Universidad Católica De Honduras

(UNICAH)

"Nuestra Señora Reina de La Paz"

Asignatura:

Seguridad Informática

Catedrática:

Lic. Patricia Medina

Tema:

Entregable #1, Análisis de Riesgo

Alumnos:

Anthony Jafeth Portillo	0801-2000-14783
Mario José Herrera	1007-2000-00846
José Alejandro Ajuria	0801-2002-04150

Juticalpa, Olancho **30/01/2022**

Índice

Contenido

Análisis de Evaluación de Riesgos Aplicando la Metodología de Magerit Empresa OLANCHONET 1
1. Introducción 1
2. Objetivo General 2
3. Objetivo Especifico 2
4. Planteamiento del Problema 2
5. Justificación 3
6. Marco Conceptual 3
A. SEGURIDAD INFORMATICA 3
B. SGSI 4
C. ISO/IEC 31010 4
D. ISM3 4
E. RFC 2196 5
F. Metodología Magerit 5
7. Diagramas del Sistema Informático 6
Capítulo 1, Planificación 7
1.1 Planeación de la Seguridad 7
1.2 Alcance del Análisis 7
1.3 Análisis y Evaluación de Riesgos 8
Identificador de Activos 8
1.4 Objetivo de Análisis y evaluación de Riesgos 10
Capítulo 2. Análisis de Riesgos 11
2.1 Descripción de los Activos o Recursos 11
Características 12
2.2 Valoración de los Activos o Recursos 12
2.3 Identificación De Amenazas Y Probabilidad 12
2.4 Amenazas clasificadas por su tipo y su nivel de probabilidad 14
2.5 Matriz de impacto potencial 15
2.6 Riesgo Potencial 16
2.7 Número de amenazas por zona de riesgo y tipo de activo 16
2.8 Matriz de riesgo potencial 17
2.9 Salvaguardas o controles existentes 1

2.9.1 Controles implementados según el activo, la amenaza y su nivel de efectividad. 1
2.10 Impacto residual 8
2.11 Matriz de impacto residual y riesgo residual. 16

Análisis de Evaluación de Riesgos Aplicando la Metodología de Magerit
Empresa OLANCHONET

1. Introducción

En el presente informe detallaremos nuestra evaluación de riesgos utilizando la Metodología de Magerit para la Empresa OLANCHONET, dicha empresa es una de las proveedoras del servicio de internet para varios sitios del departamento de Olancho. Presentaremos nuestros objetivos principales, identificaremos los problemas y también explicaremos con detalle sus soluciones y evaluaciones. Para comprender el Método Magerit, debemos tener algunos conceptos básicos antes de empezar por lo que antes de comenzar la evaluación daremos las definiciones de algunas palabras que se irán utilizando a lo largo del documento y proyecto.

Algo que debe quedar muy en claro antes de comenzar, es que en el presente documento no se hará Ciberseguridad, que es la seguridad de las redes y el internet, si no que será Seguridad Informática que es la seguridad tanto física (Ubicación, Hardware, temperaturas), como de software.

2. Objetivo General

Crear un Análisis de Riesgo útil para la empresa de OLANCHONET, darles soluciones a todos sus problemas y crear planes tanto de contingencia como planes preventivos utilizando como base la metodología Magerit en conjunto con los datos ofrecidos por la empresa.

3. Objetivo Especifico

- Definir los problemas que tenga la empresa en su seguridad informática.
- Analizar la empresa correctamente.
- Poner en Práctica la Metodología Magerit
- Crear Plan de Contingencia.
- Crear Plan de Prevención.
- Crear Plan de Emergencia
- Cumplir con los requerimientos de la ISO 27000, ISO 27001 y la ISO 27002.

4. Planteamiento del Problema

La seguridad es primordial en el ser humano y en la realización de cualquier proyecto o situación de la vida. Establecemos que "La seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella". En todo objeto de estudio de la humanidad, se necesita estabilidad y protección de información o bienes, en informática sabemos que la herramienta principal que ayudo a su divagación en el mundo, son las computadoras, cualquiera que sea la categoría.

Las empresas tienen riesgo de perder información, esto podría detener su operación, deteniendo procesos de producción o administrativos, para ello es necesario proteger el funcionamiento de la información, existen diferentes maneras o métodos de proteger un sistema de información, todas estas partes del sistema de seguridad deben trabajar en conjunto para asegurar la informática de la empresa. Una de las principales amenazas que enfrenta toda organización para proteger su información es el factor humano la cual es capaz de atentar contra la seguridad de la información. Esto se debe a que, a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad, la creciente rentabilidad de los ataques, han provocado en los últimos años un 70% el aumento de amenazas intencionales.

En este trabajo de investigación identificaremos las realidades acerca de la seguridad informática y describir recomendaciones, estrategias, errores comunes y amenazas para con la seguridad informática.

5. Justificación

La empresa que elegimos es una empresa de internet donde fluyen muchos datos y donde la información personal de las personas se almacenan, por esta razón debemos tener mucho cuidado con nuestros servidores, switch, computadoras, etc. EN las cuales trabajamos en la empresa, pues si nos ocurre un accidente o algún ataque, nos veremos vulnerables y como consecuencia la reputación bajase, junto con la fiabilidad, lo que resultaría en números negativos. Por esta razón hay muchos tipos de amenazas e intentar identificarlas y arreglarlas es lo que debemos hacer antes de que sea tarde.

