Universidad Católica De Honduras

"Nuestra Señora Reina De La Paz"

Campus Santiago Apóstol

Asignación:
Tercer entregable

Catedrático:
Ing. Patricia Medina

Asignatura:
Seguridad informática y gestión de riesgos

Integrantes:

Nombre	Nº de cuenta
Nicolle Nayeli Benavides Ardón	0801-2001-09649
Angel David Quintanilla Ferrufino	0704-2003-00059
Carlos Alberto Ardón Izaguirre	0703-2001-03774
Luis Adolfo Flores Castellanos	0703-2000-03793

Fecha:
19 de julio de 2022

Danlí, El Paraíso

Análisis de evaluación de riesgo de la empresa Mi Pyme Financiero S de R.L de C.V

Índice

Introducción

El objetivo principal de la seguridad informática es llevar a cabo la prevención y detección de acceso y eventual uso malicioso a sistemas informáticos y sus recursos por parte de terceros, anónimos e incluso a veces personas pertenecientes a la misma organización.

Por ello, la importancia de la seguridad informática de las empresas radica esencialmente en que la utilización maliciosa de sus sistemas de información privados y de los recursos internos puede acarrear desastrosas consecuencias en todas las áreas de la organización, deviniendo en problemas tanto productivos como financieros. Por ende, la seguridad informática de las empresas debe estar dirigida a prevenir las amenazas y los riesgos a los sistemas de información internos.

Por estas razones el presente informe expondrá el análisis de sistemas de información de seguridad y riesgos de la empresa Mi Pyme Financiero S de R.L de C.V y como se podría implementar una mejora para dicho sistema.

Por consiguiente, para llevar a cabo el análisis de dicho proyecto se utilizará la metodología Magerit para poder evaluar y gestionar los riesgos de una manera más óptima y, asimismo, analizar el impacto que puede influir en la empresa. Dicha metodología Magerit ayuda a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.

Objetivos

Objetivo general

- ✓ Conocer cuáles son los sistemas de seguridad, y la administración de los procesos relacionados con la gestión de los riesgos empleados en la compañía Mi Pyme financiera.

Objetivos específicos

- ✓ Conocer los procesos de seguridad en funcionamiento de la compañía.
- ✓ Comprender los protocolos de seguridad de la información que se implementan.
- ✓ Afianzar los conocimientos de la metodología Magerit.
- ✓ Analizar cuáles son las posibles fallas de seguridad que posee la empresa al no hacer una correcta documentación de los procesos.

Planteamiento del problema

Todo lo que engloba la seguridad informática siempre ha sido de suma importancia debido a que es en lo que se relacionan las personas todos los días, existen muchos factores de riesgos a los que estamos expuestos a diario, con el paso del tiempo cada uno de debilidad en la seguridad ha seguido tomando fuerza, entre ellos tenemos virus, hackers, vulnerabilidad de los sistemas, lo cual tiene como consecuencias que para asegurar la seguridad de nuestros usuarios/clientes se tenga que estar en constante actualización de los protocolos de seguridad que se implementan en las instituciones/empresas o compañías.

De esta manera se hace un énfasis en la compañía Mi Pyme Financiera ya que es una compañía que brinda servicios de pagos diarios, refinanciamiento, represtamos, recaudación de cuotas y desembolsos, lo cual implica que deben dar prioridad los procesos de seguridad y a la gestión de los mismos, ya que como tal no existe una correcta documentación establecida, y tampoco se cuentan con protocolos de seguridad antes posibles fallas en la seguridad de la información, es claro que es un problema para la compañía y que debe ser solucionado.

Justificación

En términos generales, dicho proyecto será de suma importancia para el aseguramiento de lo que es la seguridad informática en la empresa Mi Pyme Financiera, que actualmente carece de ciertas documentaciones en cuanto a sus protocolos y actividades.

Los beneficios que aportará la implementación de este proyecto está el incremento en la adaptación de los nuevos empleados a sus labores ya que contarán con una descripción detallada de los protocolos que puedan necesitar, una mejora en lo que es la capacitación de los empleados ya que actualmente estos protocolos solo son enseñados mediante una capacitación oral, es decir sin contar con explicaciones por escrito, así mismo se espera un incremento en la seguridad tanto del hardware como el software en la empresa ya que si los empleados saben bien como manipular los sistemas físicos e informáticos el que estos comentan un error perjudicial al manipularlos será un evento aislado o que no se producirá.

Este proyecto no solo será de utilidad en casos de capacitación, sino que también puede ser de utilidad en momentos de crisis si es que es necesaria la intervención de uno de los protocolos, ya que en momentos de pánico es vital no cometer errores por lo que tener una documentación del protocolo o medida a efectuar es de suma importancia.

La comunicación con la empresa es algo que se nos facilita en gran medida ya que contamos con un buen contacto en ella, así como con el apoyo de la misma en lo que es la implementación de este proyecto.

Marco conceptual

Seguridad informática

La seguridad informática —también llamada ciberseguridad—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.

Metodología MAGERIT

Una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos. Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Análisis de riesgos

Un análisis de riesgo es la apreciación detallada de todo lo que pueda implicar peligro para la empresa. Es decir, de cualquier detalle que pueda causar un inconveniente sea financiero o funcional. Una metodología de análisis de riesgos es un procedimiento mediante el cual se realiza un análisis de riesgo para conocer sus causas y consecuencias. Es organizar toda la información necesaria que sirva de lumbrera para saber si la situación es conveniente o no para la empresa.

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.

Medidas de seguridad o salvaguardas

Una medida de seguridad o salvaguarda es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.

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.

Sistema de gestión de la seguridad de la información

Es un conjunto de políticas de administración de la información. El término se denomina en inglés "Information Security Management System" (ISMS).

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 Commission.

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.

Normas ISO en la seguridad

Las normas ISO de Gestión de la Seguridad de la Información se denominan familia de normas ISO 27000 y son las siguientes:

- ✓ **ISO 27001**: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Es la norma con arreglo a la cual se certifican por auditores externos. Su Anexo A, enumera en forma de resumen los objetivos de control y controles

que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Esta norma está publicada en España como UNE-ISO/IEC 27001:2007. Otros países donde también está publicada en español son, por ejemplo, Colombia, Venezuela y Argentina.

- ✓ **ISO 27002**: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- ✓ **ISO 27005**: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ✓ **ISO 27006**: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.
- ✓ **ISO 27000**: Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de la Seguridad de la Información (SGSI). Generalidades y vocabulario.
- ✓ **ISO 27003**: Sistema de Gestión de la Seguridad de la Información (SGSI). Guía de implantación.
- ✓ **ISO 27004**: Tecnología de la información. Técnicas de Seguridad. Gestión de la Seguridad de la Información. Métricas.
- ✓ **ISO 27007:** Tecnología de la información. Técnicas de Seguridad. Guía de auditoría de un SGSI. Iniciadas las votaciones al DIS (cinco meses).

