UNIVERSIDAD CATÓLICA DE HONDURAS

“Nuestra Señora Reina de la Paz”

Asignatura:

Seguridad Informática y Gestión de Riesgos

Grupo:

8

Integrantes:

Carlos Alvarado Osorto

Olman Martinez

Kevin Lopez

Catedrático:

Lic. Patricia Medina

Tema:

Propuesta Análisis y Evaluación de riesgo Entregable

Fecha:

10/6/2022

Introducción

El Informe a presentar corresponde a lo adquirido e investigado en la clase de Seguridad Informática y Riesgo. Con respecto a la Metodología de MAGERIT. Como correspondencia nos tocará evaluar el posible riesgo, oportunidades y ventajas que pueda tener la empresa.

La seguridad informática en las empresas es grande los posibles defecto que puede llegar a tener a futuro e incluso en el presente pueden denotar un gran problema en dado caso que la información de la empresa sea filtrada ya sea de clientes o cuentas bancarias.

Se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas.

Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

Teniendo en cuenta la información, definición y metodología a usar. Los principales beneficios que pueden llegar a tener la empresa son comparados como ventajas sobre otras empresas.

Objetivo General

Poder buscar e implementar los datos obtenidos en clases e investigaciones previas. La base que planteamos es desarrollar un análisis de riesgo de la empresa Olancho Net. Con la información obtenida poder ver si el análisis puede sacar pros y contras en las medidas de seguridad. De poder descubrir los pros que tiene la empresa sería poder mejorar su sistema de seguridad ya sea intangible o físico. En el caso de tener contras poder tener una solución de la misma e implementar cual sea los beneficios para la empresa y eficaz.

Objetivos Específico

- Poder implementar la metodología MAGERIT con respecto a poder aprovechar las ventajas que esta tiene a favor de la empresa.
- Tomar en cuenta cuales son los activos de la empresa y que estos sean usados adecuadamente.
- Justificar por qué un análisis de riesgo es requerido en una empresa y cómo se puede desarrollar en el ámbito laboral.
- Como la empresa se puede desenvolver mejor, si las instalaciones de la empresa se encuentran en las condiciones adecuadas.
- Prevenir cualquier tipo de interrupción en el sistema de seguridad de la compañía.

Planteamiento del Problema

La seguridad informática en la década de los 80 y 90 formó parte de una salvación para distintas empresas. Ahora en día la tecnología avanza y los mismos problemas que la empresa puede llegar a tener es igual por eso en el ámbito que tiene que ver con la protección de la infraestructura informática y/o telemática y toda la información contenida en ella. Dentro de esta área se incluyen: cualquier tipo de software como bases de datos o archivos, hardware, redes de ordenadores y aquello que conlleve información confidencial en un medio informático.

Al mismo tiempo, el volumen de amenazas y la amplia gama de de aplicaciones adoptadas por los usuarios corporativos también incluyen nuevos problemas en la gestión eficiente de los recursos de la red.

Para hacer frente a este escenario, en condiciones adecuadas, las organizaciones deben contar herramientas para dar seguimiento a su entorno de TI, así como contar con el apoyo de especialistas que trabajan constantemente para mantener las configuraciones bien ajustadas a las necesidades de protección y rendimiento de la red.

Nosotros con los previos estudios y análisis tendremos que buscar las posibles vulnerabilidades que puede llegar a tener una empresa. La constante información que se filtra ilegalmente en el mercado cibernético es grande. Por eso debemos regirnos bajo los estándares de calidad.

Los diversos problemas que pueden llegar a las empresas es de día a día. ya sea si es el ámbito de hardware y software o poder burlar las entradas de seguridad, de llegar a burlar las defensas dejaría el sistema de la empresa vulnerable a posibles ataques o robos.

Justificación

Este proyecto será necesario en llevar a cabo para mejorar la seguridad informática de la empresa Olancho Networks que actualmente no presentan en una manera demasiado amplia con respecto a la seguridad de software.

Este proyecto ayudará a la identificación de posibles amenazas y proporcionará posibles soluciones a estas amenazas al igual que abrir más puertas a la empresa para poder utilizar mejores prácticas en casos de seguridad.

Uno de los beneficios que tendrá la realización de este proyecto es la mejora en la productividad en la empresa, en el apartado de ciberseguridad de sus datos, transacciones con sus clientes, mejor seguridad y confiabilidad por parte de sus clientes y socios al igual que atraer más clientes al aumentar de manera positiva la imagen de la empresa.

La comunicación con la empresa no es un problema a la hora de conseguir información relevante para ayudar a esta empresa ya que el contacto de nuestro miembro del grupo tiene una excelente relación con uno de sus empleados.

