Universidad Católica De Honduras

“Nuestra Señora Reina De La Paz”

Campus Santiago Apóstol

Asignatura:

Seguridad Informática y Gestión de Riesgos

Tema:

Análisis de evaluación de riesgo utilizando la metodología de MAGERIT

Catedrático:

Lic. Patricia Medina **Integrantes:**

- Laura Estela Galeano Martínez 0704199900809
- Gabriela Alejandra Gonzales 0709200000016
- Allan Isac Nuñez Jarquin 07041999003431
- Martha Elena Talavera 0703200001893

Sección: 1501

Fecha:08/02/2022

Índice

Introducción

Con el constante crecimiento de la dependencia de las tecnologías de la información; el cumplimiento de los principios de la gestión de seguridad basada en riesgos, así como los requisitos para el análisis y gestión de riesgos; se vuelven temas de interés primordial para las entidades en el ámbito de la seguridad.

El propósito de la investigación es presentar una propuesta de análisis e investigación para identificar los problemas en conjunto a sus causas y consecuencias que se dan en el área de laboratorio de cómputos. La utilización e implementación de la seguridad en el área es el objetivo principal a tratar. Debido a esto, se plantean estrategias que ayuden a mitigar dichas situaciones e intentar establecer los aspectos de seguridad más actualizados y necesarios en un entorno donde la computación es primordial. La metodología Magerit es un método público que se puede utilizar libremente sin la autorización. Dada la dependencia de las tecnologías de la información, el cumplimiento de los principios de la gestión de seguridad basada en riesgos, así como los requisitos para el análisis y gestión de riesgos, son de interés primordial para las entidades en el ámbito de la seguridad.

Objetivos

General

Mediante el método MAGERIT, analizar los riesgos que genera la utilización de los dispositivos y servidores en el área de laboratorio de cómputos, identificar los principales problemas y ejecutar el proyecto para evaluar y realizar estrategias cuya finalidad es aumentar la seguridad en los equipos.

Específicos

1. -Conocer y comprender los conceptos de la seguridad informática.
2. -Profundizar en el conocimiento de la metodología MAGERIT para poder crear estrategias más efectivas.
3. -Aplicar los principios de la metodología MAGERIT en el área de laboratorio de cómputo.
4. -Identificar cuáles son los riesgos y vulnerabilidades que contienen en el área de laboratorio de cómputo.
5. -Planear estrategias para evitar los problemas identificados.
6. -Aumentar la seguridad en los equipos para evitar cualquier tipo de ataque informático.

Planteamiento Del Problema

En el área de informática siempre existirán problemas de amenazas o vulnerabilidades en los equipos informáticos, esto puede darse por un uso inadecuado o porque las personas encargadas o usuarios finales no tienen el conocimiento necesario para utilizar correctamente el hardware. Internet y el mundo digital están llenos de sitios maliciosos donde fácilmente los delincuentes informáticos pueden robar información personal, confidencial o incluso acceder con total libertad a los ordenadores para realizar cualquier actividad.

Esto deriva en que la información importante que almacenamos en las maquinas está llena de riesgos, los cuales pueden convertirse en grandes y graves problemas si no se implementan estrategias adecuadas para reducir los riesgos y posibles amenazas.

Justificación

Cuando hablamos de uso inadecuado de los equipos, podemos referirnos a los casos en los que la persona no realiza una buena protección de sus dispositivos o la empresa no tiene la seguridad adecuada para sus equipos o en sus servidores, porque normalmente las personas no le tomamos tanta importancia a la ciberseguridad por ello las empresas que se crean no tienen las precauciones necesarias para evitar problemas de esta índole.

El tener un equipo bien capacitado para poder prevenir problemas de ciberseguridad o detenerlos en el momento que este sucediendo puede marcar una enorme diferencia, pero muchas veces el presupuesto para estas situaciones es el más bajo, pensando de que esto nunca llegara a pasar, por eso les toman desprevenidos y se filtra información importante de la empresa, de dañar equipos, se pierden conexiones y todo tipo de situaciones en las que se puede estar involucrado cuando no se tiene la protección adecuada.

Marco Conceptual

Seguridad Informática: La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).

SGSI: Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información.

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

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

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

-**Do (hacer):** es una fase que envuelve la implantación y operación de los controles. -**Check (controlar):** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

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

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

Normas ISO en seguridad: 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.

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

El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico.

El Consejo Superior de Informática ha sido el encargado de elaborar la primera versión de MAGERIT, con lo que promueve su utilización como respuesta a la dependencia creciente de toda la sociedad respecto a las Tecnologías de la Información. MAGERIT se encuentra muy relacionada con la generación en la que se utilizan los medios electrónicos, informáticos y telemáticos, lo que genera grandes beneficios para los empleados y los ciudadanos, aunque también puede dar lugar a diferentes riesgos que se tienen que minimizar con medidas de seguridad que generan confianza.

MAGERIT facilita que se pueda llevar a cabo:

- 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, recudir o controlar todos los riesgos que se han identificado, pudiendo de este modo reducir al mínimo la potencialidad del riesgo.

Marco Teórico

Una de las principales preocupaciones de dueños, inversionistas, directores y empleados de las compañías es tomar las medidas de seguridad informática adecuadas para proteger los datos del negocio.

Las medidas y procedimientos de seguridad implementados de acuerdo con las políticas establecidas constituyen la parte principal del sistema de seguridad. La seguridad está diseñada y representa la principal línea de defensa para proteger los activos de TI, cuya elección es fundamental. Apropiadamente, incluir las amenazas identificadas durante la evaluación de riesgos e implementarlas de manera rentable.