Marco teórico

Información general de la empresa

- ✓ *Nombre de la empresa:* Mi Pyme Financiera S de R.L de C.V.
- ✓ *Propietarios:* Lic. Donal Solórzano y Lic. César Salgado.
- ✓ *Dirección:* Calle del canal, contiguo a Librería Don Quijote; Danlí, El Paraíso.
- ✓ *Rubro de la empresa:* Empresa Financiera.
- ✓ *Teléfono:* 2763-2042
- ✓ *Correo electrónico:* rrhh@mipymefinanciero.com

Servicios que ofrece

- ✓ ***Pagos diarios:*** Es un sistema de pago en cuotas diarias fijas pactadas, en el cual pasa un cobrador todos los días por el domicilio de su comercio.
- ✓ ***Pagos semanales:*** Lo préstamos con abonos semanales, para personas que cobran sus salarios bajo la misma modalidad o quincenalmente.
- ✓ ***Refinanciamiento:*** Consiste en modificar las condiciones iniciales de un crédito e implica cambiar los términos del contrato mediante el cual se estructuró el mismo, tales como plazos.
- ✓ ***Représtamos:*** Los représtamos será el proceso mediante el cual se otorgará un nuevo crédito, reafirmando una buena relación comercial, fidelización y de servicio al cliente.
- ✓ ***Recaudación de cuotas:*** El cliente deberá haber cancelado el 50% de su monto para poder realizar una recaudación de cuotas.
- ✓ ***Desembolsos:*** Se realizarán al momento de la contratación del crédito en un solo desembolso, y se realizarán en campo, es decir en el negocio del cliente, considerando la accesibilidad, el monto del crédito y la seguridad de la zona.

Misión de la empresa

"Somos una empresa responsable, que se dedica a impulsar el crecimiento sostenible de las pequeñas y medianas empresas, brindándoles nuestros servicios de microcréditos, con pagos accesibles".

Visión de la empresa

"En 10 años ser una de las empresas líderes a nivel nacional en micro finanzas; satisfaciendo las necesidades de los clientes, velando por la correcta inversión del capital, que contribuye al desarrollo del país, con personal confiable y altamente capacitado".

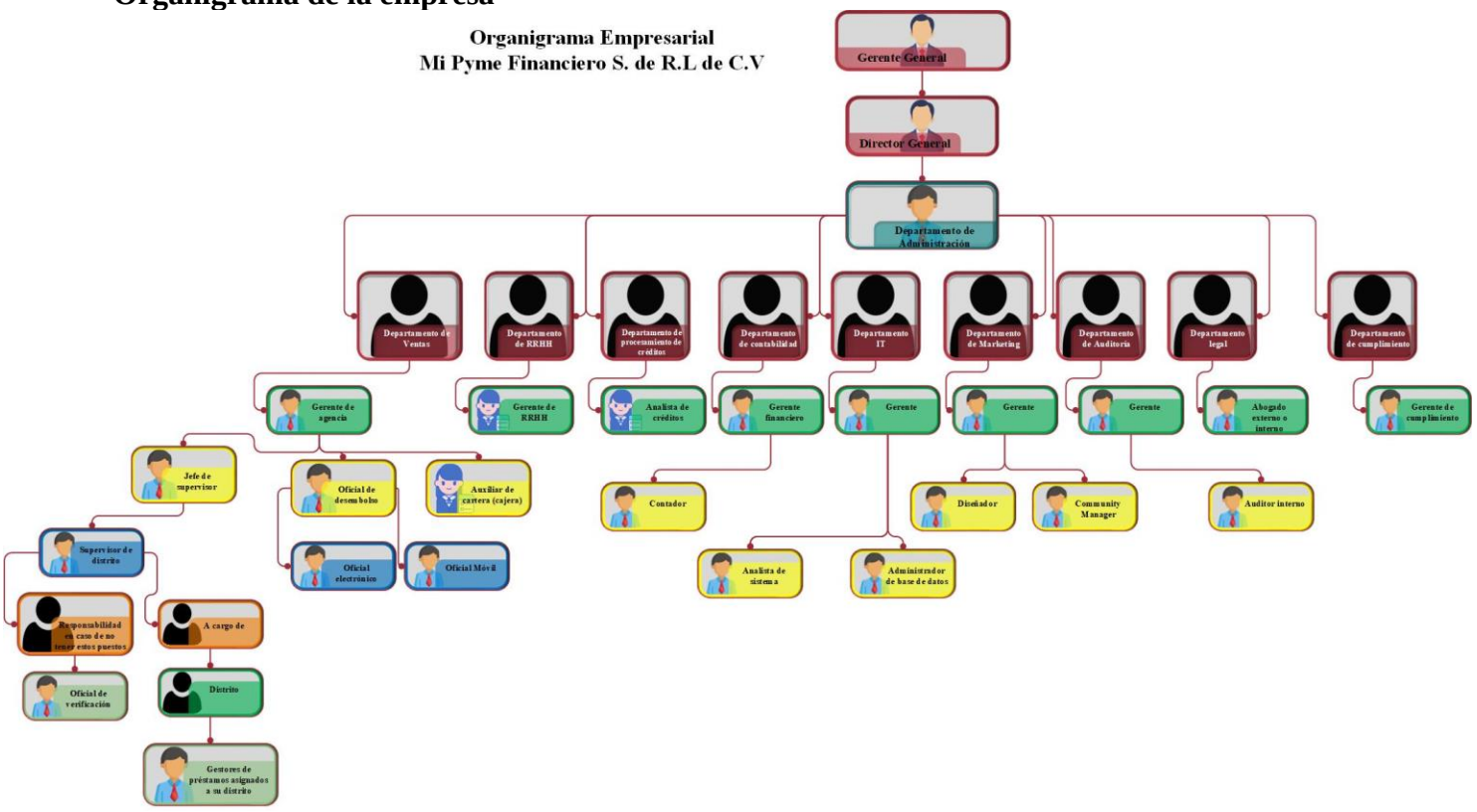
Valores de la empresa

- ✓ Principios Cristianos
- ✓ Compromiso
- ✓ Honestidad
- ✓ Trabajo en Equipo

Historia de la empresa

El 1 de octubre del año 2018 Mi Pyme Financiero surge por parte del Licenciado en Administración de empresas Donal Amahel Solórzano, el cual tenía la idea de una empresa que pudiera ayudar a financiar a todo aquel emprendedor, con una micro o mediana empresa. Pero, no contaba con la capacidad monetaria necesaria para poder aperturar una empresa de esta dimensión; por lo tanto comenzó dando créditos de pequeñas cantidades a personas cercanas ahí formo su pequeña empresa llamada "Creciendo juntos", con la cual al ver el resultado positivo de sus ganancias decidió buscar personas que quisieran invertir en su empresa, de esta manera conoció al que hoy es el gerente general de la empresa Cesar Rodolfo Salgado, quien ayudo a mejorar la idea de el Lic. Amahel, los cuales pasaron a ser fundadores de la empresa. El 2 de enero del 2019 paso de ser llamada "Creciendo juntos" a "Mi Pyme financiero S. de R.L de C.V." y se decidió que el antiguo nombre pasaría a ser el eslogan de la empresa, hoy en día se cuenta con un gran equipo conformado por 53 colaboradores altamente capacitados y responsables de darle al cliente una atención de calidad.

Organigrama de la empresa



Planificación

Planeación de la seguridad informática en la planeación

En este apartado se trabajará lo que compete la definición de los alcances del estudio informando a cada uno del personal implicado con las actividades de la empresa. Así mismo identificando cuales son los activos principales de los servicios más importantes, conociendo información relevante del sistema como su funcionalidad tanto administrativa como financieramente.

Debemos tener en consideración los problemas y amenazas en lo que respecta la seguridad de la información para tratar de disminuir la concurrencia de incidentes en la compañía, de esta manera logrando reducirlos lo máximo posible.

Tomar las medidas de seguridad necesarias implica tener en cuenta cada uno de los pasos a seguir para que las actividades se sigan haciendo en su orden normal sin afectar el rendimiento de la compañía. Los encargados de la supervisión y manejo de los protocolos de seguridad deben conocer a fondo el sistema, de esa manera saber cuáles son vulnerabilidades, y cómo manejar el sistema.