Una de las principales amenazas que enfrenta toda organización para proteger su información es el factor humano De acuerdo a estudios de mercado, 63% de las empresas públicas y privadas pierden anualmente archivos de información valiosa, pero solo 23% es por robo. De la pérdida de información 75% se debe al extravío de equipos portátiles, como computadoras, celulares, agendas electrónicas, o dispositivos como discos compactos y memorias USB."

6. Marco Conceptual

A. SEGURIDAD INFORMATICA

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.2 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, convirtiéndose así en información privilegiada.

B. SGSI

Tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa. El SGSI es un elemento fundamental de la norma internacional ISO 27001 (Sistemas de Gestión de la Seguridad de la Información), que persigue asegurar la integridad y confidencialidad de los datos y los sistemas encargados de procesarlos. 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.

C. ISO/IEC 31010

Es una norma que nace en el año 2009. Si bien, diez años después, se publica una nueva versión: la ISO 3010:2019. Esta norma presenta 42 técnicas relacionadas con la gestión de riesgo en alguna de sus etapas. Respecto a la versión anterior, presenta las siguientes novedades:

- Se amplía el número de técnicas.
- Incluye algunas técnicas nuevas.
- Se eliminan algunas de las anteriores.

D. 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.

E. RFC 2196

Es 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.

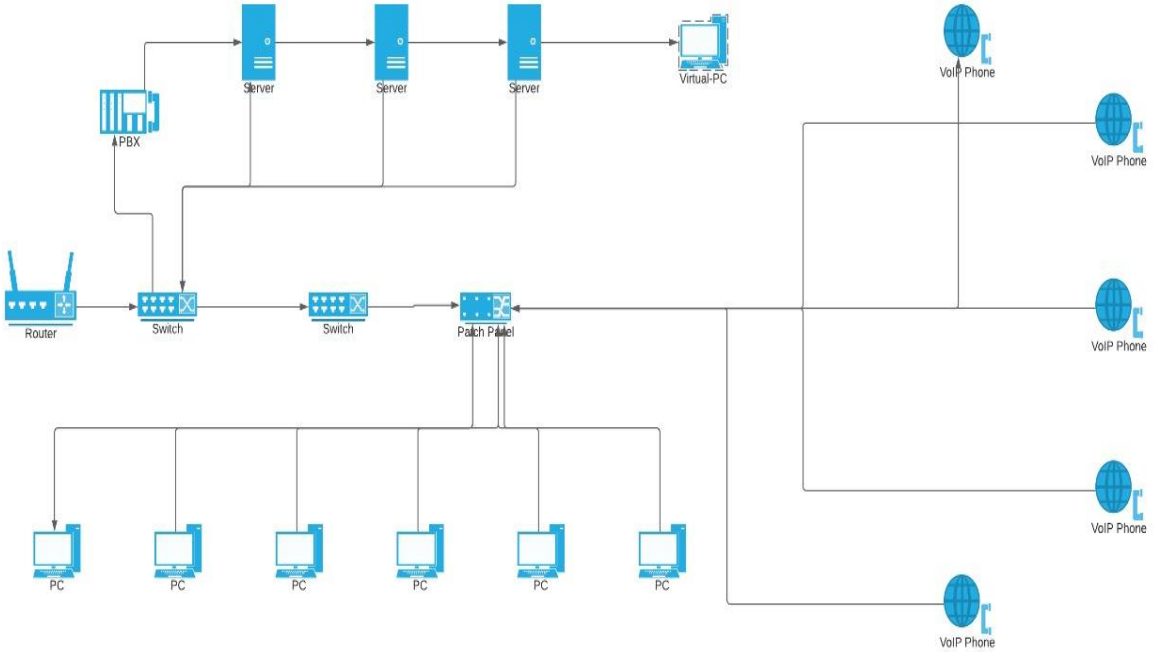
F. Metodología Magerit

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.

7. Diagramas del Sistema Informático



Capítulo 1, Planificación

1.1 Planeación de la Seguridad

En este punto debemos planificar cada movimiento para mejorar la seguridad informática de la empresa. Como primer punto debemos informar a los encargados del sector que vamos a estudiar, de que tomaremos nota de la situación del lugar para mejoras de la ubicación. También debemos informar que necesitaremos una lista de todos los activos para identificar los riesgos de cada uno utilizando la metodología de Magerit. Es de vital importancia que se capacite al personal para evitar algunos posibles riesgos.

Algunas de las capacitaciones deben ser de seguridad al usuario, pues estos deben mantener todos sus dispositivos vinculados a la empresa en el edificio de la misma, para evitar perdidas accidentales o robos, de esta misma forma, enseñarles a no dar sus credenciales de usuario y sobre esto a que no deben entrar en zonas no autorizadas, pues al ser un servicio de internet no todos en la empresa tienen los conocimientos necesarios para saber que se puede modificar y que no.

En cuanto al Hardware se debe verificar la zona en la que se encuentra y verificar si esta en condiciones seguras y protegidas, sumado a esto debemos buscar las posibles fugas en la infraestructura de la red.

Investigaremos todo esto, para crear los planes de protección, contención, prevención y emergencia. Para mejorar la Seguridad del la Empresa.