Si la mayor amenaza para el sistema es el acceso remoto, es posible que no obtenga mucha conveniencia de utilizar dispositivos técnicos de control de acceso para los usuarios endulzado. Por otro lado, si la mayor amenaza es el uso no autorizado de activos para los usuarios ordinarios del sistema, es probable deben existir procedimientos estrictos de control y gestión. auditoría.

La seguridad se hará especificando un número valla protectora, ordene la selección de una variedad de formas. Combinados y concéntricos, logrando así cierta repetición asegúrese de que, si la acción falla o se infringe, la siguiente acción intermedia continúe trabajando para proteger la propiedad o los recursos. No apropiado la falla del mecanismo afecta completamente la seguridad. Algunas medidas simples se pueden implementar en muchos casos mucho más seguro que usar una báscula muy sofisticada. cobrar más cálido cuando no se puede aplicar una determinada medida por restricciones existentes, tales como: equipo insuficiente, impedir la ejecución de una acción técnica. En este caso, lo harán medidas adicionales o medidas propuestas de otro tipo garantizar un nivel adecuado de seguridad.

También cabe señalar que el uso del sentido común y la bondad la gestión es la herramienta de seguridad más adecuada. No vale la pena diseñar un sistema de medición complejo y costoso entonces supervisión más básica. Porque Ya sea un sistema de control de acceso, usuario simple un interruptor de mala calidad o descuidado puede abrir la puerta del sistema. Algunas medidas simples se pueden implementar en muchos casos mucho más seguro que usar una báscula muy compleja.
cobrar más válido cuando no se puede aplicar una determinada medida por restricciones.

Los Sistemas de Información deben preservar la confidencialidad, disponibilidad e integridad, asegurándose que la información es accesible sólo a las personas autorizadas, permitiendo proteger la información contra accesos o divulgación no autorizados. (Fernández y Álvarez, 2012 p. 20)

Por lo anterior es necesario realizar el análisis de riesgo ya que nos permite identificar las vulnerabilidades que debilitan el sistema y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Planeación de la seguridad informática en la organización.

Garantizar la prevención y detección de accidentes, ataques, daños por causas naturales, así como la existencia de medidas definidas para afrontar los desastres y lograr el restablecimiento de las actividades.

La seguridad depende, fundamentalmente, de la integridad de los individuos que conforman una organización o departamento. No existe una seguridad total y cada institución depende de su personal para lograr los niveles de seguridad

- Limitaciones de la seguridad. – Requiere personal honesto, a mayor seguridad, mayor costo y menores beneficios.
- Equilibrio entre las medidas de seguridad y los niveles de riesgo. – Mal manejo o negligencia. – Ataques deliberados.

Cuando se establece el grado de riesgo, es importante considerar primero los tipos de riesgos a los que están expuestas las instalaciones de computación. Entre los riesgos principales encontramos los accidentes causados por el mal manejo y ataques deliberados en forma de robo, fraude, sabotaje o huelga.

Toda la información que se obtenga y las decisiones que se tomen se deben documentar de manera progresiva, lo que consolida el informe final ante la dirección. Es conveniente convocar a una reunión de los directivos correspondientes para evaluar tanto los hallazgos como las recomendaciones, a fin de que se obtenga una decisión y que se apruebe un plan de acción destinado a la investigación y a la aplicación más detallada. Como se debe hacer en la planeación de revisión preliminar:

- Aplicaciones, programas y archivos específicos.
- Planes de detección y métodos para prevenir abusos o desastres.
- Prioridades, que son acciones que se requieren a corto plazo, y los elementos que se deben considerar de manera detallada a mediano y largo plazo.
- Estos pasos conducen hacia la recolección y la presentación de todos los informes necesarios para una decisión bien fundada sobre los costos y beneficios de la estrategia de seguridad en cómputo.

División de responsabilidades

1. El personal que prepara los datos no debe tener acceso a las actividades de operación.
2. Los analistas y programadores no deben tener acceso a las actividades de operación y viceversa.
3. Los operadores no deben tener acceso irrestricto a las funciones de protección de información o departamentos donde se localicen los archivos maestros.

4. Los operadores no deben tener los controles únicos del procesamiento del trabajo y se les debe prohibir que inicien las correcciones de errores.

Sistemas de control interno.

1. Verificación documentada de evidencias requiere:
2. Modificación de programas autorizada y probada.
3. Documentar desarrollo y prueba de sistema nuevo.
4. Verificar datos de los archivos, contra impresos que sean editados en el ordenador.
5. Que los datos de entrada se agrupen y revisen.
6. Se documenten los errores y se autoricen y comparen las correcciones con el material impreso por la computadora.

Alcance del análisis y evaluación de riesgos del Sistema Informático.

El proyecto abarca la evaluación de la infraestructura tecnológica que hace parte de la red LAN que actualmente está instalada en el centro de cómputo de el laboratorio de computo de la UNICAH, Se busca al desarrollar el proyecto, el mejoramiento de la seguridad informática mediante controles que permitan mitigar los riesgos y su impacto en los activos infraestructura tecnológica o componentes de la red de UNICAH, esto es, dispositivos intermedios a nivel de switchs de capa 2 y capa 3 y los routers con conexión Ethernet.

