UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES

COHORTE 2021

Tema: EVALUACIÓN DE RIESGOS INFORMÁTICOS Y DISEÑO DE UN PLAN DE CONTINGENCIA PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., UBICADA EN LA CIUDAD DE AMBATO.

Trabajo de Titulación, previo a la obtención del Grado Académico de Magíster en Tecnologías de la información Mención Seguridad en Redes y Comunicaciones.

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada

Autor: Ingeniero Juan Pablo Aranda Moposita

Director: Ingeniero Héctor Fernando Gómez Alvarado Doctor

Ambato – Ecuador

2022

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado. PhD, e integrado por los señores: Ingeniera Wilma Lorena Gavilanes López Magister e Ingeniera, Lorena del Carmen Chiliquinga Vejar Magister, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "*Evaluación de riesgos informáticos y diseño de un plan de contingencia para el área de tecnología de la empresa IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., ubicada en la ciudad de Ambato."* elaborado y presentado por el señor Ingeniero Juan Pablo Aranda Moposita, para optar por el Grado Académico de Magíster en Tecnologías de la Información; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.

Presidente y Miembro del Tribunal

Ing. Wilma Lorena Gavilanes López, Mg

Miembro del Tribunal

Ing. Lorena del Carmen Chiliquinga Vejar, Mg

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Evaluación de riesgos informáticos y diseño de un plan de contingencia para el área de tecnología de la empresa IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., ubicada en la ciudad de Ambato., le corresponde exclusivamente a: Ingeniero, Juan Pablo Aranda Moposita, Autor bajo la Dirección de Ingeniero, Héctor Fernando Gómez Alvarado, Doctor, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato

---

I*ngeniero Juan Pablo Aranda Moposita*

c.c.: 1804704755

AUTOR

Ingeniero Héctor Fernando Gómez Alvarado Doctor

c.c.: 1103474589

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniero Juan Pablo Aranda Moposita
c.c.: 1804704755

INDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

Quiero agradecer primeramente a Dios por guiarme en el transcurso de toda mi vida y por llenar sus bendiciones a toda mi familia.

A la empresa Importadora Alvarado por permitirme realizar mi trabajo de titulación.

.

A los docentes de la Universidad Técnica de Ambato y a mis compañeros de aula Juan Mecánico que fueron un apoyo y guía para la culminación de este proyecto.

Juan Pablo Aranda Moposita

DEDICATORIA

A mi esposa Paulina, a mis hijos Pablito y Juanito que son el pilar más importante en mi vida, por su constante apoyo y motivación que me han acompañado para la conclusión de mi maestría.

A mis padres Jacinto y Esperanza quien me apoyaron incondicionalmente en todo momento, gracias por inculcar en mí el ejemplo de trabajo y respeto que hicieron de mí una mejor persona

A mis hermanos y a mis tías que me apoyaron con un granito de arena durante todo el transcurso de mi carrera.

Juan Pablo Aranda Moposita

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

EVALUACIÓN DE RIESGOS INFORMÁTICOS Y DISEÑO DE UN PLAN DE CONTINGENCIA PARA EL ÁREA DE TECNOLOGÍA DE LA EMPRESA IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., UBICADA EN LA CIUDAD DE AMBATO.

DEGREE MODALITY: *Proyecto de Titulación con Componente de Investigación Aplicada*
AUTHOR: *Ingeniero. Juan Pablo Aranda Moposita*
DIRECTED BY: *Ingeniero. Héctor Fernando Gómez Alvarado, Doctor*
DATE: *Veintidós de noviembre de dos mil veintidós*

RESUMEN EJECUTIVO

Las empresas cada día van creciendo su información y sus activos lo cual tienen la necesidad de salvaguardar la integridad de su información ante los posibles riesgos, dichos riesgos si no son detectados y controlados a tiempo pueden causar grandes daños y pérdidas económicas, para mitigar estos riesgos es necesario contar con una metodología de análisis y gestión de riesgos.

Por este motivo se ha visto la necesidad de implementar la metodología MAGERIT versión 3.0, que nos ayuda a gestionar de manera eficaz los riesgos a los que están expuestos nuestros activos más críticos para el área de tecnología de la empresa Importadora Alvarado Vásconez Cía. Ltda., con base a la norma ISO 31000, el cual nos permitirá prevenir y detectar los incidentes que llegaran a presentarse, obteniendo información sobre las vulnerabilidades a las que están expuestas, determinar el impacto que pueda generar y las amenazas en caso de materializarse en los sistemas

de información, logrando establecer procesos para identificar y reducir los riesgos que pondrán en amenaza la estabilidad de la empresa, la infraestructura de TI y lo más importante la información.

Después del análisis de riesgos se elaborará un plan de contingencia en base a la norma ISO/IEC 27001:2013 el cual constará de 4 etapas, el cual nos ayudará en los procesos críticos de la empresa continúen funcionando ante algún fallo en los sistemas tecnológicos y les permita seguir operando, aunque sea al mínimo de sus actividades.

Los resultados obtenidos ayudarán a identificar el nivel de riesgo en que se encuentra los activos más críticos de la empresa, el nivel de madurez de la seguridad actual, como también las amenazas o vulnerabilidades a las que están expuestas, sus niveles de riesgos incluyendo el impacto y la probabilidad de ocurrencia, y su respectivo plan de contingencia para los procesos más críticos de la empresa.