1.2 Alcance del Análisis

Al alcance que queremos tener va desde el lugar donde tienen el control de los Switches y servidores, hasta la infraestructura de redes para el control del internet. Se desea hacer todas las mediciones cuantitativas, para tener referencias probabilísticas de las posibles debilidades que tenga la empresa y de este modo ordenarlas de manera que se muestre de forma sencilla cuales son los posibles casos de vulnerabilidad mas probables en aparecer y causar daños.

1.3 Análisis y Evaluación de Riesgos

Identificador de Activos

Identificador	Activo	Descripcion	Tipo	Cantidad
ID_01	Servidor 1	Servidor de Datos	Servidor Fisico	1
ID_02	Servidor 2	Servidor IPTV	Servidor Fisico	1
ID_03	Servidor 3	Servidor Linux	Servidor Fisico	1
ID_04	PBX	Servidor VoIP	Servidor Fisico	1
ID_05	Router	Router Principal	Router Mikrotik 3011	1
ID_06	Switch 1	Switch de distribucion	Switch CRS125 Mikrotik	1
ID_07	Switch 2	Switch de distribucion	Switch CRS125 Mikrotik	1
ID_08	PC	Computadoras de empleados	Computadora Dell	6
ID_14	VoIP Phone	Telefonos de empleados	Telefono Grandstream	6
ID_20	Patch Panel	Panel de distribución	Patch Panel 48 puertos	1
ID_21	Pc Virtual	Ubuntu para pruebas	Maquina Vitual	1

Tabla de Estimación de la Probabilidad	
Valor	Descripción
1	La amenaza se puede presentar 1 o 2 veces al año
2	La amenaza se presenta 1 o 2 veces cada 6 meses
3	La amenaza se manifiesta constantemente en periodos de tiempo menores a 4 meses

Tabla de Estimación del Impacto	
Valor	Descripción
1	El daño no afecta las funciones ni los datos de la empresa
2	El daño entorpece las funciones o los datos de la empresa y es reversible o recuperable
3	El daño es irreversible para la empresa

Tabla de Aceptación de riesgo	
Valor	Descripción
Riesgo <= 3	No es un problema para la empresa
Riesgo = 4	La empresa considera que puede desembocar en un problema mayor
Riesgo > 4	La empresa considera que es un problema y procederá a tomar medidas.

Análisis de Riesgo					
Activo	**Amenaza**	**Tratamiento de Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor (ID_01, ID_02, ID_03)	Ataque interno (Físico)	Controlar el Acceso de las personas y objetos a la sala de servidores	1	3	3
Servidor (ID_01, ID_02, ID_03)	Ataque interno	Implementar el principio de control dual	1	2	2
Servidor (ID_01, ID_02, ID_03)	Configuración Errónea	Revisión automática que audite vulnerabilidades	1	1	1
Servidor (ID_01, ID_02, ID_03)	Navegación imprudente por parte de Empleados	Implementar Filtro de Contenido web	1	2	2
Servidor (ID_02)	Servidor Web Comprometido	Auditar el código de la aplicación de TV	1	2	2
PBX	Denegación de Servicio (DoS)	Contar con Banda Ancha	2	2	4
PBX	Fuzzing	Cambiar los protocolos de Seguridad	1	3	3
Router	Firmware desactualizado	Actualizar y configurar el nuevo Firmware	1	1	1
Switch	Ataques a la tabla MAC	Port Security	1	3	3
Switch	Ataques De DHCP	DHCP Snooping	1	3	3
Switch	Ataques ARP	Dynamic ARP Inspection (DAI)	1	3	3

1.4 Objetivo de Análisis y evaluación de Riesgos

- Proteger la información de la empresa, así como su integridad
- Dar el tiempo necesario para identificar las posibles amenazas y atacarlos antes que se conviertan en problemas.
- Según el nivel de Riesgo priorizar el plan de contingencia contra esa amenaza.
- Según los estudios identificar que apartados de la empresa mejorar.
- Incentivar al personal a informar inmediatamente de un problema o error en las instalaciones.
- Aumentar las medidas de seguridad de la Empresa.
- Concientizar de todas las amenazas humanas a el personal de la Empresa.

Capítulo 2. Análisis de Riesgos

2.1 Descripción de los Activos o Recursos

Activo	Descripcion
Servidores	capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora
PBX	Se refiere a un dispositivo que conecta un determinado número de terminales de comunicación, tales como teléfonos o máquinas de fax, entre ellos y a la red telefónica pública. Para la conexión a la red telefónica se pueden utilizar una o varias líneas paralelas.
Router	guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web
Switches	encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.
PC	es un tipo de microcomputadora diseñada en principio para ser utilizada por una sola persona.
VoIP Phone	es un teléfono basado en hardware o software diseñado para usar la tecnología de voz sobre IP (VoIP) para enviar y recibir llamadas telefónicas a través de una red IP.
Patch Panel	es el elemento encargado de recibir todos los cables del cableado estructurado

Características

Activo	Descripcion
Servidores	CENTOS LINUX 16gb ram, 2tb hdd, 512ssd, ryzen 5 5700x
PBX	Grandstream Networks UCM6202, Centralita
Router	CISCO 1941 2 Ethernet 10/100/1000 integrada | 1 Servicios internos 1 Ranura del módulo de servicios internos | Seguridad Cifrado de VPN acelerado por hardware incorporado
Switches	CISCO 2960 24 puertos 10/100 + 2 puertos SFP Combo - LAN Base
PC	Windows 10, 256 SSD, 8gb Ram, i3 10300k
VoIP Phone	Motorola CT202C - Teléfono Fijo Analógico (Manos Libres, Capacidad de 30 Contactos)