Evaluación de Riesgo

Riesgo/Valoracion		Probabilidad			Impacto		
		A	M	B	L	M	C
R1	Daño de equipos informaticos(servidores y estaciones de trabajo) por exposicion a polvo			X			X
R2	Daño de equipos informaticos(servidores y estaciones de trabajo) por exposicion altas temperaturas			X			X
R3	Daño de equipos informaticos(servidores y estaciones de trabajo) por cortocircuito en celdas de potencia electrica			X		X	
R4	Acceso de personal no autorizado a afreas restringidas	X			X		
R5	Falta de soporte por parte de los desarrolladores de software	X				X	
R6	Infeccion de virus por que se tiene el antivirus desactualizado		X			X	
R7	Acceso no autorizado a los servidores	X				X	
R8	Almacenamiento no seguro de copias de seguridad y backup del sistema	X				X	
R9	Falla en las politicas de seguridad implementadas			X	X		
R10	Modificacion de informacion confidencial	X					X

Matiz de clasificación de riesgos

	LEVE	MODERADO	CATASTROFICO
ALTO	R4	R7, R8	R10
MEDIO	R5	R6	
BAJO	R9	R3	R1, R2

Los objetivos del análisis y evaluación de riesgos de sistemas informáticos son:

*Determinar los sistemas críticos para la gestión de los riesgos, en particular los soportados en redes de datos, las amenazas que actúan sobre ellos, los niveles de riesgo y el posible impacto.

* Determinar el grado de dependencia actual y perspectivo con relación al sistema de riesgos.

* Establecer las políticas que se requieran para minimizar los riesgos sobre los bienes informáticos críticos e implementar las acciones y mecanismos que se necesiten para su prevención, detección y recuperación. *Determinar parámetros que permitan establecer niveles mínimos de disponibilidades permisibles.

* Establecer un sistema que garantice la continuidad de este estudio sobre la base de los cambios que surjan y los incidentes que se produzcan.

Tipo de servicio	Información y servicios que maneja
Servidor web	Se encargan de ejecutar la capa de presentación e interactúan el resto de elementos del back-end.
Estaciones de trabajo	Se encargan de brindar las herramientas tecnológicas y accesos a los diferentes servidores de la organización, desde aquí se realizan los diferentes desarrollos de software.

Redes de comunicación	Se encarga de proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores, entre los diferentes equipos informáticos de la compañía.
Usuarios (alumnos)	Se encarga de administrar y monitorizar el correcto funcionamiento del sistema incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo.
Instalaciones	Se encargan de salvaguardar la integridad de los activos de la compañía. al igual que protegerlos del acceso no autorizado de personal externo.
Aplicaciones	Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos dentro y fuera de la compañía, además permite comunicarse de manera asertiva con los servidores y clientes del sistema informático.
Suministro eléctrico	Se encarga de proveer alimentación eléctrica de buena calidad a todos los equipos electrónicos que conforman el sistema de información de la compañía.
Sistema de apantallamiento y puestas a tierra	Se encarga de proteger a las personas y de paso a los equipos informáticos de descargas eléctricas ocasionadas por descargas atmosféricas y corrientes.

Descripción de los activos o recursos informáticos del laboratorio.

Tipo de servicio	Características mínimas
Servidores	Intel Xeon, o AMD Opteron 2 núcleos Memoria RAM 8GB 2 discos duros de 1TB 2 tarjetas Ethernet
Estaciones de trabajo	15 Intel Core i5-4570 15 memorias RAM 8GB 15 discos duro 1TB 15 tarjetas Ethernet
Hardware	Firewall físico
Red	Router Punto de acceso 5 switchs
Software	Windows 10 Windows server 2010

Capítulo 2 Análisis de Riesgos

2.3 Identificación de amenazas y probabilidades

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

2.4 Amenazas clasificadas por su tipo y su nivel de probabilidad

Tipo	Nivel de amenazas	Descripción de Probabilidad	NP	Razón de la calificación
AI	Entrada a los Laboratorios de Cómputo	Con el sistema de control de acceso al laboratorio, se registra la entrada de las personas encargadas del lugar.	1	Hay una baja probabilidad de que otra persona sin permiso tenga el acceso a la entrada, pero en caso de que la persona autorizada pierda la tarjeta, aunque esto no ha ocurrido.
AII	Electricidad	Los equipos y servidores en los laboratorios siempre están conectados, sin embargo debe hacer una revisión en caso de que algo falle.	3	En el área hay probabilidades de que la energía eléctrica se vaya, para evitar esto hay que implementar UPS para evitar que los equipos y los servidores se dañen.
AIII	Incendio	En caso de que suceda un incendio, todos los equipos se dañan si no se tienen preparadas las seguridades y protocolos para prevenir un desastre.	1	Esto no tiene registro de que ha ocurrido eso, pero no tienen la seguridad robusta, como el extintor para evitar que el incendio empeore.

AIV	Daños por objetos que contengan agua o comida	Personas o estudiantes que llevan botes, u otra cosa.	1	Evitar llevar botes a los laboratorios de cómputos para prevenir que ocasione daños en los equipos.
V	Desastres Naturales	Lluvia, terremotos, huracanes, tsunamis, inundaciones, etc. Mencionando que estos desastres naturales pueden afectar a los laboratorios de cómputos.	2	El lugar donde están los laboratorios es seguro ya que está en la segunda planta, así que hay menos riesgo que uno de estos desastres sucedan.
VI	Daños por agua	goteras en los techos de los laboratorios, fugas o tuberías de agua reventadas.	1	Tiene techo falso que permite absorber goteras, impidiendo que las gotas de agua dañen los dispositivos.
AVII	Intromisión en la red y ataques de ingeniería social	La ingeniería social es un método para descifrar información sensible a través de la vulnerabilidad humana. Es la disciplina de sustraer información, derechos de acceso o privilegios de un sistema de información con base en la buena fe de algunos usuarios.	1	No se han presentado ataques en la seguridad de la red.
AVIII	Saqueos de equipos	El robo de equipos de cómputo en la actualidad es muy común en los laboratorios por contar equipos costosos, y la mayoría son los más atacados en el robo de equipos de cómputo porque estos últimos son los que cuentan con una gran cantidad de equipos para realizar sus actividades y posiblemente más vulnerables debido a las condiciones físicas necesarias. y las medidas de seguridad lógica no siempre están en su lugar.	1	No se han presentado robos de equipos ya que los laboratorios tiene que tener un acceso con la tarjeta. Y este tiene mayor seguridad.