Marco Conceptual

Seguridad Informática

El proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

Riesgos

Los riesgos son la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. El nivel de riesgo depende del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que estas puedan tener en el funcionamiento de la organización.

Análisis de riesgos

Esta **metodología de gestión de riesgos** también forma parte del análisis inicial. Se utiliza para identificar posibles riesgos cuando el proyecto apenas está comenzando. El primer paso en el análisis preliminar de riesgos es identificar todas las actividades que

forman parte de un proyecto o de un proceso, intentando reconocer los posibles problemas que se puedan enfrentar en cada fase.

Metodología MAGERIT

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Amenazas

Una amenaza se puede definir entonces como un evento que puede afectar los activos de información y están relacionadas con el recurso humano, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el fluido eléctrico.

Marco teórico

La Empresa con la que Trabajaremos Este Periodo Académico en la Clase de Seguridad Informática y Gestión de Riesgos Tiene Como Nombre Llama Olancho Networks es una Empresa de Internet Ubicada en la Col. Santo Calix , Juticalpa, Honduras. se Pueden Comunicar al celular 9501-5187 y por correo electrónico a ventas@olanchonet.com

Nuestra historia

El 18 de abril del 2014 estando en Guarizama recibí una llamada de mi jefe para enviar unos reportes en la cual necesitaba acceso a internet de inmediato para generar reportes desde el servidor.

Ese día dejé de estar en un evento familiar importante, para conducir hasta Juticalpa y enviar lo que me habían pedido.

De regreso se me ocurrió que con la experiencia que tenía podría instalar un enlace de internet para servir a mi familia y los centros educativos que atendí en mi infancia y adolescencia.

Al día siguiente juntos a mis hijos, sobrino y cuñado emprendimos viaje hasta un cerro para confirmar que había línea vista hasta una montaña en Juticalpa y así empezar la búsqueda de recursos y materiales necesarios para instalar el proyecto.

Junto a mis hermanas y mi esposa empezó el gran sueño y con la ayuda de amigos, empresas se logró el enlace inicial el 5 marzo del 2015 hasta el municipio de Guarizama.

Misión

Con infraestructura en torno a Fibra GPON y tecnología inalámbrica, brindamos servicio de Internet Residencial y Pyme ilimitado; garantizando la calidad de servicio y con una atención personalizada.

Visión

Innovación constante para siempre estar competitivos y con el compromiso de llegar a todos los lugares rurales como urbanos del departamento de Olancho y más allá.

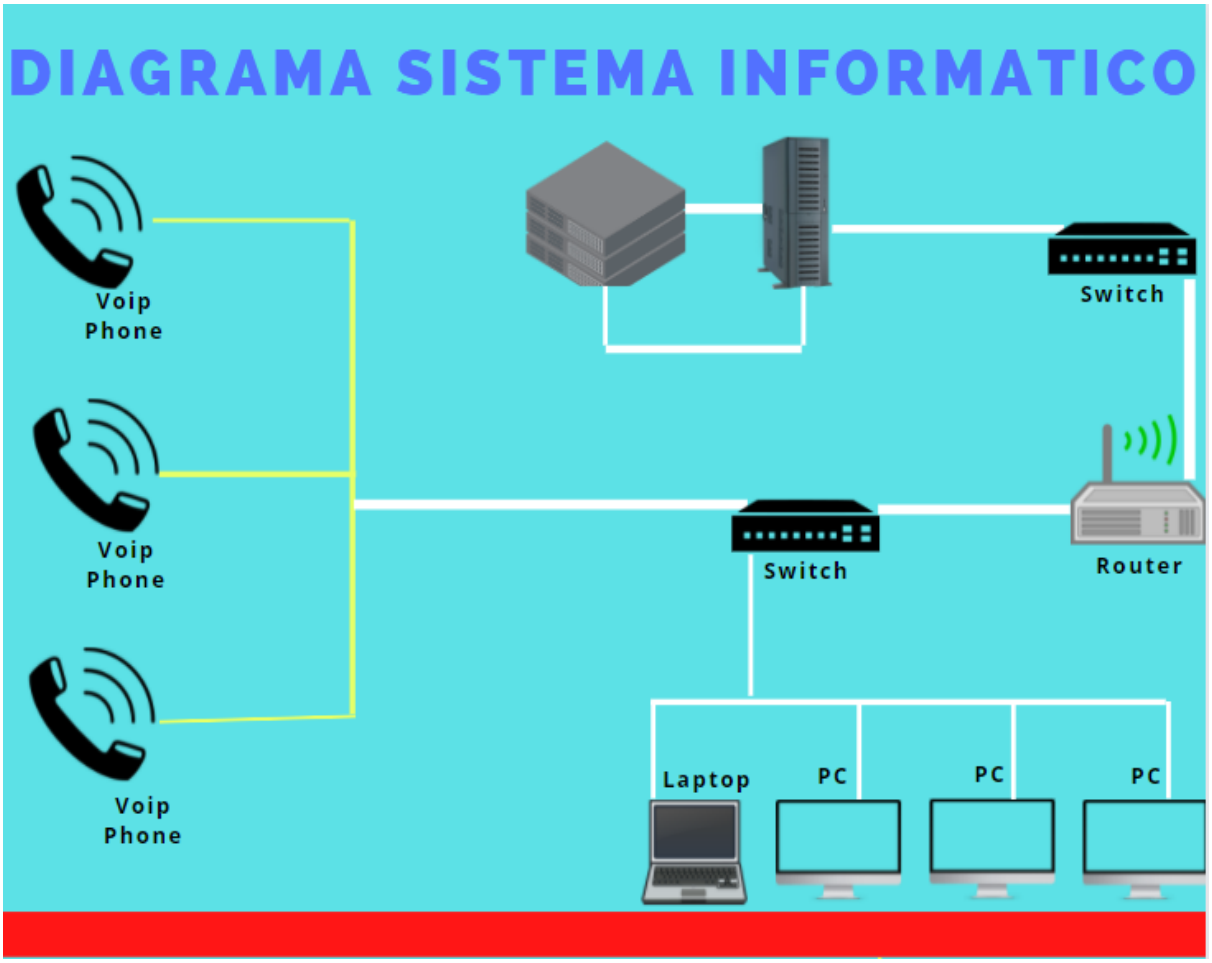
Esta Empresa Cabe recalcar que Cuenta con una Gran Variabilidad de Servicios Como:

