de agua en los edificios para reducir las llamas. Que también se pueda contar con protocolos de seguridad contando con salidas seguras y rutas de escape para la seguridad de los empleados.

2. Inundaciones: Obtener un breaker de apagado total de toda electricidad del edificio para evitar propagación eléctrica por el agua hacia los empleados en peligro. Asimismo hay que contar con un protocolo de evacuación con salida de emergencia y un punto de encuentro seguro para el personal del instituto.

3. Sismos: Este desastre es uno de los más difíciles de afrontar, para estos se debe de realizar simulacros para entrenar al personal para poder prepararlos para posibilidad del desastre. Realizar protocolos de evacuación con rutas de escape seguras para los empleados.

4. Humedad: Realizar chequeos de los equipos tanto eléctricos como de la mueblería. Mantener ventilación del lugar de trabajo y que se mantenga en una temperatura óptima. Limpieza de desagües y mantenimiento del aire acondicionado para que mantenga la temperatura adecuada y revisión para confirmar que el aire acondicionado no tenga una fuga.

5. Robos: Mantener la seguridad tanto física como informática. De la parte física se debe de realizar un listado de cada activo tangible del laboratorio, y en caso de la

falta de un dispositivo, tener un respaldo o reemplazo del dicho. Y de la parte informática es que se debe de mantener monitoreada la información de la red institucional para confirmar que no haya alguna perpetración de la información.

6. Actos Vandálicos: Realizar horarios de vigilancia del centro de cómputo y cerrar con llave cuando el laboratorio no se encuentre en uso.

7. Fraude: Realizar verificación de la información recibida y utilizada en el lugar para evitar accidentes de grado mayor y guardar dicha información.

8. Sabotaje: Mantener un respaldo de la información usurpada y hacer uso de programas de seguridad tanto para las mismas computadoras como para sistemas de red. Realizar un chequeo de personal y de dispositivos traídos fuera del laboratorio

3.4 Costos en Seguridad Informática

Problemas	Soluciones a los Problemas	Costo Mensual	Costo Anual	Costo Instantáneo
Mal uso del software y virus informáticos	Adquirir licencias de software especializado para contrarrestar los toda clase de virus	$140.00	$1,700.00	
	Tutorías a los estudiantes y docentes de cómo se debe de manejar ciertos programas informáticos			$3,500.00
Riesgos contra incendios	Compra de equipo contra incendios, extintores			$1,600.00
Mala configuraciones en routers o switches	Contratar técnicos para las soluciones			$3,000.00
Hardware en mal estado(mouse, teclados, etc)	Compra de hardware que no se pueda recuperar o repararlos si son daños menores			$2,000.00

3.5 Conclusiones

- Se dieron a conocer los problemas y se encontraron soluciones para que el laboratorio de cómputo logre ser mucho más seguro y organizado

- La implementación de metodologías MAGERIT promete no solo hacer un análisis de la seguridad del laboratorio de cómputo, pero también buscar una solución para la seguridad del mismo

- Los activos lograron ser analizados e implementados dentro de la solución de seguridad del centro de cómputo para un uso más adecuado y más eficiente

- Los planes de contingencia siempre serán una parte fundamental para la seguridad tanto del centro de cómputo como de los usuarios que lo utilizan

3.6 Bibliografía

➔ Gómez Vieites, A. (). Enciclopedia de la seguridad informática. Alfaomega

➔ Gael. 2019. RIESGOS EN EL LABORATORIO DE INFORMÁTICA. Recuperado el 31 de jul. de 22 de: https://riesgosenellaboratoriodeinformaica.blogspot.com/2019/03/riesgos-en-el-centro-de-computo.html

➔ Oscar Delgado. 2022. 10 consejos de buenas prácticas para garantizar la seguridad de la información en tu laboratorio. Recuperado el 31 de jul. de 22 de: https://sgc-lab.com/10-consejos-de-buenas-practicas-para-garantizar-la-seguridad-de-la-informacion-en-tu-laboratorio/