AIX	Mal uso del sistema	Utilizar el software ilegal o copia de software no autorizada que este no cuenta con una correspondiente licencia. Y esto será conceptuado como mal uso.	1	En los laboratorios no se han mostrado acontecimientos sobre el mal uso del software.
AX	Fallas en la base y en las redes	Con estas fallas causan disconformidades con la disponibilidad de los servicios e impide comunicación con las otras áreas.	1	No se han presentado acontecimientos, aunque es una posibilidad de que pase.
AXI	Errores humanos	Esto puede pasar cuando una persona desconoce el uso de los sistemas o también puede ser negligencia, por ejemplo al instalar software ilegal o programas que no tienen licencias.	2	No se han presentado acontecimientos, aunque existe una posibilidad de que esto suceda.
AXII	Amenazas legales	Sucede en circunstancias las cuales se descubre que uno o varios de los equipos están utilizando software con licencias ilegales o en el peor de los casos tráfico de información personal de sus clientes o empleados	1	No se han presentado acontecimientos, aunque es una posibilidad de que pase.

Clasificamos todas las amenazas para evaluar que tan alta o que tan baja es la probabilidad de que puedan llegar a suceder

Matriz de Impacto Potencial

Tipo de Activo	Código de Amenaza	Amenaza	Impacto
Hardware	AI	Entrada a los Laboratorios de Cómputo	4
	AII	Electricidad	3
	AIII	Incendio	5
	AIV	Daños por objetos que contengan agua o comida	4
	V	Desastres Naturales	5
	VI	Daños por agua	5
	AVII	Intromisión en la red y ataques de ingeniería social	3
	AVIII	Saqueos de equipos	5
	AIX	Mal uso del sistema	4
	AX	Fallas en la base y en las redes	1
	AXI	Errores humanos	2
	AXII	Amenazas legales	1
Software	AI	Entrada a los Laboratorios de Cómputo	4
	AII	Electricidad	4
	AIII	Incendio	3
	AIV	Daños por objetos que contengan agua o comida	3
	V	Desastres Naturales	5
	VI	Daños por agua	3

	AVII	Intromisión en la red y ataques de ingeniería social	5
	AVIII	Saqueos de equipos	4
	AIX	Mal uso del sistema	4
	AX	Fallas en la base y en las redes	4
	AXI	Errores humanos	4
	AXII	Amenazas legales	5
Información	AI	Entrada a los Laboratorios de Cómputo	4
	AII	Electricidad	2
	AIII	Incendio	5
	AIV	Daños por objetos que contengan agua o comida	4
	V	Desastres Naturales	5
	VI	Daños por agua	5
	AVII	Intromisión en la red y ataques de ingeniería social	5
	AVIII	Saqueos de equipos	5
	AIX	Mal uso del sistema	4
	AX	Fallas en la base y en las redes	4
	AXI	Errores humanos	3
	AXII	Amenazas legales	4

Se listan todos los tipos de amenazas posibles y se evalúa el impacto que estas podrían tener de suceder en el laboratorio.

Riesgo Potencial (Número de amenazas por zona de riesgo y tipo de activo)

Matriz de impacto potencial

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

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

Zona de riesgo	**Hardware**	**Información**	**Software**	**Total General**
Zona B	4	3	5	12
Fallas en la base y en las redes	1	1	1	3
Amenazas legales	1	1	0	2
Errores humanos	1	0	1	2
Daños por objetos que contengan agua o comida	1	1	1	3
Incendio	0	0	1	1
Saqueos de equipo	0	0	1	1
Zona M	5	4	3	12
Errores humanos	1	0	0	1
Daños por agua	0	0	1	1

Desastres Naturales	1	1	1	3
Incendio	1	1	0	2
Intromisión en la red y ataques de ingeniería social	1	0	0	1
Electricidad	0	1	0	1
Saqueos de Equipos	1	1	0	2
Amenazas Legales	0	0	1	1
Zona A	2	3	1	6
Electricidad	1	1	0	2
Errores humanos	0	1	0	1
Entrada a los Laboratorios de Cómputo	1	1	1	3
Zona E	2	3	4	9
Daños por agua	1	1	0	2
Mal uso del sistema	1	1	1	3
Electricidad	0	0	1	1
Intromisión en la red y ataques de ingeniería social	0	1	1	2
Errores humanos	0	0	1	1

Este es simplemente un conteo general de los datos que encontramos en el siguiente cuadro, por ejemplo.
Fallas en la base y en las redes, podemos ver que se encuentra tanto en hardware, información y software porque están marcados con un uno y en las 3 áreas se encuentran en la zona de riesgo B.
Cuando ese problema no se encuentra en una de estas áreas entonces lo marcamos con un 0, al final simplemente se suma la cantidad de 1s que hubo por fila y luego la suma total por zona

Riesgo Potencial

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

Matriz de Riesgo Potencial

Tipo de Activo	Código de Amenaza	Amenaza	Impacto	Nivel de Probabilidad	Riesgo potencial	Zona de Riesgo
Hardware	AI	Entrada a los Laboratorios de Cómputo	4	2	8	A
	AII	Electricidad	3	3	9	A
	AIII	Incendio	5	1	5	M
	AIV	Daños por objetos que contengan agua o comida	4	1	4	B
	V	Desastres Naturales	5	1	5	M
	VI	Daños por agua	5	2	10	E
	AVII	Intromisión en la red y ataques de ingeniería social	3	2	6	M