Para que el control de los riesgos sea exitoso, se debe de mantener una constante revisión diaria y monitoreo de las mismas para verificar que todo se está realizando de la manera correcta evitando el riesgo en la seguridad de la información.

Algunas decisiones que podemos tomar en cuenta son las siguientes:

- Establecer e implantar un plan de tratamiento de riesgos.
- Implementar los controles anteriormente seleccionados.
- Definir un sistema de métricas para medir la eficacia de los controles.
- Implantar procedimientos para detectar y resolver los incidentes de seguridad.

Alcance del análisis y evaluación de riesgos del sistema informático

El alcance establecido para el análisis, son lograr evaluar los niveles de seguridad que maneja la financiera **My Pime** ubicados en Danlí, El Paraíso se intenta darle una orientación basada en identificar las diferentes vulnerabilidades con las que cuenta la empresa de igual manera se trata también analizar el nivel de seguridad que tiene la información que se maneja, los respectivos accesos al sistema, los usuarios, la confidencialidad de la información al igual que al ingreso del establecimiento, entre otras actividades de seguridad.

Como resultado se espera obtener las diferentes amenazas que pueden afectar a la empresa de esa manera lograr implementar un plan de gestión de riesgos para evitar toda amenaza, actividad maliciosa o incidente que pueda presentarse a futuro logrando evitar posibles pérdidas a la compañía; manteniendo así en óptimas condiciones seguridad las actividades de la misma.

Objetivos del análisis y evaluación de riesgos del Sistema Informático.

- Hacer un análisis exhaustivo sobre el estado de la documentación de los protocolos y procesos, para saber dónde tienen fallas y así saber qué puntos mejorar.
- Buscar la manera más adecuada para poder realizar la documentación de manera que sea entendible para cualquier usuario.
- Exponer los beneficios que traen a la empresa el de tener estos procesos documentados.
- Inculcar el uso de estos procesos en las futuras capacitaciones al personal.

Análisis de riesgos

Descripción de los activos de la empresa

Activo	Descripción
Computadoras	La empresa cuenta con muchos dispositivos que se encuentran conectados a la red para realizar diferentes funciones en la empresa como facturar, revisión de cuentas ingreso de clientes nuevos, revisión de correos electrónicos, tener un control de las finanzas y las cámaras de seguridad.
Celulares	La mayoría de los empleados cuenta con un celular que proporciona la empresa al gerente general, supervisor, gerente de distrito y a los gestores que se encargar de realizar los cobros de los diferentes préstamos.
Impresoras	Dispositivos conectados a la red cuya función es imprimir cosas como: facturas, hojas de resultados, hojas de trabajo, recibos de planilla, recibos de caja, sobres para los resultados, e informes.
Televisor	Dispositivo para proyectar las presentar informes de la empresa cuando realizan reuniones de suma importancia
Centro de Computo	El centro de cómputo de la empresa cuenta con un aire acondicionado con la capacidad de 18 btu y un UPS forza 750 VA, Switch y router.
Servidor	La empresa con servidores virtual el cual está ubicado en USA el cual usan para producción y desarrollo.

Características de los activos de la empresa

Activo	Características
Computadoras	Monitor Dell P190SD 8 / 4 GB de RAM Teclado Weibo FC-530 Mouse Pad Argom Cable HDMI 1 M Win 7 professional Procesador i3

Celulares	Marca Huawei Android 10 6 GB de RAM 4200 mA
Memorias USB	Memorias Kingston 16 GB Memoria Adata 16 GB
Aire Acondicionado	Aire Acondicionado LG de 18,000 BTU Dual Inverter Modelo: VM182C6
Impresoras	Impresora Canon Multifuncional Láser Monocromática Tecnología de conectividad: Wifi
Switch	Switch Gigabit TP-Link no administrable de 24 puertos 10/100/1000 Mbps. Capacidad de conmutación de 48 Gbps
Router	Huawei Wifi Mesh 3AX3000
Televisor	LG Televisor 50 in Smart TV

Valoración de los activos de la empresa

Clasificación de la confidencialidad

Principio de seguridad	Clasificación	Definición
Confidencialidad	*Público* ***(1)***	Este activo es considerado de carácter público y puede ser divulgado a cualquier persona o entidad interna o externa a la empresa.
	Interna ***(2)***	Este activo es utilizado por los funcionarios autorizados de la empresa para la ejecución de sus labores, y no puede ser conocida por terceros sin autorización del responsable del activo de información o directivas de la empresa.
	Confidencial ***(3)***	Este activo se considera altamente sensible y es utilizada por solo un grupo limitado de funcionarios o áreas para la ejecución de labores y no puede ser conocida por otros funcionarios de la empresa o terceros externos sin

		autorización especial del responsable de la información o directivas de la empresa.
Integridad	*No sensitiva* ***(1)***	La pérdida o modificación no autorizada de este activo podría causar un daño leve o nulo para la empresa.
	Sensitiva ***(2)***	La pérdida o modificación de este activo podría causar un daño que genera perjuicios importantes que afecten a la empresa, pero puede ser absorbido o asumido por este.
	Altamente sensitiva ***(3)***	La pérdida o modificación de este activo podría causar un daño grave que genere perjuicios que afecten significativamente a la empresa y que difícilmente podrían ser asumidos por ésta.
Disponibilidad	*No critico* ***(1)***	El activo puede no estar disponible por un periodo de tiempo extendido, sin afectar la operación de la empresa.
	Importante ***(2)***	La no disponibilidad de este activo afectaría operaciones y servicios de los funcionarios.
	Misión crítica ***(3)***	La no disponibilidad de este activo afectaría significativamente las operaciones, servicios de la empresa y el acceso a la información.

Valoración y confidencialidad de los activos

Activos	**Valoración de confidencialidad**				
	Descripción	***C***	***I***	***D***	***Valor final***
Computadoras	Este activo es esencial y necesario para el óptimo desempeño de la empresa.	1	3	3	3
Celulares	Muy importante para la empresa	1	1	1	1
Impresoras	Importante para la empresa.	1	2	2	2
Televisor	Importante para la empresa.	2	1	1	1
Centro de cómputo	Muy importante para la empresa.	3	3	3	3
Servidor	Este activo es esencial y necesario para el óptimo desempeño de la empresa.	3	3	3	3
Información	Este activo es fundamental para la compañía.	3	3	3	3

Identificación de amenazas

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

Estimación de las probabilidades

Valor	Descripción
1	Es muy improbable que la amenaza ocurra 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.

Listado de amenazas

Id	Amenaza	Descripción	P	Razón de Clasificación.
A1	Daños físicos al activo.	Daños que son generados a los activos de la empresa ya sea por algún golpe recibido o dejado caer.	4	A menudo ocurren algunos daños físicos dentro de las empresas por parte de empleados o ladrones.
A2	Daños de software al active.	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.
A3	Virus, gusanos y ransomware.	Daños generados por la implantación de algún virus, gusanos o ransomware en los activos de la empresa como las computadoras.	4	Es muy probable que los empleados conecten algún disco externo que contenga virus o descarguen alguno al utilizar las computadoras.
A4	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.