2.2 Valoración de los Activos o Recursos

Valor			**Criterio**
10	INSERVIBLE	I	Equipo obsoleto
7-9	Muy dañado	MU	Debe cambiarse para mantener la integridad de la red
4-6	Medianamente dañado	ME	Equipo propenso a dañarse sino se tiene cuidado
1-3	Levemente Dañado	LE	Daño menor al equipo
0	Nuevo	N	Equipo recien instalado

2.3 Identificación De Amenazas Y Probabilidad

Nivel	Descripción de probabilidad
1	Improbable y no se tiene evidencia de que ha ocurrido
2	Probable que se produzca una vez cada dos años
3	Probable que se produzca una vez cada trimestre

Amenazas Identificadas		
Código	**Amenaza**	**Descripción**
A1	Incendio	Un incendio provocado por un error humano o una falla eléctrica puede provocar daños irreversibles a los Activos
A2	Daños por Agua	Una inundación o gotera, incluso la mala circulación del aire que pueda provocar humedad en el ambiente pueda afectar a los equipos electrónicos o circuitos eléctricos del local
A3	Desastres Naturales	Terremotos o Tormentas, tornados, Huracanes, Tsunamis
A4	Personal Malintencionado	Robo de Información por parte del personal o sabotaje a los equipos de la empresa.
A5	Mal Uso del Software	Utilización errónea del software o utilización de Software diferente al especificado por la empresa
A6	Errores Humanos	Equivocaciones por parte del personal de la Empresa, ya sea tanto en físico como en sistemas.
A7	Fallas en la Infraestructura de la Red	Problemas con la conexión de internet de proveedores, distribución a clientes, caídas de servidor o servicios.

2.4 Amenazas clasificadas por su tipo y su nivel de probabilidad

Código	Amenaza	Descripción	NP	Razón de la Calificación
A1	Incendio	Un incendio provocado por un error humano o una falla eléctrica puede provocar daños irreversibles a los Activos	1	En años de trabajo nunca se ha producido un incendio, ni siquiera una chispa. El Local no cuenta con las herramientas de control de incendios de Aspersores
A2	Daños por Agua	Una inundación o gotera, incluso la mala circulación del aire que pueda provocar humedad en el ambiente pueda afectar a los equipos electrónicos o circuitos eléctricos del local	1	Daños por inundación son imposibles debido a que los equipos están en la segunda planta del edificio. Se regula la temperatura del lugar con aires acondicionados para no generar humedad en el ambiente. No hay precedentes de goteras en el local.
A3	Desastres Naturales	Terremotos o Tormentas, tornados, Huracanes, Tsunamis	2	En la ubicación Geográfica del edificio no hay suelen pasar terremotos, ni tornados, ni Huracanes y al estar lejos de la costa tampoco es susceptible a Tsunamis. Las Tormentas tropicales suelen hacer fallos en las líneas eléctricas del Departamento
A4	Personal Malintencionado	Robo de Información por parte del personal o sabotaje a los equipos de la empresa.	1	Durante los años de existencia de la empresa nunca ha habido un sabotaje por parte de empleados dentro de la empresa.
A5	Mal Uso del Software	Utilización errónea del software o utilización de Software diferente al especificado por la empresa	2	Existen precedentes de la mal utilización del Software y puede volver a pasar.
A6	Errores Humanos	Equivocaciones por parte del personal de la Empresa, ya sea tanto en físico como en sistemas.	2	Suelen haber errores muy poco seguidos, en las instalaciones de los servicios o en las actualizaciones de software o inclusión de nueva indumentaria.
A7	Fallas en la Infraestructura de la Red	Problemas con la conexión de internet de proveedores, distribución a clientes, caídas de servidor o servicios.	2	Existen precedentes de caídas por parte del proveedor y servicios de la empresa.

2.5 Matriz de impacto potencial

Valor Numérico	Valor	Descripción
1	Muy Bajo	Consecuencia muy bajas o mínimas sobre la empresa
2	Bajo	Consecuencia bajas y poco molestas sobre la empresa
3	Medio	Consecuencias medianas y lo suficientemente problemáticas para empresa
4	Alto	Consecuencia Altas y Bastante molestas sobre la empresa
5	Extremo	Consecuencia Muy Altas e Irreversibles sobre la empresa

Tipo de Activo	Código Amenaza	Amenaza	Impacto
Hardware	A1	Incendio	5
	A2	Daños por Agua	5
	A3	Desastres Naturales	2
	A4	Personal Malintencionado	4
	A5	Mal Uso del Software	4
	A6	Errores Humanos	4
	A7	Fallas en la Infraestructura de la Red	3
Software	A1	Incendio	1
	A2	Daños por Agua	1
	A3	Desastres Naturales	1
	A4	Personal Malintencionado	4
	A5	Mal Uso del Software	4
	A6	Errores Humanos	3
	A7	Fallas en la Infraestructura de la Red	4
Información	A1	Incendio	5
	A2	Daños por Agua	5
	A3	Desastres Naturales	2
	A4	Personal Malintencionado	5
	A5	Mal Uso del Software	4
	A6	Errores Humanos	4
	A7	Fallas en la Infraestructura de la Red	3