	AVIII	Saqueos de equipos	5	1	5	M
	AIX	Mal uso del sistema	4	3	12	E
	AX	Fallas en la base y en las redes	1	1	1	B
	AXI	Errores humanos	2	3	6	M
	AXII	Amenazas legales	1	1	1	B
Software	AI	Entrada a los Laboratorios de Cómputo	4	2	8	A
	AII	Electricidad	4	3	12	E
	AIII	Incendio	3	1	3	B
	AIV	Daños por objetos que contengan agua o comida	3	1	3	B
	V	Desastres Naturales	5	1	5	M
	VI	Daños por agua	3	2	6	M
	AVII	Intromisión en la red y ataques de ingeniería social	5	2	10	E
	AVIII	Saqueos de equipos	4	1	4	B
	AIX	Mal uso del sistema	4	3	12	E
	AX	Fallas en la base y en las redes	4	1	4	B

	AXI	Errores humanos	4	3	12	E
	AXII	Amenazas legales	5	1	5	M
Información	AI	Entrada a los Laboratorios de Cómputo	4	2	8	A
	AII	Electricidad	2	3	6	M
	AIII	Incendio	5	1	5	M
	AIV	Daños por objetos que contengan agua o comida	4	1	4	B
	V	Desastres Naturales	5	1	5	M
	VI	Daños por agua	5	2	10	E
	AVII	Intromisión en la red y ataques de ingeniería social	5	2	10	E
	AVIII	Saqueos de equipos	5	1	5	M
	AIX	Mal uso del sistema	4	3	12	E
	AX	Fallas en la base y en las redes	4	1	4	B
	AXI	Errores humanos	3	3	9	A
	AXII	Amenazas legales	4	1	4	B

En este cuadro lo que haces es que misma mides el nivel de impacto y de probabilidad, en base a eso sacas el riesgo potencial y la zona de riesgo.
Riesgo potencial es igual a impacto X nivel de probabilidad

y la Zona de riesgo la sacas según el cuadro de la diapositiva #26 en donde si el Riesgo potencial esta entre 1 y 4 entonces es Zona de riesgo B, de 5 a 6 entonces la zona de riesgo es M y así sucesivamente

Salvaguardas o controles existentes

Nivel	Descripción de la efectividad del control
1	Es probable la falla en todo caso de ocurrencia de la amenaza o no existe un control
2	Es parcialmente eficaz y podría funcionar la mayor parte del tiempo
3	Garantiza un eficaz funcionamiento en cada caso de ocurrencia de las amenazas

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

AI. Amenaza de entrada a los laboratorios de computo

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Hardware	Robo del equipo	Deberían implementar un nuevo tipo de acceso en el que sea biométrico	administrativa	SI	3	Se establece por medio de protocolos de seguridad
	Recursos insuficientes para la seguridad física	Hacer una inversión requerida para mejorar la seguridad biométrica	administrativa	SI	3	Mantiene bajo la mejora del funcionamiento y la seguridad de los equipos
	Control de acceso inadecuado - sala	Se deberá incorporar nuevos soportes de seguridad cada mes	prevención	PARCIAL	2	Se cuenta con la protección de firewall con protocolos
Software Información	Robo de la información	Se deberá cambiar la contraseña y clave de acceso de los usuarios permitidos cada mes	prevención	PARCIAL	2	Con protocolos de mejora a la seguridad estableciendo perímetros estrictos

	Distorsión de la información	Se mantendrá una copia de la copia de la información	prevención	PARCIAL	3	Al resguardar la información será complejo su distorsión

AII. Amenaza de electricidad

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Hardware	Falta de personal para mantenimiento y control del equipo	Al tener bajo personal se debe adquirir al menos 2 empleados dedicado al mantenimiento de los equipos	administrativo	SI	3	Contratación de personal evitara errores de la electricidad
	Fallas eléctricas en la zona	Ampliar los métodos de protección para que no afecte a los equipos como ser una planta eléctrica	administrativo	NO	1	Se deberá aplicar un sistema que proteja al personal y al equipo
	Falta de un sistema de corriente regular	Aplicar protección de circuitos	administrativo	SI	2	Al tener un sistema de regulación se evita que el fator humano este expuesto a que un bastidor tenga un alto voltaje

AIII. Amenazas de Incendio

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Hardware	Inadecuado manejo de los equipos de seguridad contra incendios	Capacitar a los empleados para el manejo de este equipo	administrativo	SI	3	Se encuentra solo un cilindro inflamable
Hardware, software, información	Equipos de circuito de baja calidad	El material contra incidíos deberá resguardarse en una zona lejana a estos	minimizadores	SI	3	El laboratorio se encuentra lejos de cualquier riesgo a un cortocircuito

	Ausencia de equipo contra incendios	Los equipos contra incendios se proporcionarán y se colocarán adecuadamente	minimizadores	PARCIAL	2	No existe un sistema de detección de humo
	Falta de un backup en un lugar diferente	Ubicar los backup en lugares diferentes	Recuperación	NO	1	Se encuentran backup
Hardware, información	Ausencia de control de temperatura y humedad	Sistema de monitoreo para la temperatura y la humedad	Monitorización	PARCIAL	2	Se está implementando los dos sistemas de seguridad para la regulación de la temperatura y humedad
		Deben ser monitoreadas	monitorización	PARCIAL	2	

AIV. Amenaza por desastres naturales

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Hardware, información	Capacidad baja en la construcción del edificio	Debe ser resistente a fugas de agua y terremotos	Minimizadoras	SI	3	Los edificios no cumplen con los requerimientos
	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones		SI	3	El laboratorio se encuentra en el segundo piso
	Ausencia de control de temperatura y humedad	Deben ser monitoreadas	monitorización	PARCIAL	2	Se está implementando los dos sistemas de seguridad para la regulación de la temperatura y humedad
Hardware	Estructura de la construcción y techos de baja calidad	Se debe implementar una protección apropiada contra terremotos	Minimizadores	SI	3	El edificio, aunque es nuevo no cuenta con regulaciones antisísmicas
	Ubicado en una zona de alto nivel sísmico			SI		
	Falta de mecanismos alternos en caso de destrucción total	Desarrollar e implementar planes para mantener o	Administrativo	PARCIAL	2	

		restaurar las operaciones y asegurar la información				

AV. Amenaza de daños por agua

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Hardware, información	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones	Minimizadores	SI	3	El laboratorio de computo esta en el segundo piso
	Sistema de drenaje débil	Se debe implementar protección contra de inundaciones y fugas de agua	Minimizadores	SI	3	No se cuenta con sistema de drenaje