DESCRIPTORES: *AMENAZAS, ACTIVOS, CONTINGENCIA, CUALITATIVO, ISO, INFRAESTRUCTURA, MAGERIT, RIESGOS, SEGURIDAD, VULNERABILIDADES*.

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

THEME:

COMPUTER RISK ASSESSMENT AND DESIGN OF A CONTINGENCY PLAN FOR THE TECHNOLOGY AREA OF THE COMPANY IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA. LOCATED IN THE CITY OF AMBATO.

DEGREE MODALITY: *Graduation Project with Applied Research Component*
AUTHOR: *Ingeniero Juan Pablo Aranda Moposita*
DIRECTED BY: *Ingeniero Héctor Fernando Gómez Alvarado Doctor*
DATE: *Veintidós de noviembre de dos mil veintidós*

EXECUTIVE SUMMARY

Companies every day are growing their information and assets which have the need to safeguard the integrity of their information against potential risks, these risks if not detected and controlled in time can cause great damage and economic losses, to mitigate these risks it is necessary to have a methodology for analysis and risk management.

For this reason we have seen the need to implement the methodology MAGERIT version 3.0, which helps us to effectively manage the risks to which our most critical assets are exposed to the technology area of the company Importadora Alvarado Vásconez Cía, based on the ISO 31000 standard, which will allow us to prevent and detect incidents that may occur, obtaining information about the vulnerabilities to which they are exposed, determine the impact that can generate and the threats if they materialize in the information systems, establishing processes to identify and reduce

the risks that threaten the stability of the company, IT infrastructure and most importantly the information.

After the risk analysis, a contingency plan will be developed based on ISO/IEC 27001:2013, which will consist of 4 stages, which will help us to ensure that the company's critical processes continue to function in the event of a failure in the technological systems and allow them to continue operating, even at the minimum level of their activities.

The results obtained will help to identify the risk level of the company's most critical assets, the current security maturity level, as well as the threats or vulnerabilities to which they are exposed, their risk levels including the impact and probability of occurrence, and their respective contingency plan for the company's most critical processes.

KEYWORDS: *THREATS, ASSETS, CONTINGENCY, QUALITATIVE, ISO, INFRASTRUCTURE, MAGERIT, RISK, SECURITY, VULNERABILITIES*.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

Los dinámicos avances tecnológicos conlleva a las empresas a tener un desconocimiento sobre la gestión de riesgo y que no sepan el valor e importancia de sus activos tecnológicos lo que es aprovechado por los piratas informáticos(Bernal, 2021).

Los ataques informáticos y las amenazas cada vez son más constantes en las empresas ya sean grandes o pequeñas afectando la confidencialidad, integridad y disponibilidad de la información, estos ataques pueden ser provocados accidentalmente o con un fin malicioso ocasionando pérdidas o alteración de la información, debido a que existen riesgos que afectan la seguridad de la empresa y por lo general no se tiene un proceso para la gestión de análisis de riesgos, la empresa Importadora Alvarado Vásconez se ve en la obligación de identificar las amenazas y las vulnerabilidades de sus activos logrando controlar estos riesgos para evitar que se materialicen causando pérdidas económicas en la organización y sobre todo la credibilidad de sus clientes.

El presente estudio, se plantea la metodología MAGERIT v3 el cual nos permite realizar una gestión de riesgos y que mejor guía que la ISO 31000 que se encarga del sistema de gestión de riesgo, se ha convertido en una herramienta fundamental para la valoración de activos, posee un análisis cualitativo y cuantitativo que ayudara a la empresa a tener una información más clara para la toma de decisiones, además se tendrá un plan de contingencia en base a la norma ISO/IEC 27001 que ayudara a la continuidad del negocio en caso de que alguna amenaza se materialice y puedan seguir operando aunque sea al mínimo de sus actividades.

El capítulo I El problema de investigación contiene: la introducción del tema planteado, la justificación de la investigación y los objetivos.

El capítulo II Antecedentes investigativos establece: el estado del arte donde nos muestra información relevante de otras empresas con características similares acerca de nuestro tema de investigación, la fundamentación teórica donde nos muestra la definición de los diferentes términos y la metodología de investigación aplicada para el análisis de riesgos y su respectivo plan de contingencia.

El capítulo III Marco metodológico menciona: el enfoque de investigación, el tipo de investigación, la población o muestra, la recolección de información para el levantamiento de los activos y las variables de respuestas.

El capítulo IV Resultados y discusión abarca: la entrevista al coordinador de TI con su respectiva discusión sobre las preguntas planteadas y la aplicación de la metodología desarrollada en dos fases que son el análisis de riesgos y el plan de contingencia.

El capítulo V Conclusiones y recomendaciones constituye: la comprobación de los objetivos específicos, las recomendaciones, la bibliografía y los anexos de la investigación planteada.

1.2. Justificación

Actualmente la empresa no cuenta con una metodología que pueda sistematizar el análisis de riesgos que puedan presentar los activos de la empresa, además no cuenta con procedimientos que garanticen la seguridad de la información y con el pasar de los años los equipos informáticos y la infraestructura tecnológica de la empresa comienzan a presentar fallos físicos y lógicos, esto da lugar a la aparición de vulnerabilidades y amenazas los cuales deben ser eliminados cuando sea posible realizarlo y en otros casos ser controlados para que su impacto no sea tan significativo, lo que podría ocasionar que la empresa detenga sus actividades comerciales lo que conllevaría pérdidas financieras y afectando la credibilidad de sus clientes, proveedores y perjudicando la imagen de la empresa.