A5	Desperfectos al equipo	Fallos que se pueden ocasionar por algún equipo que venga mal de fábrica y tenga algún defecto.	2	Es muy probable que se compren activos que estén en mal estado o que no funcionen adecuadamente.
A6	Fallas de Escaneo	Fallas generadas por el mal escaneo al utilizar la impresora.	5	Es muy probable que se den casos donde se realice un escaneado mal de documentos.
A7	Fallo de configuración	Fallas que puedan ocurrir en el presente o futuro en los activos debida a la mala instalación y configuración del activo.	3	Algunos activos se instalan de forma incorrecta y provocan demoras en las tareas de la empresa.
A8	Fallas al imprimir	Mala impresión de páginas al utilizar la impresora al generar facturas u otros documentos.	5	Siempre las impresoras fallan al momento de imprimir por una innumerable cantidad de razones.
A9	Secuestro de registros	Secuestro de información por parte de personas de los servidores o computadoras.	1	No hay mucha competencia ni ha habido tantos secuestros de registros en Honduras.
A10	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.
A11	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, en algunas ocasiones pueden sobrecargarse por exceso de información.
A12	Problemas por contraseñas	Problemas ocurridos por el acceso a otras personas por los empleados al utilizar contraseñas con un menor.	3	Los empleados siempre buscan alguna contraseña fácil de colocar o fácil de débiles nivel de seguridad recordar y descifrar.
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.	4	Es muy frecuente que se den casos en donde los empleados olviden sus credenciales para utilizar el sistema.
A14	Inundaciones	Fugas de agua o inundaciones ocasionados por ríos cercanos a la empresa o desastres naturales.	1	Siempre hay casos de desastres naturales que pueden ocurrir ya que no se está exentos de ellos.
A15	Terremotos	Movimientos súbitos de la tierra que podrían ocasionar	1	Se pueden presentar temblores o terremotos en raras ocasiones.

		la caída física de activos o daño a la infraestructura de la empresa.		
A16	Fuegos	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.
A17	Error Humano	Fallos ocasionados por los errores que los empleados podrían ocasionar.	5	Siempre puede ocurrir un imprevisto o error al utilizar dispositivos de una manera o con un fin incorrecto.

Amenazas clasificadas por su nivel y tipo de probabilidad

A continuación, las amenazas y la división de ellas que se presentan en la siguiente tabla fueron clasificadas por medio de los activos que puedan afectar dentro de la compañía. Hay algunas amenazas que atacan a ciertos equipos, sin embargo, a otros no.

Asimismo, por cada amenaza identificada por equipo se le asignó un criterio de probabilidad que fue evaluado por cuantas veces esta amenaza podría ocurrir en la empresa en ciertas cantidades de tiempo. En este caso 1 siendo el valor de que es poco probable y 5 siendo de que la amenaza ocurra cada mes.

Estimación de la probabilidad de las amenazas

Valor	Descripción
1	Es muy improbable que la amenaza ocurra 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.

Identificación de amenazas y criterio de probabilidad

Activo	Descripción de amenazas			Criterio de probabilidad
	ID	Amenazas	Tratamiento del Riesgo	Probabilidad
Celulares	A1	Daños físicos al activo.	Uso de protector y cristal de protección.	3
	A5	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	1
	A10	Phishing	Prohibir navegación en sitios no autorizados.	4
	A12	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	4
	A13	Problemas por olvido o robo de cuentas.	Cambio de contraseñas sin autorización prohibido.	3
Centro de Cómputo	A1	Daños físicos al activo.	Cumplir con los estándares y normas de seguridad establecidos.	2
	A4	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	5
	A5	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	2
	A14	Inundaciones	Siempre verificar que no se dejen grifos abiertos.	1
	A15	Terremotos	Contar con un plan de acción en caso de desastre.	1
	A16	Fuegos	Contar con un extintor de polvo químico seco.	1
Computadoras	A1	Daños físicos al activo.	Cumplir con los estándares y normas de seguridad establecidos.	2
	A2	Daños de software al Activo.	Contar con capacitaciones y manuales sobre el buen uso del software.	5
	A3	Virus, gusanos y ransomware.	Contar con un buen antivirus y cumplir con las medidas de navegación en la red segura.	3
	A5	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	2
	A7	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	2
	A9	Secuestro de registros.	Establecer jerarquía de acceso a la información.	1

	A10	Phishing	Prohibir navegación en sitios no autorizados.	4
	A12	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	4
Impresoras	A4	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	5
	A6	Fallas de Escaneo.	Contar con una capacitación para el uso adecuado del equipo.	3
	A7	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	2
	A8	Fallas al imprimir.	Revisar que todo esté en orden con la impresora a la hora de imprimir.	4
	A17	Error humano.	Utilizar la impresora solo para fines laborales.	2
Servidor	A4	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	5
	A7	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	2
	A5	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	2
	A11	Caídas del activo por sobrecargas.	Tratar de evitar en la medida de lo posible la carga excesiva de información.	3
	A12	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	4
Televisores	A1	Daños físicos al activo.	Cumplir con los estándares y normas de seguridad establecidos.	2
	A5	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	2
	A7	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	2
Información	A1	Daños físicos al activo	Cumplir con los estándares y normas de seguridad establecidos.	2
	A9	Secuestro de registros.	Establecer jerarquía de acceso a la información.	1
	A10	Phishing	Prohibir navegación en sitios no autorizados.	4
	A17	Error humano.	Utilizar la impresora solo para fines laborales.	2

Matriz de impacto potencial

Por consiguiente, una vez identificada las amenazas por activo, se les asignó un criterio de impacto a estas amenazas. El impacto se refiere a que tan dañino es que cada una de estas amenazas ocurran, y que tanto puedan afectar a la empresa esta amenaza al dañar el activo. La evaluación se hizo de 1 siendo el valor de que no tendría consecuencias si este activo se daña por cierto tiempo y 3 siendo el valor más alto que al dañarse este activo, la empresa no podría seguir con sus actividades laborales.

Estimación de impacto

Valor	Descripción
1	El daño derivado de la materialización de la amenaza no tiene consecuencias poco relevantes para la organización.
2	El daño derivado de la materialización de la amenaza tiene consecuencias relevantes para la organización.
3	El daño derivado de la materialización de la amenaza tiene consecuencias muy relevantes para la organización.

Impacto potencial

Activo	Descripción de amenazas		Criterio de impacto
	ID	Amenazas	Impacto
Celulares	A1	Daños físicos al activo.	2
	A5	Desperfectos al equipo.	1
	A10	Phishing	2
	A12	Problemas por contraseñas.	3
	A13	Problemas por olvido o robo de cuentas.	1
Centro de Cómputo	A1	Daños físicos al activo.	2
	A4	Problemas de red.	3
	A5	Desperfectos al equipo.	2
	A14	Inundaciones	3
	A15	Terremotos	3
	A16	Fuegos	3
Computadoras	A1	Daños físicos al activo.	2

	A2	Daños de software al Activo.	3
	A3	Virus, gusanos y ransomware.	3
	A5	Desperfectos al equipo.	2
	A7	Fallos de configuración.	2
	A9	Secuestro de registros.	3
	A10	Phishing	2
	A12	Problemas por contraseñas.	3
Impresoras	A4	Problemas de red.	3
	A6	Fallas de Escaneo.	3
	A7	Fallos de configuración.	2
	A8	Fallas al imprimir.	2
	A17	Error humano.	3
Servidor	A4	Problemas de red.	3
	A7	Fallos de configuración.	3
	A5	Desperfectos al equipo.	2
	A11	Caídas del activo por sobrecargas.	2
	A12	Problemas por contraseñas.	3
Televisores	A1	Daños físicos al activo.	2
	A5	Desperfectos al equipo.	2
	A7	Fallos de configuración.	2
Información	A1	Daños físicos al activo	2
	A9	Secuestro de registros.	3
	A10	Phishing	2
	A17	Error humano.	3

Riesgo potencial

Posteriormente luego de haber obtenido el impacto y la probabilidad de amenazas que nuestros activos pueden llegar a tener llevaremos a cabo un procedimiento para obtener nuestro riesgo potencial. El riesgo potencial es el producto del impacto y la probabilidad. Luego el valor

que tenemos, lo debemos de comparar con la matriz de potencial de riesgo la cual visualizaremos a continuación.