- Redes Cableado estructurado
- Sistemas de video vigilancia
- Redes fibra óptica
- Radiocomunicación
- Casa y Oficina Inteligente
- Sistemas Telefónicos VoIP

Y esta es Su Área:Salamá, Honduras · Jano, Honduras · Guata, Honduras · Guarizama, Honduras · Manto, Honduras · San Esteban, Honduras · San Francisco de la Paz, Honduras · Silca, Honduras · Gualaco, Honduras · Juticalpa, Honduras

Como Aporte Según lo que Investigamos Toda Empresa que se Dedique al Rubro del Internet y las Tecnologías de la Información debe estar a la Vanguardia y Actualizados porque en la Actualidad Cada dia que Pasa hay más Procesos de Cambio está Para nosotros es una Ventaja fundamental Para garantizar de esta Manera el Éxito de la

Empresa y no olvidar Siempre Preservar un desempeño exitoso en el trabajo y como la Empresa lo Utiliza Como lema “Acercando al Mundo un paso con la Tecnología”.
Y no olvidar Nunca los principios de la Seguridad Informática Resguardar y Proteger los Activos de la Información y Nunca dejar de la Mano la Confidencialidad,La Integridad y la Disponibilidad.



1. Planificación

1.1 Planeación de la seguridad informática en la organización

Lo que vamos a realizar es un análisis de las posibles desventajas que puede llegar a tener la empresa. como primer punto definir los software que se utilizan y los hardware. Ya teniendo el conocimiento requerido tendremos que verificar si están en la condición óptima para lo que requiere la empresa. los datos que tenemos que evaluar serían los ataques si tiene la empresa las amenazas que podría enfrentar con el robo de información.

En dado caso que la empresa lo requiera se podrá realizar una actualización de los sistemas de software o hardware.
Garantizar un acceso y uso seguro de la información registrada en equipos informáticos, así como del propio sistema, protegiéndolos posibles ataques y amenazas, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior es fundamental para cualquier organización.

Es un tema que está a la orden del día, en el que es necesario fortalecer la protección de las amenazas en la nube e invertir más en seguridad informática. El trabajo remoto ha llegado para quedarse y la ciberseguridad se ha convertido en prioritaria ante los ataques informáticos. ¿Te interesa? Presta atención al siguiente artículo y fórmate a nivel experto con el Máster en Seguridad Informática e Informática Forense.

1.2 Alcance del análisis y evaluación de riesgos del sistema informático

El alcance para el análisis son lograr evaluar los niveles de seguridad que maneja la empresa Olancho Networks ubicados en Olancho, 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, esto es, dispositivos intermedios a nivel de switches de capa 2 y capa 3 y los routers con conexión Ethernet. En los resultados esperamos obtener las diferentes amenazas que pueden afectar a la empresa para así poder implementar un plan de gestión de riesgos para evitar toda amenaza que pueda presentarse a futuro y así poder evitar grandes pérdidas.

1.3 Objetivos del análisis

1. 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.
2. Establecer un sistema que garantice la continuidad de este estudio sobre la base de los cambios que surjan y los incidentes que se produzcan.
3. Analizar el tiempo, esfuerzo y recursos necesarios para atacar los problemas
4. Determinar e identificar los riesgos y debilidades.
5. Proteger la información de la empresa, así como su integridad.
6. Aumentar las medidas de seguridad de la Empresa.