Por estos motivos es de gran importancia la implementación de una metodología de gestión de riesgos que permita valorar los activos otorgándoles un nivel de

importancia, identificar las amenazas y los riesgos a las que están expuestas los activos y sobre todo que nos permita salvaguardar los activos ante posibles riesgos garantizando la continuidad del negocio.

Esta investigación es factible de realizar debido a que se cuenta con el apoyo del coordinador de TI de la empresa para el levantamiento de información de los activos, el análisis de amenazas, los riesgos que están expuestos para así desarrollar el plan de contingencia de los activos.

Al desarrollar el análisis de riesgos y el plan de contingencia se beneficiará la empresa en caso de que alguna amenaza se materialice puedan tener una guía para evitar que las actividades de la empresa se paralicen y poder reducir el tiempo de respuesta, y así garantizar la continuidad del negocio.

Debido a que la empresa en algún momento sufrió un escenario en donde el Blade que se encuentran los servidores virtualizados sufrió un daño físico por razones desconocidas, lo que ocasiono pérdidas económicas, por esta razón se elaborara un plan de contingencia en donde se pueda tener procesos y políticas en caso de algún evento no programado para así poder reducir el tiempo de respuesta.

1.3. Objetivos

1.3.1. General

Evaluar los riesgos informáticos para el área de tecnología de la empresa IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA, ubicada en la ciudad de Ambato.

1.3.2. Específicos

a. Identificar los activos más críticos y de mayor impacto dentro del área de tecnología.

b. Aplicar la metodología más adecuada para la evaluación de riesgos informáticos dentro de la empresa.
c. Elaborar un plan de contingencia de los activos más críticos del área de tecnología.

CAPITULO II

ANTECEDENTES INVESTIGATIVOS

2.1. Estado del arte

Debido a que en la actualidad existen diferentes formas de ataque a las empresas públicas o privadas, además a las amenazas que están expuestos ya sean externas o internas, lo que ha llevado a que las empresas se preocupen de la seguridad de su información y de los activos tecnológicos para así contar con un plan de contingencia en caso de materializarse las amenazas, la empresa pueda continuar sus operaciones en caso de algún desastre.

La pandemia del COVID-19 está generando nuevos desafíos para las empresas ecuatorianas, en el 2020 la frecuencia de virus informáticos en la región aumentaron significativamente y posteriormente en el 2021 los ciudadanos ecuatorianos conocieron el primer ataque informático con impacto a nivel nacional, donde por medio de un ataque del tipo secuestro de datos realizado a una institución financiera la información de identificación personal de un gran número de ciudadanos fue expuesta y divulgada en el internet(Suastegui Jaramillo, 2022).

Luego de investigar diferentes artículos científicos de diferentes universidades relacionadas a la evaluación de riesgos informáticos y diseño de un plan de contingencia se encuentran diferentes conceptos las cuales se describe a continuación:

- La implementación de una gestión de riesgos de TI para la empresa Mapusys a los activos tecnológicos con la metodología MAGERIT se pudo identificar los principales activos, otorgándoles un nivel de importancia a los mismos y determinando el impacto que pueden generar y los riesgos potenciales a los que están expuestos, finalmente con el estudio realizado pudieron identificar el

nivel de riesgo en que se encuentran los activos, el nivel de madurez de la seguridad actual y sobre todo establecieron procesos de gestión a la seguridad de la información y recursos que permitirán la reducción del impacto que pueda ocasionar la materialización de una amenaza(Huefle Arévalo, 2020).

- El diseño de un plan de contingencia informático con la norma ISO 27001:2013 en la unidad educativa Atenas les permitió evaluar cada una de las amenazas y las vulnerabilidades que se encuentran expuestos los activos más críticos de la institución, con el objetivo que permitirá la recuperación ante cualquier eventualidad que afecte la continuidad de las actividades de la institución. Con el plan de contingencia se pudo reducir el impacto producido por alguna amenaza que se haya materializado ya que detalla las acciones a tomar antes, durante y después, realizando la restauración de sus activos y las actividades normales evitando la perdida de información(Burgos Gordón, 2020).

- El diseño para la gestión de la seguridad de la información para una institución educativa con un SGSI con las directrices de la norma ISO 27001 aplicado al modelo de ciclo de Deming o PHVA se pudo observar el mejoramiento continuo y la utilización de la metodología MAGERIT para la valoración de sus 3 dimensiones a sus activos más críticos, y su respectivo análisis de riesgos. Con el resultado obtenido de este diseño fue la identificación de las amenazas que representan mayor riesgo para los activos con su respectivo plan de tratamiento y gestión del riesgo que ayuda a la protección de sus activos y la mitigación de los riesgos con su proceso de mejora continua(Montalbán et al., 2020).

- La aplicación de la metodología MAGERIT versión 3 y la herramienta PILAR en la empresa Deco Interiors se pudo verificar el análisis de riesgos con el objetivo de identificar, controlar y mitigar los riesgos para los sistemas de información, con la metodología implementada les ayudo a tener un mejor control de su información, la identificación de sus riesgos y amenazas a lo que

se encuentra expuesto su información y sobre todo los permitirá tener estrategias en situaciones que puedan presentar daños en la organización, donde se pudo observar que las personas encargadas pudieron tomar conciencia de los riesgos que existen dentro de la organización y saber cómo tratarlos, mitigarlos o transferir esos riesgos a las personas encargadas(Cabrejos Torres, 2020).