Matriz de potencial de riesgos				
		Impacto		
		Bajo (B)	*Medio (M)*	*Grave (G)*
Probabilidad	***Valor***	**1**	**2**	**3**
Casi seguro (CS)	**5**	5	10	15
Alto (A)	**4**	4	8	12
Media (M)	**3**	3	6	9
Baja (B)	**2**	2	4	6
Rara (R)	**1**	1	2	3

Simbología

	Riesgo intolerable **(IN)**
	Riesgo importante **(I)**
	Riesgo moderado **(M)**
	Riesgo tolerable **(T)**

Estimación del impacto y probabilidad					
Activo	**Riesgo**	**Impacto**	**Probabilidad**	**Valor**	**Nivel de riesgo**
Celulares	Daños físicos al activo.	2	3	6	I
	Desperfectos al equipo.	1	1	1	T
	Phishing	2	4	8	I
	Problemas por contraseñas.	3	4	12	IN
	Problemas por olvido o robo de cuentas.	1	3	3	M
Centro de cómputo	Daños físicos al activo.	2	2	4	M
	Problemas de red.	3	5	15	IN
	Desperfectos al equipo.	2	2	4	M
	Inundaciones	3	1	3	M
	Terremotos	3	1	3	M
	Fuegos	3	1	3	M
Computadoras	Daños físicos al activo.	2	2	4	M
	Daños de software al Activo.	3	5	15	IN
	Virus, gusanos y ransomware.	3	3	9	I
	Desperfectos al equipo.	2	2	4	M
	Fallos de configuración.	2	2	4	M

	Secuestro de registros.	3	1	3	M
	Phishing	2	4	8	I
	Problemas por contraseñas.	3	4	12	IN
Impresoras	Problemas de red.	3	5	15	IN
	Fallas de Escaneo.	3	3	9	I
	Fallos de configuración.	2	2	4	M
	Fallas al imprimir.	2	4	8	I
	Error humano.	3	2	6	I
Servidor	Problemas de red.	3	5	15	IN
	Fallos de configuración.	3	2	6	I
	Desperfectos al equipo.	2	2	4	M
	Caídas del activo por sobrecargas.	2	3	6	I
	Problemas por contraseñas.	3	4	12	IN
Televisores	Daños físicos al activo.	2	2	4	M
	Desperfectos al equipo.	2	2	4	M
	Fallos de configuración.	2	2	4	M
Información	Daños físicos al activo	2	2	4	M
	Secuestro de registros.	3	1	3	M
	Phishing	2	4	8	I
	Error humano.	3	2	6	I

Numero de amenaza por zona de riesgo y tipo de activo

En la tabla que se muestra a continuación se encuentran seccionadas las amenazas por el tipo de riesgo y activos, mostrando primero los riesgos marginales seccionados por los activos y a su vez cada uno de los activos con sus riesgos, para luego poner la cantidad de riesgos que hay en cada activo, y de igual forma en cada uno de los seis activos.

Número de amenazas por potencial de riesgo y tipo de activo		
Riesgo Tolerable		
Activos	**Riesgos**	**Total**
Celulares	Desperfectos al equipo.	1
Total de Riesgos Tolerables		**1**
Riesgo Moderado		
Celulares	Problemas por olvido o robo de cuentas.	1

Centro de Computo	Daños físicos al activo	5
	Desperfectos al equipo.	
	Inundaciones	
	Terremotos	
	Fuegos	
Computadoras	Desperfectos al equipo.	3
	Fallos de configuración.	
	Secuestro de registros.	
Impresoras	Fallos de configuración.	1
Servidor	Desperfectos al equipo.	1
Televisores	Daños físicos al activo.	3
	Desperfectos al equipo.	
	Fallos de configuración.	
Información	Daños físicos al activo	2
	Secuestro de registros.	
Total de Riesgos Tolerables		**17**
Riesgo Importante		
Celulares	Daños físicos al activo.	2
	Phishing.	
Computadoras	Virus, gusanos y ransomware.	2
	Phishing.	
Impresoras	Fallas de Escaneo.	3
	Fallas al imprimir.	
	Error humano.	

Servidor	Fallas de configuración.	2
	Caídas del activo por sobrecarga.	
Información	Phishing.	2
	Error humano.	
Total de Riesgos Importantes		11
Riesgo Intolerable		
Celulares	Problemas por contraseñas.	1
Centro de Computo	Problemas de red.	1
Computadoras	Daños de software al Activo.	2
	Problemas por contraseñas.	
Impresoras	Problemas de red.	1
Servidor	Problemas de red.	2
	Problemas por contraseñas.	
Total de Riesgos Intolerables		**7**
Total de Riesgos		**36**

Matriz de riesgo potencial

En la siguiente representación se da a demostrar una combinación de los siguientes datos: tabla de Riesgo Potencial y la Tabla de matriz de impacto potencial mostrando lo que compete el código de amenaza, la descripción de la amenaza, de igual manera información importante como ser: el nivel de impacto, nivel de probabilidad, riesgo potencial y la zona de riesgo.

Activo	Código de Amenaza	Amenazas	Impacto	Probabilidad	Riesgo Potencial	Zona de Riesgo
Celulares	A1	Daños físicos al activo.	2	3	6	Moderado
	A5	Desperfectos al equipo.	1	1	1	Tolerable
	A10	Phishing	2	4	8	Importante
	A12	Problemas por contraseñas.	3	4	12	Intolerable
	A13	Problemas por olvido o robo de cuentas.	1	3	3	Moderado

Centro de Cómputo	A1	Daños físicos al activo.	2	2	4	Moderado
	A4	Problemas de red.	3	5	15	Intolerable
	A5	Desperfectos al equipo.	2	2	2	Tolerable
	A14	Inundaciones	3	1	3	Moderado
	A15	Terremotos	3	1	3	Moderado
	A16	Fuegos	3	1	3	Moderado
Computadoras	A1	Daños físicos al activo.	2	2	2	Tolerable
	A2	Daños de software al Activo.	3	5	15	Intolerable
	A3	Virus, gusanos y ransomware.	3	3	9	Importante
	A5	Desperfectos al equipo.	2	2	4	Moderado
	A7	Fallos de configuración.	2	2	4	Moderado
	A9	Secuestro de registros.	3	1	3	Moderado
	A10	Phishing	2	4	8	Importante
	A12	Problemas por contraseñas.	3	4	12	Intolerable
Impresoras	A4	Problemas de red.	3	5	15	Intolerable
	A6	Fallas de Escaneo.	3	3	9	Importante
	A7	Fallos de configuración.	2	2	4	Moderado
	A8	Fallas al imprimir.	2	4	8	Importante
	A17	Error humano.	3	2	6	Importante
Servidor	A4	Problemas de red.	3	5	15	Intolerable
	A7	Fallos de configuración.	3	2	6	Importante
	A5	Desperfectos al equipo.	2	2	4	Moderado

	A11	Caídas del activo por sobrecargas.	2	3	6	Importante
	A12	Problemas por contraseñas.	3	4	12	Intolerable
Televisores	A1	Daños físicos al activo.	2	2	4	Moderado
	A5	Desperfectos al equipo.	2	2	4	Moderado
	A7	Fallos de configuración.	2	2	4	Moderado
Información	A1	Daños físicos al activo	2	2	4	Moderado
	A9	Secuestro de registros.	3	1	3	Moderado
	A10	Phishing	2	4	8	Importante
	A17	Error humano.	3	2	6	Importante

Salvaguardas o controles existentes

Luego de establecer los riesgos potenciales a los activos se prosigue a definir las salvaguardas o controles existentes que existen para proteger a los activos en el caso de una posible amenaza. La efectividad de los controles se dividió en 3 niveles: el nivel 1 representa la menor cantidad de efectividad, el nivel 2 representa una cantidad regular de efectividad, y el nivel 3 representa la mayor cantidad de efectividad.