Análisis de Riesgos

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

Activo	Descripción
CPU	En el Servidor también conocido como el Procesador es lo que interpreta y ejecuta Instrucciones, datos de procesamiento y tareas de rendimiento como mostrar páginas web, ejecutar consultas de la base de datos y ejecutar otros comandos de programas y computación.
Servidor Torre	Un servidor de torre es muy similar a una computadora de escritorio, ya que está compuesto por un gabinete, tarjeta madre, procesador, memoria ram, disco duro, fuente de poder y sistema operativo, pero cada uno de estos elementos cuenta con un rendimiento superior al de una computadora ordinaria.
Router	Enrutador o en caminador es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y el dispositivo de destino.
Servidor Rack	Es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para el ancho están normalizadas para que sean compatibles con equipamiento de distintos fabricantes, y está estipulada en 19 Pulg.
Impresora	Es un dispositivo periférico de salida del ordenador que permite producir una gama permanente de textos o gráficos

	de documentos almacenados en un formato electrónico.
PC	Una computadora personal, computador personal u ordenador, conocida como PC, es un tipo de microcomputadora diseñada en principio para ser utilizada por una sola persona.
VoIP phone	Una central telefónica IP es un equipo telefónico diseñado para ofrecer servicios de comunicaciones a través de una base de datos, ubicado por lo general en la sede principal donde se encuentra la tarjeta madre.
Ups	Es un dispositivo que gracias a sus baterías y otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado.
Laptop	Se denomina computadora Portátil u Ordenador Portátil o Portátil es un dispositivo informático que se puede mover o transportar con relativa facilidad.
Tablet	Es un dispositivo informático móvil en el que la pantalla táctil ocupa casi todo su tamaño y en el que no existe un teclado físico.
Switches	Es el Dispositivo Digital Lógico de Interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.
Móviles	Un dispositivo móvil es un pequeño dispositivo de computación portátil que generalmente incluye una pantalla y un método de entrada (ya sea táctil o teclado en miniatura). Muchos dispositivos móviles tienen sistemas operativos que pueden ejecutar aplicaciones.
Scanner	Un Scanner de un ordenador es un Periférico que se Utiliza Para Copiar Mediante el uso de Luz Imágenes Impresas o Documentos en Forma

	Digital.

2. Valoración de los activos o recursos.

Activo	Descripción
CPU	Procesador Intel Core i5-10400 de 6 núcleos de hasta 4,3 GHz LGA1200 (chipset Intel serie 400) 65 W, número de modelo: BX8070110400
Servidor Torre	Servidor HPE proliant ML30 Gen Con una capacidad de almacenamiento de hasta 72 TB, el HPE ML30 Gen10 Plus es una plataforma de memoria ideal para las empresas en crecimiento que tienen que hacer frente a cantidades de datos cada vez más grandes
Router	RadioShack RadioShack Router Wi-Fi EasyMesh / 2505005
Impresora	HP HP Impresora / 7FR21A / Multifuncional
PC	MSI PRO AP241 - Escritorio para computadora todo en uno, LED FHD de grado IPS de 23.8 pulgadas, Intel Core i3-10105, memoria de 8 GB, SSD de 500 GB, WiFi 6, BT 5.1, negro, Windows 10 Home (11M-630US)
VoIP phone	Ooma Telo VoIP Servicio de teléfono doméstico gratuito por Internet con 3 teléfonos HD3. Reemplazo de línea fija asequible. Llamadas nacionales ilimitadas. Contestador automático. Opción para bloquear llamadas automáticas

Ups	RadioShack UPS de 1000VA 480W 220VAC 2733354
Laptop	DELL Dell Laptop Intel® UHD Graphics 600 Intel N4020 9GY76
Tablet	Huawei Huawei Tablet MATEPADT10 9.7"
Switches	NETGEAR Conmutador PoE Gigabit Ethernet Plus de 24 puertos (JGS524PE) - Gestionado, con 12x PoE a 100 W, montaje en sobremesa o en bastidor, y protección limitada de por vida
Móviles	Huawei Huawei Tablet Mate Pad T8 / T8KOBE2 / 16 GB
Scanner	Brother ADS-1200 - Escáner de escritorio, compacto y fácil de usar, rápida velocidad de escaneo, ideal para el hogar, la oficina, o los profesionales en movimiento