- La implementación de una gestión de riesgos de TI en una empresa dental les permitió desarrollar un resumen identificando y valorizando los activos tecnológicos, valorizando los riesgos encontrados en la empresa y establecieron planes de acción sobre los riesgos identificados. La empresa utilizo la metodología MAGERIT para identificar los riesgos y tratar los riesgos encontrados con los 3 pilares que son la confidencialidad(C), disponibilidad(D) y la integridad(I), la empresa también realizo charlas sobre la concientizar a todo el equipo lo importante que es la gestión de riesgos en las empresa(Bernal, 2021).

- La implementación de una gestión de riesgos alineada a la ISO 27005 y MAGERIT a una empresa de facturación electrónica se pudo evidenciar la identificación de los activos y gestionar sus riesgos para mitigarlos o llevarlos a un nivel aceptable con el objetivo de concientizar a los participantes para que tengan clara la importancia de generar los riesgos adecuadamente para que no se materialicen, con la implementación de esta metodología cumplieron los requisitos más importantes para el cumplimiento de la ISO 27001 de la cual la empresa desea certificarse(Carmona Torres, 2021).

- Una evaluación de riesgos a la infraestructura de la empresa Logban con la ISO 31000 les permitió regular y gestionar el riesgo existente con las herramientas necesarias para implementar todos los procesos, con el objetivo principal de identificar y evaluar los riesgos más importantes que afectan a la infraestructura donde desempeñan las actividades de ventas y exportación del banano. Concluyendo que la implementación de la ISO 31000 se pudo

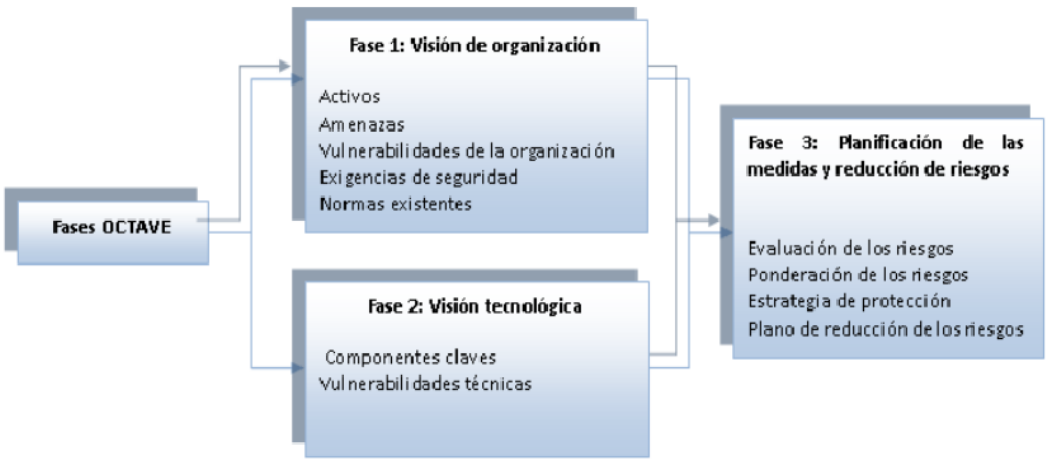
comprender mejor los riesgos con su impacto potencial con el fin de brindar la información a la gerencia para una mejor toma de decisiones y estar preparados en caso de que alguna amenaza se materialice(Mayorga Guacon, 2022).

2.2. Fundamentación teórica

2.2.1. Octave

Por sus siglas en inglés (Operational Critical Threat Asset and Vulnerability Evaluation), es un método de evaluación y gestión de riesgos en base a sus 3 principios: confidencialidad, integridad y confidencialidad para asegurar los sistemas de información, esta metodología guía a las organizaciones para proteger su información ante diferentes riesgos, con el fin de identificar los riesgos, evaluar los riesgos y sobre todos les ayuda de cómo proteger los riesgos de la información(Bernal, 2021).

Figura 1
Fases y elementos de OCTAVE



Nota. Fases para implementar la metodología OCTAVE. Adaptado de *Fases y*

elementos de OCTAVE, Silva Miranda O. M., 2019, Fuente (https://repositorio.uta.edu.ec/bitstream/123456789/30111/1/Tesis_t1639si.pdf)

2.2.2. Magerit

Esta metodología describe los pasos para realizar un análisis del estado del riesgo y gestionar su reducción, detallando las tareas para llevarlo a cabo, de manera que el proceso este bajo control en todo momento, contempla aspectos prácticos para la realización de un análisis y gestión efectiva.