Nivel	Descripción de la efectividad del control
1	Es muy probable que el control falle ante la presencia de una amenaza.
2	El control es funcional y es probable que funcione en la mayoría de los casos en los que haya algún tipo de amenaza.
3	Está garantizado que el control va a funcionar y va a cumplir con los niveles de protección necesarios para proteger los equipos.

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

En la siguiente tabla se definen los niveles de efectividad de los controles implementados a cada activo con sus posibles amenazas y su nivel de efectividad. Primero se especifica el activo, luego se especifican sus posibles amenazas, después se le asigna el nivel de efectividad del control utilizado para las posibles amenazas, y por último se hace un comentario con respeto a la seguridad del activo.

Activos	Amenazas	Nivel de efectividad del control	Comentarios
Celulares	Daños físicos al activo	2	La empresa tiene un acuerdo para el seguro de los teléfonos.
	Desperfectos al equipo	2	
	Phishing	3	
	Problemas por contraseña	3	
	Problemas por olvido o robo de cuentas.	2	
Centro de cómputo	Daños físicos al activo.	2	El centro de cómputo se encuentra bien estructurado siguiendo todas las directrices necesarias para su funcionamiento.
	Problemas de red.	2	
	Desperfectos al equipo.	2	
	Inundaciones	2	
	Terremotos	1	
	Fuegos	2	
Computadoras	Daños físicos al activo.	2	Las computadoras están bien configuradas en lo único que suelen fallar es en sus componentes físicos.
	Daños de software al Activo.	2	
	Virus, gusanos y ransomware.	3	
	Desperfectos al equipo.	2	
	Fallos de configuración.	2	
	Secuestro de registros.	3	
	Phishing	2	
	Problemas por contraseñas.	2	
Impresoras	Problemas de red.	2	La impresora presenta algunos casos que tiene problemas de configuración o no se conecta a la red.
	Fallas de Escaneo.	3	
	Fallos de configuración.	2	
	Fallas al imprimir.	2	
	Error humano.	2	
Servidor	Problemas de red.	2	La empresa utiliza sus servidores en la nube donde lo administran remotamente.
	Fallos de configuración.	2	
	Desperfectos al equipo.	2	
	Caídas del activo por sobrecargas.	2	

	Problemas por contraseñas.	3	
Televisores	Daños físicos al activo.	2	El televisor lo usan para reuniones y proyectar información.
	Desperfectos al equipo.	3	
	Fallos de configuración.	3	
Información	Daños físicos al activo	3	La información es el activo primordial de toda compañía, ya que es el punto de trabajo de toda actividad.
	Secuestro de registros.	3	
	Phishing	3	
	Error humano.	3	

Impacto residual

El impacto residual se define como el daño sobre el activo debido a la materialización de la amenaza aun existiendo las salvaguardas que lo protejan. Por consiguiente, en la tabla que se presenta a continuación se mostrarán los controles de cada amenaza por cada uno de los activos y con ello visualizar si el control está siendo implementado o no en la empresa.

Fórmula para obtener el impacto residual

$$\frac{Impacto\ potencial}{Eficacia\ del\ control}$$

Simbología de los tipos de control

Prevención	**P**
Minimizadora	**MZ**

Tabla de impacto residual

Tipo de activo	Amenazas	Controles	Tipo de control	¿Control implementado?	Eficacia del control	Impacto potencial	Impacto residual
Celulares	Daños físicos al activo	Los dispositivos tienen que ser cuidados por los empleados.	**MZ**	Sí	2	2	1
	Desperfectos al equipo	Verificar que los dispositivos funcionen de la manera correcta.	**MZ**	Sí	2	1	0.5
	Phishing	Los dispositivos solamente deben contar con aplicaciones aprobadas por la compañía y prohibir navegación en sitios no autorizados.	**P**	Sí	3	2	0.6666
	Problemas por contraseña	Realizar una capacitación a los usuarios para que estos utilicen el estándar de contraseña ya estipulado.	**P**	Sí	3	3	1
	Problemas por olvido o robo de cuentas.	Mantener actualizado el sistema operativo y no visitar sitios maliciosos.	**P**	Sí	2	1	0.5
Centros de cómputo	Daños físicos al activo.	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas.	**P**	Sí	2	2	1
	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	**P**	Sí	2	3	1.5
	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo	**MZ**	Sí	2	2	1

		contrario notificarlo con el supervisor.					
	Inundaciones	Siempre verificar que no se dejen grifos abiertos.	**P**	Sí	2	3	1.5
	Terremotos	Contar con un plan de acción en caso de desastre.	**P**	Sí	1	3	3
	Fuegos	Contar con un extintor de polvo químico seco.	**P**	Sí	2	3	1.5
Computadoras	Daños físicos al activo.	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas.	**P**	Sí	2	2	1
	Daños de software al Activo.	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento.	**P**	Sí	2	3	1.5
	Virus, gusanos y ransomware.	Mantener actualizado el sistema operativo, verificado el antivirus y sobre todo navegar en páginas seguras.	**P**	Sí	3	3	1
	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	**MZ**	Sí	2	2	1
	Fallos de configuración.	Asignar a una persona calificada para la instalación o implementación de un software.	**MZ**	Sí	2	2	1

	Secuestro de registros.	Establecer jerarquía de acceso a la información.	**P**	Sí	3	3	1
	Phishing	Los dispositivos solamente deben contar con aplicaciones aprobadas por la compañía y prohibir navegación en sitios no autorizados.	**P**	Sí	2	2	1
	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	**MZ**	Sí	2	3	1.5
Impresoras	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	**P**	Sí	2	3	1.5
	Fallas de Escaneo.	Contar con una capacitación para el uso adecuado del equipo.	**P**	Sí	3	3	1
	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	**P**	Sí	2	2	1
	Fallas al imprimir.	Revisar que todo esté en orden con la impresora a la hora de imprimir.	**MZ**	Sí	2	2	1
	Error humano.	Utilizar la impresora solo para fines laborales.	**MZ**	Sí	2	3	1.5
Servidor	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	**P**	Sí	2	3	1.5
	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	**P**	Sí	2	3	1.5

	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	**MZ**	Sí	2	2	1
	Caídas del activo por sobrecargas.	Evitar en la medida de lo posible la carga excesiva de información.	**P**	Sí	2	2	1
	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	**MZ**	Sí	3	3	1
Televisores	Daños físicos al activo.	Los dispositivos tienen que ser cuidados por los empleados.	**P**	Sí	2	2	1
	Desperfectos al equipo.	Verificar que los dispositivos funcionen de la manera correcta.	**MZ**	Sí	3	2	0.6666
	Fallos de configuración.	Asignar a una persona calificada para la instalación.	**P**	Sí	3	2	0.6666
Información	Daños físicos al activo	La información es altamente corruptible y se debe implementar una medida para ello.	**P**	Si	3	2	0.6666
	Secuestro de registros.	Establecer jerarquía de acceso a la información.	**P**	Si	3	3	1
	Phishing	Mejora de los esquemas de seguridad de la compañía.	**P**	Si	3	2	0.6666
	Error humano.	Acceso solamente al personal autorizado.	**P**	Si	3	3	1