2.2.1 Valoración y confidencialidad de activos

ACTIVOS	VALORACIÓN DE ACTIVOS		VALORACIÓN DE CONFIDENCIALIDAD			
Activo	**Valor**	**Descripción**	**C**	**I**	**D**	**Valor Final**
Servidor	10	Esencial para el desempeño de la empresa	3	3	3	3
Impresoras	7	Importante para la empresa	1	2	2	2
Control de acceso	3	Importancia menor para la empresa	2	1	2	2
Gabinete de red	10	Esencial para el desempeño de la empresa	2	3	3	3
Computadoras	10	Esencial para el desempeño de la empres	1	3	3	3

2.3 Identificación de amenazas y probabilidad

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

Tabla de estimación de probabilidad

NIVEL	DESCRIPCIÓN DE PROBABILIDAD
1	No hay posibilidad de que suceda o haya ocurrido.
2	La amenaza podría ocurrir una o dos veces a lo largo del tiempo de actividad de la empresa
3	La amenaza se materializa a lo mínimo una vez cada uno o dos años

4	La amenaza se materializa a lo mínimo una vez cada tres a seis meses.
5	La amenaza se materializa a lo mínimo una vez cada mes.

2.4 Amenazas clasificadas por su tipo y su nivel de probabilidad

TIPO	NIVEL DE AMENAZAS	DESCRIPCIÓN DE PROBABILIDAD	NP	RAZÓN DE LA CALIFICACIÓN
A1	Entrada de los laboratorios de computo	Con el sistema de control de acceso al laboratorio, se registra las entradas de las personas encargadas al 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.
A2	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.
A3	Daños de software al activo	Daños que son ocasionados por mal uso de algún software o mala utilización de programas que podrían causar problemas.	4	Es fácil que los empleados utilicen de mala manera el software por falta de capacitación
A4	Desperfectos al equipo	Fallos que se pueden ocasionar por algún equipo que venga mal de fábrica y tenga algún defecto.	2	Ocasiones que se han comprado activos que han sido comprados en mal estado o que no funcionen adecuadamente
A5	Phishing	Robo de información por parte del engaño o fraude que puedan ocasionar en los empleados	1	No ha habido casos de robo de información ocasionados de parte externa.

A6	Problemas por contraseñas débiles	Problemas ocurridos por el acceso a otras personas por los empleados al utilizar contraseñas con un menor nivel de seguridad	3	Los empleados siempre buscan alguna contraseña fácil de colocar o fácil de recordar y descifrar.
A7	Incendios	Fuegos ocasionados por incendios ocurridos dentro de la empresa o algún otro edificio cercano	1	Puede que haya algún incendio que podría ocasionar pérdidas dentro del equipo
A8	Error humano	Fallos ocasionados por los errores que los empleados podrían ocasionar.	5	Siempre puede ocurrir en cualquier operación a realizar el error humano
A9	Caída del activo por sobrecargas	Apagado o lentitud de los activos ocurridas por la gran carga que podrían recibir los activos	2	Siempre los activos tienen algún límite de carga que puedan tener, pero los activos de la empresa son algo potentes por lo tanto no puede ocurrir tan a menudo.
A10	Problemas de red	Problemas de conexión con el router a los activos o caídas de internet del servicio proveedor de internet	5	Es casi seguro que el proveedor de internet tenga alguna caída de servicio que podría inhabilitar las actividades de la empresa.
A11	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.
A12	Amenazas legales	Sucede en circunstancias las cuales se descubre que uno o varios de los equipos están utilizando software con licencias	1	No se han presentado acontecimientos, aunque es una posibilidad de que pase.

		ilegales o en el peor de los casos tráfico de información personal de sus clientes o empleados		
A13	Problemas por olvido o robo de cuentas	Problemas y pérdida de tiempo que ocurren cuando los empleados de la empresa pierden su contraseña y podría ser utilizada por alguna otra persona.	3	Ha habido casos en donde los empleados han olvidado sus credenciales para utilizar el sistema.

Matriz de Impacto potencial

Valor	Descripción	Descripción del Impacto
1	Bajo	Impacto muy Bajos en la Empresa
2	Moderado	Impactos moderados en la Empresa
3	Severo	Impacto Severos en la Empresa
4	Crítico	Impacto Sumamente Crítico en la Empresa

Tipo de Activo	Código de Amenaza	Amenaza	Impacto
Hardware	A1	Fallas en la Red	2
	A2	Pérdida de Datos	3
	A3	Desastres Naturales	4
	A4	Virus informáticos	3
	A5	Incendios	4
	A6	Equipos Mal Usados	2
	A7	Errores de Los Empleados	2
Software	A1	Fallas en la Red	2
	A2	Pérdida de Datos	3

	A3	Desastres Naturales	4
	A4	Virus informáticos	3
	A5	Incendios	4
	A6	Equipos Mal Usados	2
	A7	Errores de Los Empleados	2
Información	A1	Fallas en la Red	2
	A2	Pérdida de Datos	3
	A3	Desastres Naturales	4
	A4	Virus informáticos	3
	A5	Incendios	4
	A6	Equipos Mal Usados	2
	A7	Errores de Los Empleados	2