MAGERIT contiene los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

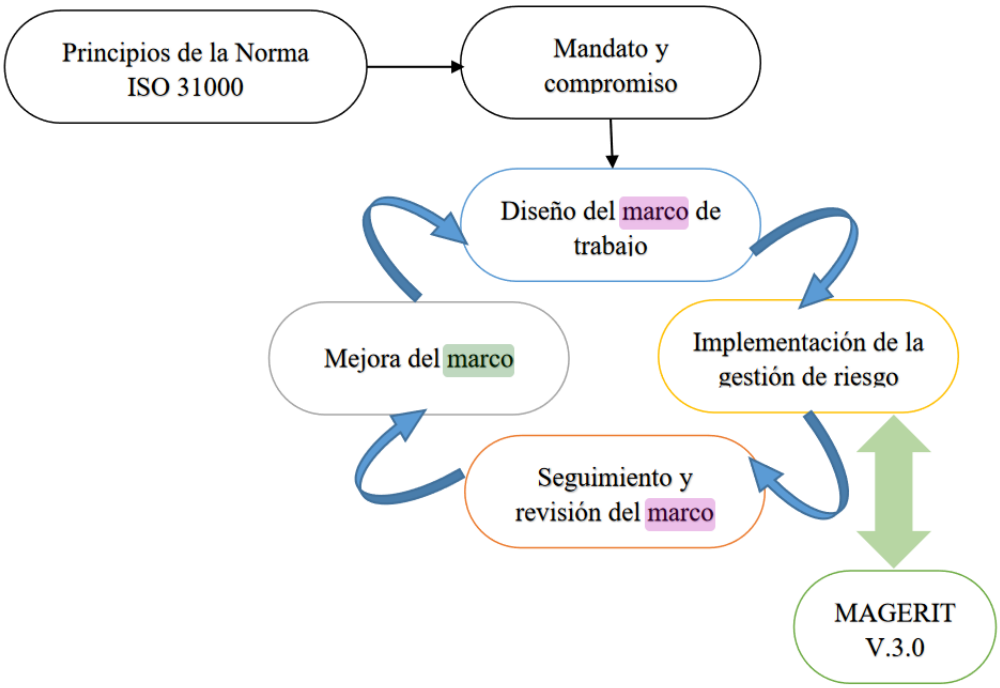
Indirectos:

- Preparar a las organizaciones para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso(Ministerio de Administraciones Públicas de España, 2012).

2.2.3. Metodología MAGERIT V.3.0

MAGERIT v3 nos brinda la metodología del análisis y la gestión del riesgo, esta metodología interesa a las organizaciones que trabajan con información digital o sistemas tecnológicos, MAGERIT nos ayudara a conocer cuánto es el valor que está en juego los activos, como protegerlos y sobre todo nos da a conocer los riesgos en el cual se encuentran expuestos nuestros activos(Guzmán Morán, 2019).

Figura 2
Marco de trabajo para la gestión de riesgos



Nota. La figura muestra los procesos para un marco de trabajo en MAGERIT v3.0. Adaptado de *Implementación de MAGERIT V3.0*, Guzmán Morán, 2019, Fuente (Guzmán Morán, 2019)

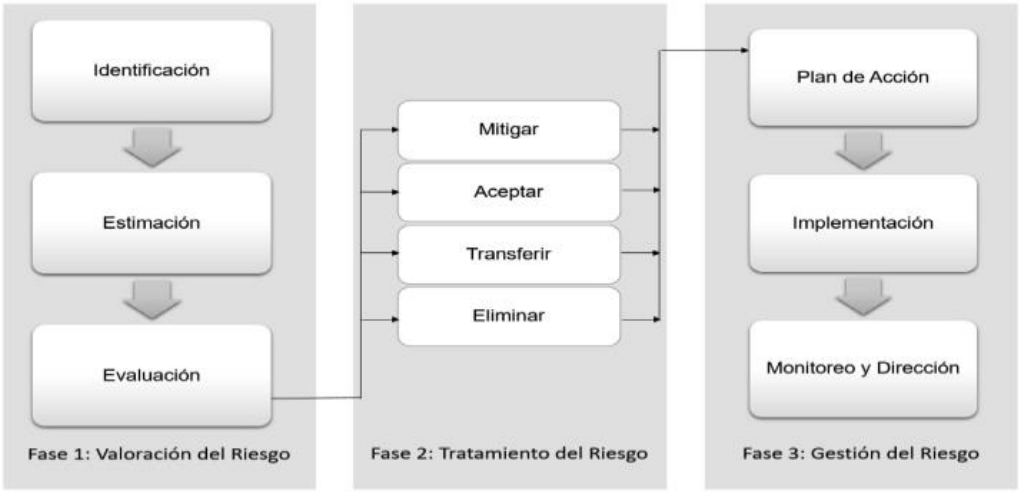
2.2.4. MEHARI

MEHARI (Method for Harmonized Analysis of Risk), es realizada por la organización francesa especializada en los sistemas de información, es una metodología que proporciona un conjunto de herramientas que permite realizar un análisis de riesgos cualitativo y cuantitativo, la metodología MEHARI hace un análisis de la seguridad basado en 3 criterios que son: confidencialidad, integridad y disponibilidad. También está comprendida en 3 fases las cuales las empresas pueden tomar para una continuidad del negocio(Lopez Rimari, 2020).

- **Análisis o evaluación de riesgos:** Es un enfoque estructural que permite identificar todas las situaciones potenciales de riesgo.
- **Evaluaciones de seguridad:** Tiene controles de seguridad lo que perite evaluar el nivel de calidad de los mecanismos y la reducción del riesgo.

- **Análisis de amenazas:** La identificación de las amenazas en las organizaciones es fundamental y que el análisis merece un nivel prioritario y un método estricto(Lopez Rimari, 2020).