Matriz de impacto residual y riesgo residual

Tipo de activo	Amenazas	Controles	Tipos de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Celulares	Daños físicos al activo	Los dispositivos tienen que ser cuidados por los empleados.	**MZ**	2	2	1	3	1	Moderado
	Desperfectos al equipo	Verificar que los dispositivos funcionen de la manera correcta.	**MZ**	2	1	0.5	1	0.5	Tolerable
	Phishing	Los dispositivos solamente deben contar con aplicaciones aprobadas por la compañía y prohibir navegación en sitios no autorizados.	**P**	3	2	0.6666	4	0.6666	Moderado
	Problemas por contraseña	Realizar una capacitación a los usuarios para que estos utilicen el estándar de contraseña ya estipulado.	**P**	3	3	1	4	1	Intolerable
	Problemas por olvido o robo de cuentas.	Mantener actualizado el sistema operativo y no visitar sitios maliciosos.	**P**	2	1	0.5	3	0.5	Moderado
Centros de cómputo	Daños físicos al activo.	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas.	**P**	2	2	1	2	1	Moderado
	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	**P**	2	3	1.5	5	1.5	Intolerable
	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario	**MZ**	2	2	1	2	1	Tolerable

		notificarlo con el supervisor.							
	Inundaciones	Siempre verificar que no se dejen grifos abiertos.	**P**	2	3	1.5	1	1.5	Moderado
	Terremotos	Contar con un plan de acción en caso de desastre.	**P**	1	3	3	1	3	Moderado
	Fuegos	Contar con un extintor de polvo químico seco.	**P**	2	3	1.5	1	1.5	Moderado
Computadoras	Daños físicos al activo.	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas.	**P**	2	2	1	2	1	Tolerable
	Daños de software al Activo.	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento.	**P**	2	3	1.5	5	1.5	Intolerable
	Virus, gusanos y ransomware.	Mantener actualizado el sistema operativo, verificado el antivirus y sobre todo navegar en páginas seguras.	**P**	3	3	1	3	1	Importante
	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	**MZ**	2	2	1	2	1	Moderado
	Fallos de configuración.	Asignar a una persona calificada para la instalación o implementación de un software.	**MZ**	2	2	1	2	1	Moderado

	Secuestro de registros.	Establecer jerarquía de acceso a la información.	**P**	3	3	1	1	1	Moderado
	Phishing	Los dispositivos solamente deben contar con aplicaciones aprobadas por la compañía y prohibir navegación en sitios no autorizados.	**P**	2	2	1	4	1	Importante
	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	**MZ**	2	3	1.5	4	1.5	Intolerable
Impresoras	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	**P**	2	3	1.5	5	1.5	Intolerable
	Fallas de Escaneo.	Contar con una capacitación para el uso adecuado del equipo.	**P**	3	3	1	3	1	Importante
	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	**P**	2	2	1	2	1	Moderado
	Fallas al imprimir.	Revisar que todo esté en orden con la impresora a la hora de imprimir.	**MZ**	2	2	1	4	1	Importante
	Error humano.	Utilizar la impresora solo para fines laborales.	**MZ**	2	3	1.5	2	1.5	Importante
Servidor	Problemas de red.	Contar con un proveedor de servicios de red de respaldo.	**P**	2	3	1.5	5	1.5	Intolerable
	Fallos de configuración.	Asegurarse de asignar a una persona calificada para la instalación o implementación de un software.	**P**	2	3	1.5	2	1.5	Importante

	Desperfectos al equipo.	Comprobar que el equipo este en óptimas condiciones, de lo contrario notificarlo con el supervisor.	**MZ**	2	2	1	2	1	Moderado
	Caídas del activo por sobrecargas.	Evitar en la medida de lo posible la carga excesiva de información.	**P**	2	2	1	3	1	Importante
	Problemas por contraseñas.	Cumplir con el estándar de contraseña segura.	**MZ**	3	3	1	4	1	Intolerable
Televisores	Daños físicos al activo.	Los dispositivos tienen que ser cuidados por los empleados.	**P**	2	2	1	2	1	Moderado
	Desperfectos al equipo.	Verificar que los dispositivos funcionen de la manera correcta.	**MZ**	3	2	0.6666	2	0.6666	Moderado
	Fallos de configuración.	Asignar a una persona calificada para la instalación.	**P**	3	2	0.6666	2	0.6666	Moderado
Información	Daños físicos al activo	La información es altamente corruptible y se debe implementar una medida para ello.	**P**	3	2	0.6666	2	0.6666	Moderado
	Secuestro de registros.	Establecer jerarquía de acceso a la información.	**P**	3	3	1	1	1	Moderado
	Phishing	Mejora de los esquemas de seguridad de la compañía.	**P**	3	2	0.6666	4	0.6666	Importante
	Error humano.	Acceso solamente al personal autorizado.	**P**	3	3	1	2	1	Importante

Comunicación del riesgo y recomendaciones

Por consiguiente, una vez finalizada la etapa del análisis de riesgo los resultados que obtuvimos se presentaron al gerente general de la empresa Mi pyme financiera con el fin de que él decida qué acciones llevar a cabo para mitigar los riesgos que se encontraron. Asimismo, se le recomienda al gerente llevar a cabo la implementación de las medidas del tratamiento de riesgo con base a la metodología Magerit.

Por otro lado, se exhorta que los riesgos tolerables y moderados sean considerados aceptables, sin embargo, estos riesgos deben contar con una supervisión e iniciar a buscar y proponer futuras soluciones por si estas exposiciones traen conflictos más adelante a la empresa. Por lo cual los riesgos importantes e intolerables se recomienda que sean vistos y solucionados lo más pronto posible ya que son de alto nivel y pueden ocasionar desperfectos en la funcionalidad de la empresa.

Ahora, las opciones de tratamiento para los riesgos importantes e intolerables que se sugieren son los que a continuación se mencionan:

- ***Mitigación de un proveedor de red:*** Contar con un proveedor de servicios de red de respaldo, ya que con ello tendremos mayor efectividad en la productividad y eficacia del trabajo.
- ***Financiación de un seguro:*** La empresa debe contar con un fondo de contingencias para cubrir con los daños de los activos dentro de la empresa.
- ***Capacitación:*** A cada uno de los empleados de la empresa capacitarlos para que así ellos utilicen de una manera correcta y adecuada los activos de la empresa evitando así desperfectos en estos.

En conclusión, el gerente general de la empresa Mi pyme financiera accedió a llevar a cabo cada una de las recomendaciones que se mencionaron con respecto a los riesgos tolerables y moderados. Asimismo, actuará de manera inmediata con respecto a los riesgos importantes e intolerables para así evitar daños en la empresa.