2.6 Riesgo Potencial

Probabilidad	Impacto				
	Muy Bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Extremo (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 bajo: Asumir el riesgo (1-4)				
	M: zona de Riesgo Medio: Asumir el riesgo, reducir el riesgo (5-8)				
	A:Zona de Riesgo Alto: Reducir el riesgo, evitar el riesgo (9-12)				
	E: Zona de Riesgo Extremo: Reducir, evitar, eliminar (12-15)				

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

Zona de Riesgo	Hardware	Informacion	Software	Total General
Zona B	2	1	4	7
Desastres Naturales	1	1	1	3
Personal Mal intencionado	1	0	1	1
Incendio	0	0	1	1
Daños por Agua	0	0	1	1
Zona M	4	5	2	11
Daños por Agua	1	1	0	2
Mal Uso del Software	1	1	1	3
Errores Humanos	1	1	0	2
Fallas en la Infraestructura de la Red	1	1	1	3
Personal Mal intencionado	0	1	0	1
Zona A	1	1	1	3
Incendio	1	1	0	2
Errores Humanos	0	0	1	1
Total General	7	7	7	21

2.8 Matriz de riesgo potencial

Tipo de Activo	Codigo Amenaza	Amenaza	Impacto	NP	Riesgo Potencial	Zona de Riesgo
Hardware	A1	Incendio	5	2	10	A
	A2	Daños por Agua	5	1	5	M
	A3	Desastres Naturales	2	1	2	B
	A4	Personal Malintencionado	4	1	4	B
	A5	Mal Uso del Software	4	2	8	M
	A6	Errores Humanos	4	2	8	M
	A7	Fallas en la Infraestructura de la Red	3	2	6	M
Software	A1	Incendio	1	1	1	B
	A2	Daños por Agua	1	1	1	B
	A3	Desastres Naturales	1	1	1	B
	A4	Personal Malintencionado	4	1	4	B
	A5	Mal Uso del Software	4	2	8	M
	A6	Errores Humanos	3	3	9	A
	A7	Fallas en la Infraestructura de la Red	4	2	8	M
Informacion	A1	Incendio	5	2	10	A
	A2	Daños por Agua	5	1	5	M
	A3	Desastres Naturales	2	1	2	B
	A4	Personal Malintencionado	5	1	5	M
	A5	Mal Uso del Software	4	2	8	M
	A6	Errores Humanos	4	2	8	M
	A7	Fallas en la Infraestructura de la Red	3	2	6	M

2.9 Salvaguardas o controles existentes

La empresa en cuetion no tiene ningún salvaguardas en caso de desastres naturales, sismos, incendios, inundaciones, robo o hurto. Solamente cuenta con planta de energía eléctrica cuando esta baja voltaje para salvar la integridad de todos los equipos y con auto backups de la información crucial de la empresa en la nube que se actualiza semanalmente en los servidores

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

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Implementado?	Eficacia	Comentarios
Hardware, Software, Informacion	Proximidad a plantas de producción de Petróleo,gasolina	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de Petroleo, Gasolina y Quimicos inflambales	Minimizadoras	PARCIAL	2	Instalaciones cercanas a gasolinera Texaco.
	Proximidad a áreas de combustión o áreas de almacenamiento de material inflamable					
	Interiores construidos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente	Minimizadoras			

	Equipos y circuitos eléctricos de baja calidad	Materiales inflamables o peligrosos deberán almacenarse a una distancia segura				
Hardware	Manejo inadecuado de cilindros, gas etc	Definir directrices para el manejo de cilindros,	Administrativas	SI	3	
Hardware, Software, Informacion	Ausencia de un sistema de detección de incendios	Desarrollar y mantener un proceso de ges3ón para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	Administrativas	NO	1	No existe sistema de detección de incendios.
	Ausencia de un equipo contra incendios					
	Se permite fumar dentro de las instalaciones					
	Exteriores hechos con material combustible					
	La falta de mecanismos alternos en caso de destrucción total por fuego					
Hardware, Software, Informacion	Ausencia de backup en un lugar diferente o lugar alterno	Ubicar en un lugar diferente al sho de operación principal, los backup de la información.	Recuperacion	PARCIAL	2	Solamente Archivos importantes backupeados en la nube

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Implementado?	Eficacia	Comentarios
Hardware, Informacion	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un área propensa a inundaciones	Minimizadoras	SI	3	Situado en zona segura encontra de inundación, y con las medidas de seguridad adecuadas para contrarrestar cualquier tipo de tormenta.
	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones	Minimizadoras			
	Calidad baja en la construcción de los edificios	La construcción del edificio debe ser resistente a fugas de gua	Minimizadoras			
	Incapacidad para absorber rayos	Sistemas para rayos y sistemas de polo a tierra	Minimizadoras			
	Sistema de drenaje debil	Se debe implementar protección en contra de inundaciones y fugas de agua	Minimizadoras			
	Ausencia de control de temperatura y	Sistema de monitoreo adecuado para temperatura y humedad	Monitorizacion			

	humedad adecuada					
	Incapacidad para controlar la temperatura y la humedad dentro del centro de datos	Los equipos de control de humedad y temperatura deben mantenerse correctamente	Monitorizacion			
Hardware	Incapacidad para controlar la entrada de humos venenosos/ aire/ humo a través de los conductos de aire	El manejo adecuado de apertura/ cierre de los conductos de aire durante eventos como vientos fuertes	Administrativa	NO	1	Controles no implementados en las facilidades de la empresa