AIX. Amenaza por mal uso del sistema

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Software	Falta de medidas de restricción contra acceso no autorizado	Acceso a la información y las funciones del sistema solo a los usuarios de este	Prevención	PARCIAL	2	Se define que los únicos autorizados a este son los catedráticos que dan clases.
	Ausencia de conciencia de seguridad	Se debe impartir capacitaciones a los empleados para que cumplan con el manejo de la información	Concienciación	PARCIAL	1	No se establece un plan de capacitación frente a seguridades de la información
	Insuficiente capacitación a los usuarios			NO	1	

AXI. Amenaza por errores humano

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Hardware, información	Falta de una capacitación	Deben recibir capacitaciones sobre conocimientos actualizados de la seguridad de la información	concienciación	NO	1	Hay actividades de entrega para los roles. No se cuenta con un plan de capacitación
Información	No hay personal para los roles y la responsabilidad de la seguridad de la información	Los roles deben ser definidos para un mejor manejo de la información	PARCIAL	PARCIAL	2	Se cuenta con la política de seguridad en la que se definen los roles

AXII. Amenazas Legales

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Control Implementado	Eficacia del control	Comentarios
Software, información	Reglamento de los controles	Los controles deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones	Prevención	NO	1	No existe una implementación
	Comprensión insuficiente de las nuevas leyes y normas sobre las TI	Se deben establecer políticas que se ejecuten bajo las normas y leyes establecidas	Administración	PARCIAL	2	No existe política de tratamiento de base de datos
	Insuficientes procedimientos para el	Implementar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales	Administración	PARCIAL	2	Al contrato se le agregaron normas para el cumplimiento

	cumplimiento de la propiedad intelectual					
	No hay protección y privacidad de la información	Se deberá asegurar la protección de datos y la privacidad como requisito en la legislación		NO	1	No hay un procedimiento para el manejo de la información personal

Matriz de impacto residual y riesgo residual

AI. Amenaza de entrada a los laboratorios de computo

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Robo del equipo	Deberían implementar un nuevo tipo de acceso en el que sea biométrico	administrativa	**3**	**5**	**1.7**	**1**	**1.7**	**M**
	Recursos insuficientes para la seguridad física	Hacer una inversión requerida para mejorar la seguridad biométrica	administrativa	**3**	**4**	**1.3**	**2**	**2.6**	**M**
	Control de acceso inadecuado - sala	Se deberá incorporar nuevos soportes de seguridad cada mes	prevención	**2**	**4**	**2**	**2**	**4**	**A**
Software Información	Robo de la información	Se deberá cambiar la contraseña y clave de acceso de los usuarios permitidos cada mes	prevención	**2**	**4**	**2**	**1**	**4**	**B**
	Distorsión de la información	Se mantendrá una copia de la copia de la información	prevención	3	**4**	**1.3**	**3**	**3.9**	**E**

AII. Amenaza de electricidad

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Falta de personal para mantenimiento y control del equipo	Al tener bajo personal se debe adquirir al menos 2 empleados dedicado al mantenimiento de los equipos	administrativo	3	3	1	3	3	A
	Fallas eléctricas en la zona	Ampliar los métodos de protección para que no afecte a los equipos como ser una planta eléctrica	administrativo	1	3	3	3	9	A
	Falta de un sistema de corriente regular	Aplicar protección de circuitos a	administrativo	2	3	1.5	3	4.5	A

AIII. Amenazas de Incendio

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Hardware	Inadecuado manejo de los equipos de seguridad contra incendios	Capacitar a los empleados para el manejo de este equipo	administrativo	3	5	1.7	1	1.7	M
Hardware, software, información	Equipos de circuito de baja calidad	El material contra incidíos deberá resguardarse en una zona lejana a estos	minimizadores	3	5	1.7	1	1.7	M
	Ausencia de equipo contra incendios	Los equipos contra incendios se proporcionarán y se colocarán adecuadamente	minimizadores	2	5	2.5	1	2.5	M

	Falta de un backup en un lugar diferente	Ubicar los backup en lugares diferentes	Recuperación	1	3	3	1	3	B
Hardware, información	Ausencia de control de temperatura y humedad	Sistema de monitoreo para la temperatura y la humedad	Monitorización	2	5	2.5	1	2.5	M
		Deben ser monitoreadas	Monitorización	2	5	2.5	1	2.5	M

AIV. Amenaza por desastres naturales

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Hardware, información	Capacidad baja en la construcción del edificio	Debe ser resistente a fugas de agua y terremotos	Minimizadoras	3	5	1.7	1	1.7	M
	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones	Minimizadoras	3	5	1.7	1	1.7	M
	Ausencia de control de temperatura y humedad	Deben ser monitoreadas	monitorización	2	5	2.5	1	2.5	M
Hardware	Estructura de la construcción y techos de baja calidad	Se debe implementar una protección apropiada contra terremotos	Minimizadores	3	5	1.7	1	1.7	M
	Ubicado en una zona de alto nivel sísmico		Minimizadores		5	1.7	1	1.7	M
	Falta de mecanismos alternos en caso de destrucción total	Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la información	Administrativo	2	5	2.5	1	2.5	M