Número de riesgos en zona de riesgo importante e intolerable

Amenaza	Zona de riesgo	
	Importante	***Intolerable***
Problemas por contraseña	3	
Problemas de red		3
Daños de software al activo		1
Virus, gusanos y ransomware	1	
Fallas de escaneo	1	
Total	**5**	**4**

Tratamiento del riesgo

A lo largo de una exhaustiva investigación y análisis de los datos se han encontrado distintas componentes de amenazas en ciertos departamentos de la organización entre ellos tenemos los departamentos de TI, lo departamentos administrativos y mediante diferentes técnicas se ha buscado dar una solución para cada tipo de amenaza registrada, estableciendo las amenazas y las fortalezas de cada uno.

Amenaza	Riesgo	Fortalezas	Debilidades	Acción
Daños físicos al activo.	Elementos de tecnológicos defectuosos.	Contar con seguridad para los activos.	No contar con seguridad en los activos.	Implementación de un sistema de seguridad de hardware.
Daños de software al activo.	Daño a los activos y un tiempo de reparación.	Contar con un personal que tenga la labor de hacer el mantenimiento y la revisión del software.	Las distintas capacitaciones que requiere dicho personal.	Capacitar al personal que utilizará el software.
Virus, gusanos y ransomware.	Daños al sistema de la empresa	Tener a disponibilidad un antivirus en todas las máquinas.	No tener antivirus para algunos de los dispositivos utilizados.	Implementación de antivirus para el sistema.

Problemas de red	Incapacidad para la realización de ciertas actividades.	Contar con el debido personal para su mantenimiento.	No contar con el personal adecuado para el mantenimiento respectivo.	Capacitación de los empleados para la reparación y mantenimiento de los problemas de red.
Desperfectos al equipo	Pérdida de tiempo para la empresa.	Sistema de contabilización para los equipos de la empresa.	No tener el equipo adecuado para dicha función.	Mantenimiento para todos los equipos.
Fallas de Escaneo	Fallas en los dispositivos al momento de escanear.	Personal especializado para el mantenimiento.	No contar con experiencia para solucionar dichos problemas.	Mantenimiento continuo.
Fallo de configuración	Sistemas obsoletos.	Personal especializado para el mantenimiento.	No contar con personal autorizado.	Configurar los sistemas para su correcto funcionamiento.
Fallas al imprimir	Utilización de más papel y tinta.	Personalizar especializado en mantenimiento.	No contar con el personal para atender dichos fallos.	Mantenimiento continuo.
Secuestro de registros	Robo de información	Capacitación al personal en caso de robo de información.	No contar con capacitaciones.	Capacitaciones de seguridad a personal.
Phishing	Robo información.	Capacitaciones al personal en cuanto seguridad de información.	No contar con capacitaciones.	Capacitaciones de seguridad a personal.
Caída del activo por sobrecargas	Daños a activos o incendios	Capacitaciones al personal en cuanto a los activos.	No contar con capacitaciones.	Capacitación del correcto uso de los equipos al personal.
Problemas por contraseñas	Robo de información.	Capacitaciones al personal en seguridad en cuanto a contraseñas.	No contar con capacitaciones.	Capacitaciones a los empleados la implementación de contraseñas seguras.
Problemas por olvido o robo de	Robo de información	Capacitación al personal en seguridad en	No contar con capacitaciones.	Capacitaciones de seguridad a personal.

cuentas		cuanto a contraseñas.		
Inundaciones	Daños a los activos.	Mantener los activos en zonas elevadas.	No mantener los activos de la empresa en zona de alto relieve.	Ubicación del hardware estratégico.
Terremotos	Daño a infraestructura y activos.	Mantener los activos en zonas protegidas.	No contar con zonas de seguridad contra terremotos.	Salidas de emergencias y equipo en lugares protegidos.
Fuegos	Daño a los activos, infraestructura y el personal de la empresa.	Contar con extintores bien posicionados.	No contar con el equipo adecuado para una emergencia.	Salidas de emergencia y equipos en lugares protegidos.
Error Humano	Daños a los activos o personal.	Evitar cometer accidentes.	Posibles accidentes ocurridos.	Plan de gestión de riesgos establecido.

Costos en seguridad informática

Coste – Beneficio: Mi Pyme Financiera			
Coste			
Categoría	***Ítem***	***Precio mensual***	***Total Anual***
Software	Licencia de antivirus (AVG Business).	$ 13.30	$ 159.59/anual por usuario.
	Programa SE Risk.	$ 40.00	$ 480/anual
	Programa Keeper Business.	$ 3.75	$ 45 anual
Recurso tecnológico	Administración de IT	$ 2,000.00	$24,000.00
	Consultoría especialista en	$ 1,000.00	$ 12,000.00

	seguridad informática.		
	Técnico en sistemas.	$ 800.00	$ 9,600.00
			Total $ 46,284.59

Beneficios

AVG Business

- Cuenta con un soporte técnico las 24 horas, 5 días a la semana.
- Administra la red y los dispositivos de forma remota desde un solo lugar.
- Detecta y elimina el malware y los virus de las PC y portátiles.
- Inspecciona el correo electrónico entrante y saliente en busca de malware y spam.
- Bloquea las descargas nocivas y los sitios web peligrosos antes de que se abran.
- Analiza cada enlace incluyendo los de Facebook y Twitter en busca de posibles amenazas.
- Analiza rápidamente su equipo en busca de problemas de rendimiento y seguridad.
- Protege automáticamente las contraseñas guardadas en los navegadores Chrome y Firefox para una mayor protección y seguridad.
- Analiza y comprueba los correos electrónicos en busca de archivos adjuntos, spam y enlaces sospechosos.
- Analiza todo lo que se carga y se descarga de sus servidores.

***SE Risk*.**

Permite administrar los riesgos y apoyar en la mejora continua. Brinda soporte a la identificación de riesgos, reduciendo pérdidas y maximizando las oportunidades de la organización. Se puede categorizar los riesgos y evaluarlos, con herramientas fáciles de aplicar

y visuales, lo que hace posible un mejor desempeño y eficacia en la prevención y el control de riesgos.

Keeper Business

- Almacenamiento encriptado de contraseñas.
- Almacenamiento seguro de datos.
- Análisis de comportamientos.
- Análisis de vulnerabilidades.
- Auditoría de seguridad.
- Autenticación.
- Autenticación de dos factores.

Conclusiones y recomendaciones

Se logró tener éxito en cada uno de los objetivos establecidos para el análisis de los riesgos de Mi Pyme financiero. La empresa por medio de este detalle desglose de información establecida en este informe ahora es consciente de todas las amenazas y riesgos con cuales podría llegar a enfrentarse, teniendo en cuenta las fallas que afectan su rendimiento y posibles soluciones a estas amenazas.

Se comprendieron los procesos y protocolos de seguridad en la información aplicándolos exitosamente a los procesos del día a día en la compañía los cuales de esta manera logran minimizar los riesgos que conllevaban el manejo de estos datos.

Se afianzaron los conocimientos acerca de la metodología que estábamos implementando en este caso la metodología Magerit.

Se establecieron los pasos para la correcta documentación para los procesos estableciendo los posibles fallos que estos tienen y mejorando la manera en que estos se realizan.

Bibliografías

Bailón-Lurido, W. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó. Pol. Con. (Edición núm. 36) Vol. 4 No 8 agosto 2019, pp. 165-189.

ISO 31000. (2013). Software ISO; ISOTools. Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

Kowask, E. et al. (s. f.). Gestión del Riesgo de las TI NTC 27005. Recuperado de: https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI9.pdf

Universidad Piloto de Colombia, (2015). Programa ingeniería de sistemas especialización en seguridad informática.

FUNDIBEQ, (s. f.). ISO – Seguridad de la información. Recuperado de: https://www.fundibeq.org/informacion/infoiso/iso-seguridad-de-la-informacion