Figura 3
Proceso de evaluación, tratamiento y gestión del Riesgo de MEHARI



Nota. Fases para la implementación de la metodología MEHARI. Adaptado por *Proceso de evaluación, tratamiento y gestión del Riesgo de MEHARI*, García, F. Y. H., & Moreta, L. M. L., 2019, Fuente (https://pdfs.semanticscholar.org/e0f8/cf42af8483db9a94996326d630888404d72d.pdf)

2.2.5. ISO 31000

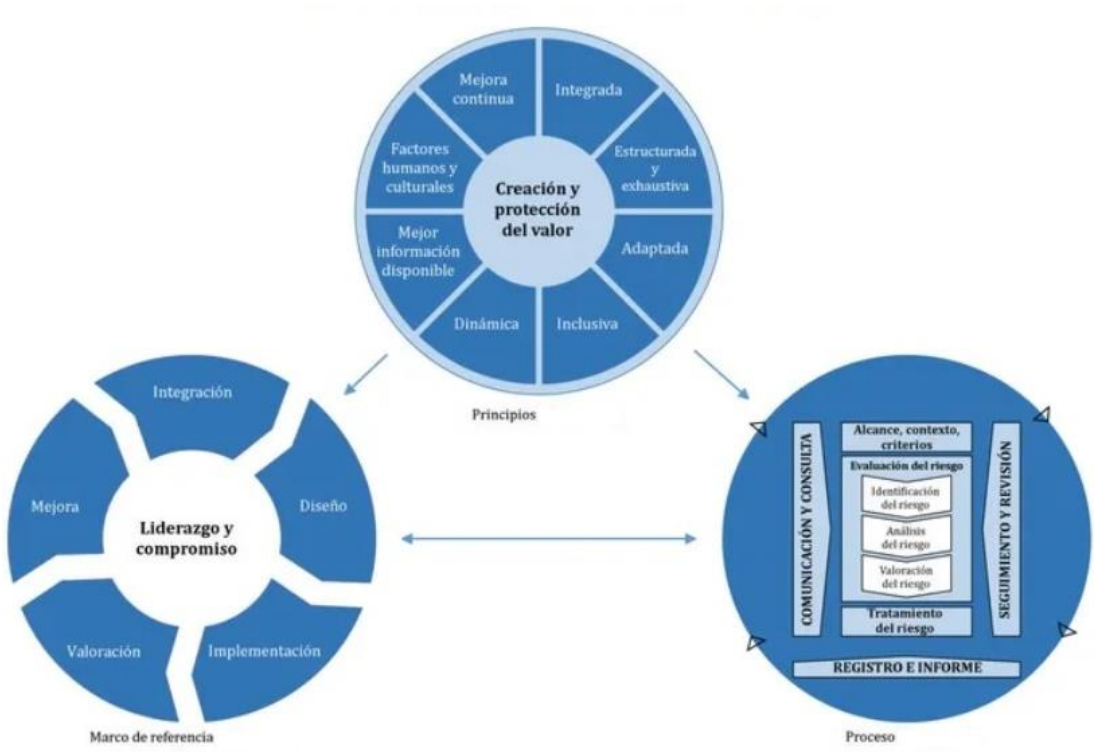
Son guías para poder realizar el proceso de la gestión de riesgos y es el más utilizado por las organizaciones, cuenta con principios para lograr una gestión optima de riesgos, la norma recomienda que las empresas u organizaciones desarrollen, implementen y tengan una mejora continua en un marco de trabajo(Bernal, 2021).

2.2.6. ISO 31000/2018 Gestión de riesgos

Una gestión de riesgo puede considerarse controlada porque dentro de las empresas se ha establecido las guías correspondientes para que el nivel de impacto del riesgo sea mínimo sobre los activos físicos o digitales, tomando en cuenta que el riesgo no puede

ser eliminado totalmente, siempre se tendrá un valor residual, es por este motivo que la gestión del riesgo cumple un proceso cíclico(Guzmán Morán, 2019).

Figura 4
Principios, marco de referencia y proceso



Nota. La imagen nos muestra las relaciones entre los principios, marco de trabajo y el proceso para una gestión de riesgos. Adaptado por *Principios, marco de referencia y proceso*, Online Browsing Platform (OBP), 2018, Fuente (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es)

2.2.7. ISO/IEC 27001:2013

Es una norma para implementar y mejorar un sistema de gestión de la seguridad de la información en cualquier tipo de organización, el cual se establece un código de mejores prácticas para la administración de la seguridad de la información.

- **Ventajas de implementar un plan de contingencia informático con la norma ISO/IEC 27001:2013**

- Garantizar la continuidad del negocio
- Mejora la imagen corporativa y da confianza a los clientes
- Incrementa la confianza
- Reducir los costos en caso de tener incidentes
- Tener una gestión de la seguridad de la información
- Mejora los procesos de TI(Burgos Gordón, 2020)

2.2.8. Amenazas informáticas

Las amenazas informáticas están relacionadas con la posibilidad de que algún tipo de evento o amenaza pueda afectar negativamente a las operaciones de las empresas, las amenazas pueden ser accidentales o de manera accidental(Burgos Gordón, 2020).

- **Identificación de las amenazas**

Figura 5
Tipo de amenazas

Fuente: Elaboración propia

- **Valoración de las amenazas**

Cuando un activo es víctima de una amenaza o un riesgo no se ve afectado en todas sus dimensiones, cuando una amenaza perjudica a un activo se valoran en dos sentidos:

Degradación: Cuán perjudicado resultaría el activo
Probabilidad: Cuán probable o improbable se materialice una amenaza

2.2.9. Riesgos informáticos

Los riesgos informáticos son problemas muy críticos para las organizaciones ya que pueden afectar a los sistemas de información y paralizar las operaciones de sus actividades si no se tienen las medidas para salvaguardar la información dichos riesgos.