Activos afectados	**Vulnerabilidad**	**Controles**	**Tipo de control**	**Implementado?**	**Eficacia**	**Comentarios**
Hardware, Software, Informacion	Ubicado en una zona de alto nivel sismico	Las instalaciones deben ubicarsa en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremolos	Minimizadoras	SI	3	Facilidades ubicadas en un lugar seguro contra sismos y terremotos
	Estructura de construcción y techos de baja calidad	La infraestructura debo ser resistente a terremotos si se encuenira ubicada on una zona de mod o o alio nivol samico.	Minimizadoras			

		e debe implementar una protección apropiada contra terremolos				
Hardware, Software, Informacion	Ausencia de backup en un lugar diferente o lugar alterno	Ubicar en un lugar diferente al sitio de operación principal, los backup de la informacion	Administrativas	SI	2	Archivos backupeados en la nube con diferentes servidores en el planeta
Hardware, Software, Informacion	La falta de mecanismos alternos en caso de destrucción total por desastres naturales	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones.	Administrativas	PARCIAL	2	El negocio podría seguir de manera limitada en caso de destrucción total por desastres naturales

Activos afectados	Vulnerabilidad	Controles	Tipo de control	Implementado?	Eficacia	Comentarios
Transaccional	Acceso no autorizado a información confidencial del sistema Transacional	Validar y hacer los ajustes requeridos en la aplicación Web del sitio www.transacional.gov para que siempre exija autenticación a los usuarios y no pueda ser accedida por personal no autorizado desde internet	Prevencion	SI	3	Sistema transaccional manejado con la banca privada de los usuarios
Mantis Transaccional Aplicación	Divulgacion de información de PHP (expose_php) Pagina por Defecto	En el archivo de configuración de PHP 'expose_php' en 'Off' para deshabilitar este comportamiento Configure los permisos en el servidor web para denegar el directorio 'svn'	Prevencion	NO	1	Pagina susceptible a ciberataques
HC Especialistas	CGI Generic SQL injection	Configurar una pagina de inicio del sitio web en lugar de la pagina por defecto de IIS. Una pagina de 'En construcción se puede utilizar'	Prevencion	NO	1	No existe ningún tipo de prevención en contra de ataques al sistema

	CGI Generic SQL injection	Implementar mecanismos de control para filtrar caracteres peligrosos	Prevencion			

2.10 Impacto residual

Tipo de Activo	Vulnerabilidad	Controles	Tipo de Control	Control Implementado	Eficacia del control	Impacto potencial	Impacto residual
Hardware, Software, Información	Proximidad a plantas de producción de Petróleo, gasolina	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de Petróleo, Gasolina y Químicos inflamables	Minimizadoras	Parcial	2	5	2.5
	Proximidad a áreas de combustión o áreas de almacenamiento de material inflamable				2	5	2.5
	Interiores construidos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente, Materiales inflamables o peligrosos deberán almacenarse a			2	5	2.5
	Equipos y circuitos eléctricos de baja calidad				2	5	2.5

		una distancia segura					
Hardware	Manejo inadecuado de cilindros, gas etc.	Definir directrices para el manejo de cilindros	Administrativas	Si	3	5	1.67
Hardware, Software, Información	Ausencia de un sistema de detección de incendios	Desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	Administrativas	No	1	5	5
	Ausencia de un equipo contra incendios				1	5	5
	Se permite fumar dentro de las instalaciones				1	5	5
	Exteriores hechos con material combustible				1	5	5
	La falta de mecanismos alternos en caso de destrucción total por fuego				1	5	5
	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un			3	5	1.67

Hardware, Información		área propensa a inundaciones	Monitorización	Si			
	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones			3	5	1.67
	Calidad baja en la construcción de los edificios	La construcción del edificio debe ser resistente a fugas de agua			3	5	1.67
	Incapacidad para absorber rayos	Sistemas para rayos y sistemas de polo a tierra			3	2	0.67
	Sistema de drenaje débil	Se debe implementar protección en contra de inundaciones y fugas de agua			3	5	1.67
	Ausencia de control de temperatura y humedad adecuada	Sistema de monitoreo adecuado para temperatura y humedad			3	4	1.33
	Incapacidad para controlar la temperatura y la	Los equipos de control de humedad y temperatura			3	4	1.33

	humedad dentro del centro de datos	deben mantenerse correctamente					
	Incapacidad para controlar la entrada de humos venenosos/ aire/ humo a través de los conductos de aire	El manejo adecuado de apertura/ cierre de los conductos de aire durante eventos como vientos fuertes	Administrativas	No	1	4	4

Tipo de Activo	Vulnerabilidad	Controles	Tipo de Control	Control Implementado	Eficacia del control	Impacto potencial	Impacto residual
Hardware, Software, Información	Ubicado en una zona de alto nivel sísmico	Las instalaciones deben ubicarse en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremotos	Minimizadoras	Si	3	2	0.67
		La infraestructura debo ser resistente a terremotos si se encuentra ubicada en una zona de medio o alto nivel sísmico y			3	2	0.67