Riesgo Potencial

Probabilidad	Impacto			
	Bajo	Moderado	Severo	Critico
1	X(1)	X(1)	X(1)	X(1)
2	X(1)	X(1)	Y(2)	Z(3)
3	X(1)	Y(2)	Z(3)	W(4)
	X:riesgo bajo Asignado del (1)			
	Y;:riesgo Moderado Asignado del (2)			
	Z:riesgo Severo Asignado del (3)			
	W: riesgo Críticos Asignado del (4)			

Número de Amenazas por Zona de Riesgo y Tipo de Activo

Zona de riesgo	Hardware	Información	Software	Total general

Zona de riesgo x				
A1 - A10	0	0	0	0
Zona de riesgo y				
A1	1	1	1	3
A6	1	1	1	3
A7	1	1	1	3
Zona de riesgo z				
A2	1	1	1	3
A4	1	1	1	3
Zona de riesgo Cw				
A3	1	1	1	3
A5	1	1	1	3
Total general	**7**	**7**	**7**	**21**

RIESGO POTENCIAL

Tipo Activo	Código Amenaza	Amenaza	Impacto	Nivel de Probabilidad	Riesgo potencial	Zona de riesgo
Hardware	**A1**	Con el sistema de control de acceso al laboratorio, se registra las entradas de las personas encargadas al lugar.	1	2	3	Z
	A2	Daños por agua	2	2	4	W
Software	**A3**	Daños de software al activo	1	2	3	Z
	A4	Desperfectos al equipo	1	-	1	X
	A5	Phishing	2	2	4	W
	A6	Problemas por contraseñas débiles	1	-	1	X
Hardware	**A7**	Incendios	2	2	4	W
	A8	Error humano	1	1	1	X
	A9	Caída del activo por sobrecargas	1	2	2	Y
	A10	Problemas de red	2	1	3	Z
	A11	Electricidad	2	1	3	Z
Información	**A12**	Amenazas legales	1	-	1	X
	A13	Problemas por olvido o robo de cuentas	1	-	1	X

Salvaguardas	
ID	Descripción
1	Cámaras en las respectivas oficinas
2	Mantenimiento del Equipo
3	Sistema Antiincendios
4	Ups para proteger los posibles problemas
5	Antivirus en las maquinas
6	Mantenimiento del aire acondicionado
7	Extintores en las oficinas
8	Actualizaciones con el respectivo software y hardware
9	No llevar cualquier otro dispositivo de almacenamiento
10	Solo determinar ciertos empleados en determinadas áreas
11	Llevar control contra las plagas

Nivel	Descripción de la efectividad del control
1	La probabilidad de falla o no existente de un control
2	Control eficaz y con esto es probable que función en distintos casos
3	El control tiene la estabilidad de funcionar y esto con lleva una garantía

Controles implementados según el activo						
Tipo Activo	Código Amenaza	Vulnerabilidad	Controles	Nivel de Probabilidad	Control Implemented	Eficiencia del control
Hardware	**A1**	Falta de cámaras	Se necesita instalación de cámaras	Monitorización	si	3
	A2	No tener un reforzamiento del establecimiento	Poder mejorar la infraestructura	Prevención	no	3
Software	**A3**	No poder contar con antivirus y una mejor seguridad	Instalación de antivirus	Monitorización	si	2
	A4	No se realizó pruebas al dispositivo o software	Tener comprobantes de los dispositivos	Prevención	no	3
	A5	No contar con normas que puedan impedir el acceso a la web	Tener protocolos de seguridad	Monitorización	si	2
	A6	La contraseñas no son lo suficientemente seguras	Agregar más información a la contraseña	Prevención	si	2
Hardware	**A7**	Cualquier tipo de error o fuga que tenga determinado objeto	Tener relevación en los objetos inflamables y cortos	Prevención	si	3
	A8	Cualquier tipo de error ya sea de borrar bases de datos o dañar un dispositivo	Ser más precavido con lo que hacer el empleado	Prevención	si	2
	A9	Sobrecargar los dispositivos más de lo debido.	Tener paciencia con los dispositivos si no soportan una actividad	Prevención	no	2

	A10	El sistema de internet no está en funcionamiento	Tener un plan de contingencia con respecto a ello.	Monitorización	si	3
	A11	Fluido eléctrico falla	Tener una planta solar por desperfectos del fluido eléctrico.	Prevención	no	3
Información	**A12**	No poder manejar de forma legal asuntos	Ser precavidos con cada cosa que tengamos que realizar.	Monitorización	si	2
	A13	Saber llevar a cabo la vida personal de laboral y ser precavido con los datos del centro de cómputo.	Usar el sistema del centro de cómputo solo en el área de trabajo	Monitorización	no	3