2.2.10. Dimensiones de valores

- **Disponibilidad**

La disponibilidad es tener acceso a la información cuando lo necesiten, ya sean personas, procesos o aplicaciones.

- **Integridad**

Es garantizar que la información no haya sido alterada por usuarios no autorizados, evitando que los datos sean alterados mientras se almacena, procesa o trasmite.

- **Confidencialidad**

La información crítica para las empresas no se divulgue a personas no autorizados.

2.2.11. Probabilidad

La palabra “probabilidad” se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática(Ministerio de Administraciones Públicas de España, 2012).

2.2.12. Activos

Bienes pertenecientes a los sistemas de información o relacionados al mismo y que tengan valor para la empresa, se clasifican en: hardware, software, datos, redes, personal, servicios y soporte.

2.2.13. Impacto

Es la materialización de una amenaza que puede causar daño a un activo, su valoración generalmente se la realiza con las 3 dimensiones que son la confidencialidad, integridad, disponibilidad.

2.2.14. Análisis del riesgo

El análisis de riesgo comprende la identificación y la estimación del riesgo, para así poder tomar decisiones de cómo tratar el riesgo y ver que procesos o métodos serán utilizadas para su tratamiento.

Existen dos métodos de análisis de riesgos:

- Análisis de riesgo cuantitativo
- Análisis de riesgo cualitativo

2.2.15. Evaluación de riesgos

La evaluación de riesgos nos ayuda a identificar el nivel del riesgo en el que se encuentra un activo en la empresa, el riesgo se lo categoriza por la probabilidad e impacto y así se puede obtener una valoración cualitativo o cuantitativo.

Tabla 1

Matriz de riesgo

Matriz de valoración de riesgo		Impacto			
		Insignificante	Moderado	Dañino	Extremo
Probabilidad	Muy alta	Medio	Alto	Critico	Crítico
	Alta	Medio	Alto	Alto	Crítico
	Media	Bajo	Medio	Alto	Alto

	Baja	Bajo	Bajo	Medio	Medio

Fuente: Elaboración propia

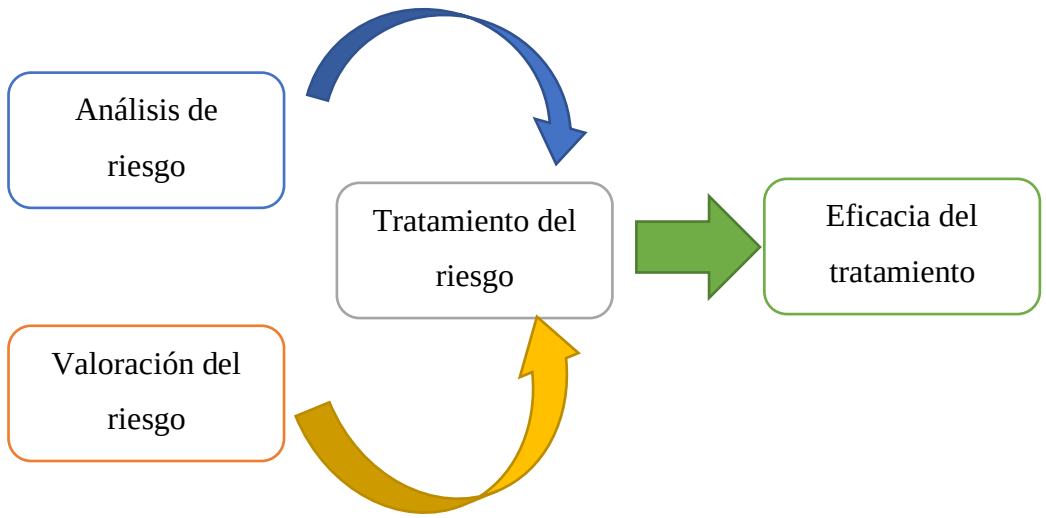
2.2.16. Tratamiento del riesgo

Se enfoca en seleccionar en una o más opciones de variación de riesgos y en ejecutar dichas opciones:

- Prevenir el riesgo (decidiendo no seguir con la tarea que lo motivo)
- Aceptar el riesgo o incrementarlo (en caso de una oportunidad)
- Quitar las fuentes del riesgo
- Cambiar las posibilidades de ocurrencia (transferir o mitigarlos)
- Aceptar el riesgo conjunto (con otras partes involucradas)

El proceso para administrar riesgos se acaba con la interrelación de todas las fases mencionadas con la comunicación y consultas, desde una perspectiva, y el control y revisión desde otra

Figura 6
Tratamiento de riesgos



Fuente: Elaboración propia

2.2.17. Valoración de riesgo

Es el primer paso en el enfoque de gestión de riesgos donde las organizaciones lo utilizan para cuantificar las amenazas y los riesgos en los sistemas tecnológicos en todo el desarrollo del proyecto.

2.2.18. Plan de contingencia

Un plan de contingencia es un conjunto de pasos o procesos cuyo objetivo principal es restablecer las actividades diarias en las organizaciones que tienen sistemas informáticos automatizados, del mismo modo que permite implantar normativas y medidas en caso de presentarse una eventualidad debido a un evento externo o interno con la finalidad de restablecer nuevamente la operatividad en las organizaciones(Burgos Gordón, 2020).