AV. Amenaza de daños por agua

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Hardware, información	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones	Minimizadores	3	5	1.7	2	3.4	E
	Sistema de drenaje débil	Se debe implementar protección contra de inundaciones y fugas de agua	Minimizadores	3	5	1.7	2	3.4	E

AIX. Amenaza por mal uso del sistema

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Software	Falta de medidas de restricción contra acceso no autorizado	Acceso a la información y las funciones del sistema solo a los usuarios de este	Prevención	2	4	2	2	4	A
	Ausencia de conciencia de seguridad	Se debe impartir capacitaciones a los empleados para que cumplan con el manejo de la información	Concienciación	1	4	4	3	12	E
	Insuficiente capacitación a los usuarios			1	4	4	3	12	E

AXI. Amenaza por errores humano

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Hardware, información	Falta de una capacitación	Deben recibir capacitaciones sobre conocimientos actualizados de la seguridad de la información	concienciación	1	2	2.00	3	6.00	M
Información	No hay personal para los roles y la responsabilidad de la seguridad de la información	Los roles deben ser definidos para un mejor manejo de la información	administrativo	2	4	2.00	1	2.00	A

AXII. Amenazas Legales

Activos Afectados	Vulnerabilidades	Controles	Tipo de control	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Riesgo residual	Zona de riesgo residual
Software, información	Reglamento de los controles	Los controles deben ser utilizados en conformidad con todos los acuerdos, leyes y regulaciones	Prevención	1	5	5.00	1	5.00	M
	Comprensión insuficiente de las nuevas leyes y normas sobre las TI	Se deben establecer políticas que se ejecuten bajo las normas y leyes establecidas	Administración	2	4	2.00	1	2.00	B
	Insuficientes procedimientos para e	Implementar los procedimientos apropiados	Administración	2	5	2.5	1	2.5	M

	cumplimiento de la propiedad intelectual	para asegurar el cumplimiento de las restricciones legales							
	No hay protección y privacidad de la información	Se deberá asegurar la protección de datos y la privacidad como requisito en la legislación	Administración	**1**	**4**	**4**	**1**	**4**	**B**

Capítulo 3 Gestión de Riesgos

Comunicación del riesgo y recomendaciones

Riesgo		Recomendación
1	Entrada a los Laboratorios de Cómputo	Se puede controlar el acceso a los laboratorios mediante claves o tarjetas de seguridad para cada integrante del personal autorizado
2	Electricidad	Utilizar baterías UPS para evitar que el equipo se apague bruscamente y pueda dañar uno de los aparatos del equipo
3	Incendio	Colocar mínimo un extintor en cada laboratorio, de fácil acceso a el usuario en caso de emergencia, así como alarmas contra incendios
4	Daños por objetos que contengan agua o comida	Prohibir determinantemente el acceso de comidas dentro del laboratorio de computo
5	Desastres Naturales	Tener un fondo de ahorros en caso de desastres, así como también respaldo de información de todo el equipo, ya sea en la nube o discos duros externos que se coloquen en un lugar seguro
6	Daños por agua	Revisar de que no exista ningún tipo de filtración de agua dentro de la instalación, así como evitar el ingresar con agua potable dentro del laboratorio
7	Intromisión en la red y ataques de ingeniería social	Tener un buen equipo capacitado para este tipo de situación a disposición para el laboratorio
8	Saqueos de equipos	Colocar alarmas contra robos en caso de que alguien no autorizado acceda, instalar cámaras y de ser posible contratar vigilancia privada para cuidar el equipo
9	Mal uso del sistema	Esto puede resolverse con capacitaciones para el personal, así como también un fácil acceso a alguien que tenga el conocimiento a quien puedan comunicarse en caso de problemas con el sistema
10	Fallas en la base y en las redes	Debe de mantenerse un respaldo de base de datos en físico en caso de que el sistema falle o que la base principal este teniendo problemas

11	Errores humanos	Es necesario que haya un técnico asignado a el laboratorio para poder controlar ese tipo de problemas, así como también una buena capacitación a el personal
12	Amenazas legales	Utilizar siempre equipo nuevo y de calidad, guardando comprobantes de las compras realizadas, también de ser necesario comprar todas las licencias de software que se vayan a utilizar o solo usar software libre dentro del laboratorio

Para los riesgos ubicados en las zonas baja (B) y media (M), se recomienda aceptarlos, siempre y cuando exista una monitorización continua de los mismos.
Para los riesgos ubicados en las zonas alta (A) y extrema (E), se recomienda que se lleve a cabo un tratamiento inmediato.

Tratamiento de Riesgos

Riesgo/Valoración		Probabilidad			Impacto			Tratamiento de riegos (Asumir, Evitar, Reducir, Mitigar o Trasferir)
		A	M	B	L	M	C	
R1	Daño de equipos informáticos (Servidores y estaciones de trabajo) por exposición a polvo			x			x	**Evitar:** Uso de papel en los servidores o materiales similares **Reducir:** El ingreso de materiales que puedan ocasionar polvo a las instalaciones. **Mitigar:** Mantenimiento más frecuente **Compartir:** Iniciar proceso al encargado de mantenimiento y limpieza por incumplimiento de obligaciones **Transferir:** No aplica
R2	Daño de equipos informáticos(servidores y estaciones de trabajo) por exposición a altas temperaturas			x			x	**Evitar:** Uso de objetos que generen calor en el laboratorio **Reducir:** Mantener los dispositivos en áreas donde estén expuesto a las altas temperaturas. **Mitigar:** Controles de mantenimiento más frecuentes **Trasferir:** No aplica
R3	Daño de equipos informáticos(servidores y estaciones de trabajo) por cortocircuito en celdas de potencia eléctrica			x		x		**Evitar:** Evitar el uso de los servidores mientras persista el problema **Reducir:** Usos de conectores que no estén verificados por los técnicos **Mitigar:** Asegurar el cableado de las celdas **Compartir:** Iniciar un análisis para ver los responsables de esta falla **Transferir:** Hacer efectivo las pólizas de cumplimiento por falta de atención del personal encargado
R4	Acceso de personal no autorizado a áreas restringidas	x			x			**Evitar:** Acceso de personal que no sea del área **Reducir:** Reducir las negligencias del personal de seguridad ene l área **Mitigar:** Control de mantenimiento **Compartir:** No aplica **Transferir:** Credenciales a ningún personal no autorizado