Impacto Residual

Tipo de activo	Vulnerabilidad	Eficacia del control	Impacto Potencial	Impacto Residual
Hardware	Derrame de líquidos al computador	4	5	1.25
	Fallas en la impresora	3	5	1.7
	Falta de material en el centro como tinta o papel	2	5	2.5
	Falta de acceso de wi-fi	1	5	1.25
	Pieza del computador no funciona	3	5	1.7
	Polvo en los dispositivos	2	5	2.5
RED	fallas naturales	2	5	2.5
	Fallas del router	3	5	1.7
	Inestable la red	1	5	5
	Conexión incorrecta	2	5	2.5
Software	Fallas con el sistema operativo	3	5	1.7
	Algunas licencias no activadas	2	5	2.5
	Drivers desactualizados	4	5	1.25
	Infección de virus	4	5	1.25
Instalación	Instalación de cableados	2	5	2.5
	Toma de corrientes protectores	3	5	1.7
	Problemas de electricidad	4	5	1.25
	Esquema de instalación	3	5	1.7
	Problemas con la temperatura	3	5	1.7

Matriz de impacto Residual y Riesgo Residual

Tipo de activo	Vulnerabilidad	Eficacia del control	Impacto Potencial	Impacto Residual	Nivel de Probabilidad	Zona de riesgo residual
Hardware	Derrame de líquidos al computador	4	5	1.25	4	W
	Fallas en la impresora	3	5	1.7	2	Y
	Falta de material en el centro como tinta o papel	2	5	2.5	1	X
	Falta de acceso de wi-fi	1	5	1.25	2	Y
	Pieza del computador no funciona	3	5	1.7	4	W
	Polvo en los dispositivos	2	5	2.5	2	Y
RED	fallas naturales	2	5	2.5	4	W
	Fallas del router	3	5	1.7	3	Z
	Inestable la red	1	5	5	2	Y
	Conexión incorrecta	2	5	2.5	1	X
Software	Fallas con el sistema operativo	3	5	1.7	2	Y
	Algunas licencias no activadas	2	5	2.5	2	Y
	Drivers desactualizados	4	5	1.25	3	Z
	Infección de virus	4	5	1.25	4	W
Instalación	Instalación de cableados	2	5	2.5	2	Y
	Toma de corrientes protectores	3	5	1.7	2	Y
	Problemas de electricidad	4	5	1.25	3	Z

	Esquema de instalación	3	5	1.7	1	X
	Problemas con la temperatura	3	5	1.7	3	Z

Comunicación del riesgo y Recomendaciones

	Riesgo	Recomendación
1	Desastres Naturales	Una recomendación puede ser tener asegurada la organización o también se puede recomendar tener un fondo de ahorros para este tipo de situaciones.
2	Fallas en la Red	Se Recomienda Tener Monitorizada la red para no tener este tipo de fallas
3	Incendios	Estar prevenidos con este tipo de percances, tener a la disposición extintores o se recomienda alarma contra incendios.
4	Errores del Personal	Es necesario contar con un compañero que pueda dar soporte o ayuda en el caso de este tipo de errores
5	Inundaciones	Elaborar un Plan de contingencias para este tipo de desastre natural o tener un sondeo del clima para estar pendientes que medidas tomar en este caso.
6	Mal Uso del Equipo	Se recomienda al Inicio de las Contrataciones capacitar al personal o contratar personal altamente calificado.
7	Fallas de Energía Eléctrica	Utilizar UPS para evitar que el equipo se apague directamente y pueda dañar algún equipo o se recomienda el uso de planta eléctrica.
8	Pérdidas de Información	Se recomienda tener un respaldo de la Información o También se puede mantener la Información en la nube.
9	Robos	Estar prevenidos a este tipo de actos y se recomienda tener alarmas y cámara de seguridad.
10	Problemas con las Direcciones Ip	Hacer una monitorización para evitar este tipo de problemas en nuestra empresa

Tratamiento del Riesgo

Valoración por Colores

Nivel	Tipo	Representación
1	Bajo	
2	Moderado	
3	Alto	
4	Extremo	

Valoración del impacto y probabilidad

Las valoraciones de las probabilidades y Impactos en los riesgos se clasifican en Cuatro rangos:

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

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

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

Para el caso del impacto

•Extremo: La Amenaza se Materializó a cada 5 años o más

. Valoración por colores Nivel de riego Categorías Representación

1=Bajo

2=Moderado

3=Alto

4=Extremo

		Probabilidad				Impacto			
C	**Riesgos**	**(1)**	**(2)**	**(3)**	**(4)**	**(1)**	**(2)**	**(3)**	**(4)**
A1	Desastres Naturales	**X**							**X**
A2	Fallas en la Red		**X**					**X**	
A3	Incendios	**X**							**X**
A4	Errores Personales				**X**	**X**			
A5	Inundaciones	**X**							**X**
A6	Mal Uso del Equipo		**X**			**X**			
A7	Fallas de Energía Eléctrica		**X**			**X**			
A8	Pérdidas de Información		**X**					**X**	
A9	Robos		**X**					**X**	
A10	Problemas con la dirección Ip		**X**				**X**		

3.2 Costos estimados

A continuación, se presentará un estimado sobre los costos que tendría que realizar esta empresa para que las amenazas, riesgos y defectos sean solucionados y además se presentará el coste del proyecto de este informe para que la empresa considere que nuestro equipo realice todo lo que listamos.

Problemas a solucionar	Solución al problema	Valor mensual	Valor anual	Valor instantáneo
Daños físicos al activo	Comprar equipos más robustos.			L. 100,000
Daños de software al activo	Capacitación a los usuarios sobre la utilización adecuada de los activos			L. 5,000
Virus, gusanos y ransomware	Contratar un antivirus seguro	L. 208.3	L. 2,500	
Fallas de escaneo	Comprar mejores herramientas para escaneos			L. 50,000
Fallo de configuración	Capacitación para las personas que instalan los activos en la empresa			L. 30,000
Fallas al imprimir	Comprar mejores herramientas para imprimir			L. 20,000
Secuestro de registros	Capacitación a empleados y escaneo mensual de estas amenazas		L. 5,000	L. 5,000
Problemas por contraseñas débiles y robo de cuentas	Capacitación a los empleados			L. 10,000
Terremotos	Mejorar la infraestructura del edificio y la ubicación de los activos			L. 150,000
Fuegos	Más extintores al igual que instalacion de alarma de humos			L. 30,000
Servidor en riesgo de	Instalacion de piso falso en el área del			L. 30,000

3.3 Conclusiones y recomendaciones

3.3.1 Conclusiones

● Se cumplieron todos los objetivos específicos. La empresa por medio de este informe ahora es consciente de todos las amenazas que podría tener, las fallas que afectan su rendimiento y posibles soluciones a estas amenazas.

● Se hizo una descripción de todos los activos importantes para el funcionamiento completo de la empresa, y se identificó de manera exitosa todas las fallas que estos activos podrían tener, logrando mejorar la visión sobre estos activos y listar qué tan valiosos son para el desarrollo de la empresa.

● Es importante como empresa conocer qué elementos se podrían mejorar dentro de ellas para no sólo mejorar uno como empresa, sino también para crear un buen ambiente entre los empleados por medio de disminuir preocupaciones dentro de esta y también para mejorar el servicio al cliente y por medio de esta mejora lograr conseguir muchos más clientes.

● La identificación de todos los elementos para la creación de este informe fue muy fácil de conseguir con una gran rapidez ya que la empresa fue muy servicial y proveer esta información necesaria.

3.3.2 Recomendaciones

● Recomendamos a la empresa que tome acciones sobre la mayoría de cosas o si se podría, con todos los elementos peligrosos, advertencias, posibles fallas y lugares en donde mejorar para que la empresa pueda proveer un mejor servicio y un mayor aporte a la comunidad y a sus empleados.

● Lo más esencial que identificamos como una gran falla para la empresa es que no contenga un buen sistema de protección contra incendios dentro de su centro de datos. Es una falla grave que si esta amenaza se logra materializar haría una gran cantidad de daños ya que este es un activo crítico para la empresa. Recomendamos a la empresa que instale algún tipo de sistema de protección contra incendios dentro del centro de datos para no ocasionar pérdidas de datos de la empresa y datos de los usuarios.

● Recomendamos a la empresa que evalúe y tome nota y posibles acciones sobre las fallas graves que logramos localizar en sus activos y amenazas a estos activos como por ejemplo en los riesgos potenciales. Ya que las fallas graves que existen en estos activos son activos que son esenciales para poder operar de manera funcional dentro de la empresa.

● Los mayores riesgos que pueden existir en una empresa es que los usuarios no sepan utilizar de manera adecuada los activos importantes para el funcionamiento de la empresa, pueden ocasionarles fallas de software o dañarlos de manera física, por lo tanto, al observar que la mayoría de estas amenazas provienen de los empleados recomendamos que la empresa capacité en las áreas que más pueda a sus empleados, para ocasionar menos fallas, menos errores y así generar menos costos y mas ingresos.

3.4 Bibliografía

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

● Guamanga, C. y Perilla, C. (2015). Análisis de riesgos de seguridad de la información basado en la metodología magerit para el área de datacenter de una entidad promotora de salud