	Estructura de construcción y techos de baja calidad	debe implementar una protección apropiada contra terremotos					
Hardware, Software, Información	Ausencia de backup en un lugar diferente o lugar alterno	Ubicar en un lugar diferente al sitio de operación principal, los backup de la información	Recuperación	Si	2	5	2.5
Hardware, Software, Información	La falta de mecanismos alternos en caso de destrucción total por desastres naturales	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar	Administrativas	Parcial	2	2	1

		interrupciones.					
Transaccional	Acceso no autorizado a información confidencial del sistema Transaccional	Validar y hacer los ajustes requeridos en la aplicación Web del sitio www.transacional.gov para que siempre exija autenticación a los usuarios y no pueda ser accedida por personal no autorizado desde internet	Prevención	Si	3	4	1.33
Mantis Transaccional Aplicación	Divulgación de información de PHP (expose_php) Pagina por Defecto	En el archivo de configuración de PHP 'expose_php' en 'Off' para deshabilitar este comportamiento Configure los permisos en el servidor web para denegar el directorio	Prevención	No	1	3	3

		‘svn’					
HC Especialistas	CGI Generic SQL injection	Configurar una página de inicio del sitio web en lugar de la página por defecto de IIS. Una página de ‘En construcción se puede utilizar’	Prevención	No	1	4	4
		Implementar mecanismos de control para filtrar caracteres peligrosos					4

2.11 Matriz de impacto residual y riesgo residual.

Tipo de Activo	Vulnerabilidad	Controles	Tipo de Control	Control Implementado	Eficacia del control	Impacto potencial	Impacto residual	Nivel de Probabilidad	Riesgo Residual	Zona de Riesgo Residual
Hardware, Software, Información	Proximidad a plantas de producción de Petróleo, gasolina	Los centros de datos deben estar ubicados a una distancia segura de plantas de producción de petróleo, Gasolina y Químicos inflamables	Minimizadoras	Parcial	2	5	2.5	1	2.5	B
	Proximidad a áreas de combustión o áreas de almacenamiento de				2	5	2.5	2	5	A
	Interiores construidos con material combustible.	Un equipo contra incendios deberá ser proporcionado y colocado adecuadamente, Materiales inflamables o peligrosos deberán almacenarse a una distancia segura			2	5	2.5	1	2.5	B
	Equipos y circuitos eléctricos de baja calidad				2	5	2.5	3	7.5	B

Hardware	Manejo inadecuado de cilindros, gas etc.	Definir directrices para el manejo de cilindros	Administrativas	Si	3	5	1.67	1	1.67	B
Hardware, Software, Información	Ausencia de un sistema de detección de incendios	Desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	Administrativas	No	1	5	5	1	5	A
	Ausencia de un equipo contra incendios				1	5	5	1	5	B
	Se permite fumar dentro de las instalaciones				1	5	5	4	20	E
	Exteriores hechos con material combustible				1	5	5	3	15	B
	La falta de mecanismos alternos en caso de destrucción total por fuego				1	5	5	1	5	A
Hardware, Softw	Ausencia de backup en un lugar	Ubicar en un lugar diferente al sitio de	Recuperación	Parcial	2	4	2	1	2	B

are, Información	diferente o lugar alterno	operación principal, los backup de la información.								
Hardware, Información	Situado en una zona propensa a las inundaciones	Los centros de procesamiento de información no deberían estar localizados en un área propensa a inundaciones	Monitorización	Si	3	5	1.67	1	1.67	B
	Ausencia de pisos elevados	Se debe implementar protección contra inundaciones			3	5	1.67	1	1.67	B
	Calidad baja en la construcción de los edificios	La construcción del edificio debe ser resistente a fugas de agua			3	5	1.67	1	1.67	A
	Incapacidad para absorber rayos	Sistemas para rayos y sistemas de polo a tierra			3	2	0.67	1	0.67	B
	Sistema de drenaje débil	Se debe implementar protección en contra de inundaciones y			3	5	1.67	1	1.67	B
	Ausencia de control de	Sistema de monitoreo			3	4	1.33	1	1.33	B

	temperatura y humedad	adecuado para temperatura y humedad								
	Incapacidad para controlar la temperatura y la humedad dentro del centro de datos	Los equipos de control de humedad y temperatura deben mantenerse correctamente			3	4	1.33	1	1.33	A
	Incapacidad para controlar la entrada de humos venenosos/ aire/	El manejo adecuado de apertura/ cierre de los conductos de aire durante	Administrativas	No	1	4	4	1	4	B

Tipo de Activo	Vulnerabilidad	Controles	Tipo de Control	Control Implementado	Eficacia del control	Impacto potencial	Impacto residual	Nivel de Probabilidad	Riesgo Residual	Zona de Riesgo Residual
Hardware, Software, Información	Ubicado en una zona de alto nivel sísmico	Las instalaciones deben ubicarse en una zona de bajo nivel sísmico. Se debe implementar una protección apropiada contra terremotos	Minimizadoras	Si	3	2	0.67	1	0.67	B
	Estructura de construcción y techos de baja calidad	La infraestructura debo ser resistente a terremotos si se encuentra ubicada en una zona de medio o alto nivel sísmico y debe implementar una protección apropiada contra terremotos			3	2	0.67	1	0.67	B
Hardware, Software,	Ausencia de backup en un lugar diferente o lugar alterno	Ubicar en un lugar diferente al sitio de operación principal, los backup de la	Recuperación	Si	2	5	2.5	5	12.5	E