R5	Falta de soporte por parte de los desarrolladores de software	x				x		**Evitar:** Poco manuales de soporte **Reducir:** Fallos en los servidores y equipos informáticos **Mitigar:** Asegurar un buen desarrollo del software **Compartir:** Iniciar un proceso disciplinario o sancionario con los desarrolladores de software **Transferir:** Hacer efectiva las políticas de cumplimiento con los desarrolladores de software
R6	Infección de virus por que se tiene el antivirus desactualizado		x			x		**Evitar:** Evitar el ingreso de dispositivos USB en los computadores **Reducir:** Navegación o descarga de programas en línea **Mitigar:** Actualizar inmediatamente los antivirus **Compartir:** Reportar al personal de mantenimiento de las computadoras **Transferir:** No aplica
R7	Acceso no autorizado a los servidores	x				x		**Evitar:** Acceso de personal que no sea del área de servidores **Reducir:** Reducir las negligencias del personal de seguridad en el área de servidores **Mitigar:** Control de seguridad **Compartir:** No aplica **Transferir:** Credenciales a ningún personal no autorizado a los servidores
R8	Almacenamiento no seguro de copias de seguridad y backup del sistema	x				x		**Evitar:** Evitar el uso de dispositivos de trasferencia de datos como USB o discos extraíbles si no es un personal autorizado **Reducir:** Fallos en la seguridad del almacenamiento de backups **Mitigar:** Asegurar la el correcto trabajo del equipo de seguridad de datos **Compartir:** Reportar los problemas con el equipo de seguridad de datos **Transferir:** No aplica

R9	Falla en las políticas de seguridad implementadas			x	x			**Evitar:** Paralizar el sistema de control de seguridad de las licencias implementadas **Reducir:** Este tipo de problemas por parte de los encargados de seguridad **Mitigar:** Sancionar al equipo de seguridad **Compartir:** No aplica Transferir: Problema a los encargados de seguridad
R10	Modificación de información confidencial	x					x	**Evitar:** Evitar el acceso a información de personal no autorizado **Reducir:** Reducir la vulnerabilidad al acceso a información confidencia **Mitigar:** Tomar medidas drásticas con el encargado de la información confidencial en el laboratorio **Compartir:** Con personal de seguridad de la información **Transferir:** No aplica

Costos en Seguridad Informática

Tipo de Recurso	Descripción del recurso	Valor mensual	Valor anual
Recurso Humano	Administrador IT	L 10,000.00	L 120,000.00
	Consultorías especialistas en seguridad informática	L 10,000.00	L 120,000.00
	Técnico en sistemas	L 10,000.00	L 120,000.00
Recurso tecnológico	Hardware: Computadoras, puntos de red, switches, unidades CRAC (unidades de aire acondicionado)	L 70,000.00	L 840,000.00
	Software: Aplicaciones utilizadas para el manejo de los estudiantes dentro de las clases, conexiones e implementación de plataforma tecnológica.	L 15,000.00	L 180,000.00

	Comunicaciones: Firewall, antivirus, tipo de conexión a internet.	L 7,000.00	L 84,000.00
			L 1,464,000.00

Conclusiones y Recomendaciones

El Laboratorio de cómputo de esta institución está bien implementado cuenta con un sistema de climatización que logra suplir con las necesidades que este presenta, las computadoras en su mayoría se encuentran en buen estado, con un mantenido correctivo constate, se encuentran limpias y protegidas de polvo, humo o partículas que puedan dañar los discos duros o diversos componentes, existen fallas a nivel de software las cuales pueden fácilmente solucionadas.

Para ello recomendamos

- Tomar medidas en cuanto a los fallos eléctricos que ocurren en la zona ya que esto puede ocasionar el daño total de los equipos puede ser instalación de planta para el laboratorio o baterías que guardan energía para realizar el correcto apagado de los equipos.

- Instalar un antivirus moderno que tenga su licencia vigente en los dispositivos, así como mantenerlo actualizado para poder proteger los datos de virus y otros malware.

- Además, es importante que los usuarios de estos sean conscientes de la importancia de ser selectivos a la hora de instalar aplicaciones, visitar sitios en internet, abrir correos electrónicos, y otras situaciones riesgosas para la seguridad de la información.

- Verificar los dispositivos que se conectarán a los ordenadores como ser celulares, memorias o cables USB antes asegurarse que estos no estén infectados de algún virus.

Bibliografías

Amutio Gómez, ,. A., Candau, J., & Mañas, J. A. (2012). *MARGERIT version 3.0.* Madrid, España: Gobierno de España. [consultado de enero a marzo de 2020], disponible en: https://administracionelectronica.gob.es/pae_Home

Amutio Gómez, ,. A., Candau, J., & Mañas, J. A. (2012). *MARGERIT II version 3.0.* Madrid, España: Gobierno de España. [consultado de enero a marzo de 2020], disponible en: https://administracionelectronica.gob.es/pae_Home

Amutio Gómez, ,. A., Candau, J., & Mañas, J. A. (2012). *MARGERIT III version 3.0.* Madrid, España: Gobierno de España. [consultado de enero a marzo de 2020], disponible en: https://administracionelectronica.gob.es/pae_Home