Información		información								
Hardware, Software, Información	La falta de mecanismos alternos en caso de destrucción total por desastres naturales	Desarrollar y mantener un proceso de gestión para la Continuidad del Negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización. Identificar los eventos que pueden causar interrupciones.	Administrativas	Parcial	2	2	1	1	1	B
Transaccional	Acceso no autorizado a información confidencial del sistema Transaccional	Validar y hacer los ajustes requeridos en la aplicación Web del sitio www.transacional.gov para que siempre exija autenticación a	Prevención	Si	3	4	1.33	2	2.66	B

		los usuarios y no pueda ser accedida por personal no autorizado desde internet								
Mantis	Divulgación de información de PHP (expose_php) Pagina por Defecto	En el archivo de configuración de PHP ‘expose_php’ en ‘Off’ para deshabilitar este comportamiento Configure los permisos en el servidor web para denegar el directorio ‘svn’	Prevención	No	1	3	3	3	9	A
Transaccional Aplicación							3	2	6	B
HC Especialistas	CGI Generic SQL injection	Configurar una página de inicio del sitio web en lugar de la página por defecto de IIS. Una página de ‘En construcción se puede utilizar’	Prevención	No	1	4	4	1	4	B
		Implementar mecanismos de control para filtrar					4	1	4	B

		caracteres peligrosos								

3.3 Comunicación del riesgo y recomendaciones

Llegados a este punto y con la etapa de análisis de riesgo finalizada, los resultados de la situación de la empresa estudiada serán entregada a esta misma para que los altos cargos o directivos determinen que acciones tomar en los riesgos presentados y sus valores determinados.

Nosotros los estudiantes recomendamos que las acciones contra los riesgos sean basados en los tratamientos de la metodología de Magerit.

Para los riesgos de las zona baja (B), se recomienda aceptarlos, siempre y cuando estén monitorizados y en continua observación ya que estos pueden ser cambiantes y aumentar su posición de riesgo o de impacto.

Para los riesgos de la zona media (M) se recomienda asimilarlos y evitarlos, estos al igual que los de rango medio pueden estar en constante monitorización y analizar periódicamente en caso de que este aumente o disminuya.

Para los riesgos de Zona Media (M) y Extrema(E) se recomienda usar los tratamientos descritos en la matriz de riesgo e impacto los cuales son:

- **Reducir:** Minimizar los riesgos mediante métodos de respaldo, mantenimiento, de mejora o reparación del elemento en peligro a fin de bajar las probabilidades de ocurrencia del problema.
- **Evitar:** Es decir desviar el riesgo o cambiar su objetivo a un punto importante del sistema, esto se puede lograr mediante movimientos físicos o sistemáticos del riesgo, pedir ayuda a terceros para compartir la carga.
- **Eliminar:** Consiste en su propia palabra, deshacernos del problema desde la raíz, sea necesario invertir en reparaciones o mejoras, eliminar el riesgo y su propagación.

Respuesta y decisión de los Directivos

Actualmente no se ha presentado el documento a la directiva o encargado de la empresa por lo tanto aun no contamos con la decisión de los altos cargos.

Amenaza	Zona de Riesgo	
	Alta	Extrema
Incendios	1	0
Desastres Naturales	2	1
Mal Uso del Software	2	0
Fallas en la Infraestructura de la Red	0	1

3.3.1 Tratamiento del riesgo

Si los encargados o directivos de la empresa deciden actuar según el documento es muy probable que no cuente con los estudiantes dueños de este informe y todos sus cambios o decisiones y movimientos sean internos a la empresa. Esto fundamentado en que la empresa es una empresa hermética es decir no sale información importante o mejor dicho no sale información que la empresa no desee hacer pública.

3.2Costos en Seguridad Informática

Tipo de Recurso	Descripcion del Recurso	Valor Mensual	Valor anual
Recurso Humano	Vigilantes del Centro de Datos 24 horas	L.15,000	L.180,000
	Administrador de servicios	L.10,000	L.120,000
	Hacker Etico para testear seguridad	L.20,000 (Único pago)	
	Soporte Tecnico	L.15,000	L.180,000
Recurso Tecnologico	Pago por certificado HTTPS	L.375	L.4500
	Hosting anti-ddos	L.400	L.4800
	Licencia de Antivirus	L.465	L.5580
	Licencia paquete Office	L.1400	L.16,800

3.3Conclusiones y recomendaciones

Conclusiones

- Se logro definir cuáles eran los principales problemas que presenta la empresa en la seguridad informática, principalmente en su oficina principal y el data center
- Se creo un plan de contingencia, de prevención y de emergencia tomando en cuanta una cantidad N de situaciones posibles con una cantidad N de variables para cubrir el espectro más amplio posible.
- Se puso en práctica la Metodología Magerit en base a los datos que fueron proporcionados por la empresa

Recomendaciones

- Se recomienda el reacondicionamiento de las instalaciones físicas de la oficina y el data center ya que no cumple con algunos requerimientos
- Se recomienda la creación de un departamento de seguridad informática
- Se recomienda una capacitación para los técnicos e ingenieros para dar a conocer los conceptos básicos de la seguridad informática en caso de cualquier emergencia

• 3.4 Bibliografía

- MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método
- MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas
- AUDITORÍA DE SEGURIDAD INFORMÁTICA-Álvaro Gómez Vieites
- SEGURIDAD INFORMÁTICA. BASICO
- Enciclopedia De La Seguridad Informática Segunda Edición