2.3. Cuadro comparativo de metodologías para el análisis de riesgos

Realizaremos un cuadro comparativo de las metodologías de análisis de riesgos investigadas anteriormente.

Tabla 2

Comparación de Metodologías

Metodología	Características	Aplicación
Octave	1.- No es una metodología únicamente técnica Aplicable para seguridad 2.- Presenta principios de sistemas de básicos y mejores prácticas | información de las Internacionales PYMES 3.- Relaciona amenazas y vulnerabilidades	Aplicable para seguridad de sistemas de información de las PYMES

Magerit	1- Orientada a los Sistemas de Información 2.- Tiene como objetivos: -Crear conciencia en el usuario de la existencia de riesgos y de la necesidad de prevenirlos - Analizar bajo un método sistemático tales riesgos - Ayudar a descubrir y planificar medidas oportunas para mantener bajo control los riesgos - Que la empresa pueda estar lista para procesos de evaluación, auditoría, certificación o acreditación, según el caso	Análisis y gestión de riesgos de los sistemas de información: Gobierno, Organismos, Compañías Grandes, PYME, Compañías Comerciales y no Comerciales
Mehari	1.Análisis o evaluación de riesgos 2.Evaluaciones de seguridad 3.Análisis de amenazas	Para todas las empresas

Fuente: Elaboración propia

2.4. Metodología de investigación aplicada

Luego de realizar el análisis respectivo y cumpliendo con el objetivo específico(**b**) se utilizará la metodología MAGERIT v3 debido a que tiene casos de éxitos en organizaciones privadas y por su amplia documentación, además MAGERIT cuenta con valoración de activos, amenazas y riesgos de una manera cualitativa o cuantitativa.

Se ha considerado como guía la norma ISO 31000 y la metodología MAGERIT v3 porque nos muestra la forma correcta de establecer la gestión de riesgos la cual nos permitirá detectar, prever y tratar a tiempo los incidentes que se presenten.

El proyecto consta de dos fases la cuales son, el análisis de riesgos y el plan de contingencia.

En la fase 1 es donde se identifican los activos más importantes de la empresa mediante sus 3 dimensiones (disponibilidad, integridad y confidencialidad), también se va identificar y valorar las amenazas de los activos con los resultados de las amenazas se darán mediante fórmulas que permiten calcular el impacto y el riesgo.

La fase 2 es donde se elaborará el plan de contingencia informático que es un documento el cual contiene pasos o procedimientos para responder en casos de siniestros a los sistemas informáticos a recobrar de una manera rápida el control y poder continuar sus operaciones con normalidad.

2.4.1. Fase 1: Análisis de riesgo

La fase del análisis de riesgos es el papel fundamental para la implementación del modelo, en esta fase se identificó los activos, las amenazas y así poder medir el nivel de criticidad cuando una amenaza llegue a materializarse.

El análisis de riesgo en un proceso sistemático para evaluar el alcance de los riesgos a que está expuesta la empresa, mediante el análisis de riesgos se deberá realizar los siguientes pasos.

Tabla 3

Pasos Para El Análisis De Riesgos

Análisis de riesgos	
Paso 1: Caracterización de los activos	Identificación de los activos Valoración de los activos
Paso 2: Caracterización de las amenazas	Identificación de las amenazas Valoración de las amenazas
Paso 3: Estimación del estado de riesgo	Estimación del riesgo

Fuente: Elaboración propia

2.4.1.1. Identificación de los activos

Para la identificación de activos se establecerá a los más críticos para la empresa, a continuación, se observará una tabla con los activos de acuerdo a su función considerando con la metodología MAGERIT v3.

Tabla 4

Identificación De Activos

Activo	Función
[D]Datos/Información	La información es un activo más importante para la organización
[S]Servicios	Satisface las necesidades de los usuarios
[SW]Software-Aplicaciones informáticas	Son tareas automatizadas por un equipo informático
[HW]Equipamiento informático(hardware)	Activos físicos de la organización
[COM]Redes de comunicaciones	Medios de transporte que llevan datos de un sitio a otro
[MEDIAS]Soportes de información	Almacenar información de manera permanente o largo periodos
[AUX]Equipamiento auxiliar	Complemento de equipos informáticos

Fuente: Elaboración propia

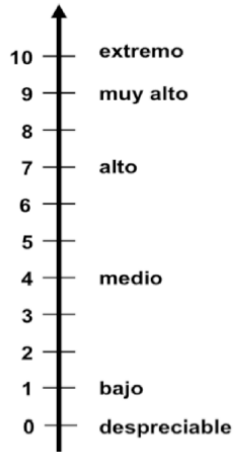
2.4.1.2. Valoración de activos

La valoración de un activo no se mide por su valor económico si no al valor de cada uno de los activos tomando en cuenta el grado de interés o su importancia.

Valoración cualitativa: Se le da valores a cada uno de los activos utilizando una escala de niveles (nulo, bajo, medio, alto, muy alto).

Criterio de valoración: Se valora a los activos, amenazas y riesgos mediante escala de niveles del 0 al 10, siendo 10 un máximo y el 0 un mínimo según el criterio de la organización.

Figura 7
Criterios de valoración



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Nota. La imagen nos muestra las escalas de valores de 0 – 10. Adaptado por Criterios de valoración, Ministerio de Administraciones Públicas de España, 2012, Fuente (Ministerio de Administraciones Públicas de España, 2012)

Dimensión de valoración: Son los atributos más valiosos de un activo, las dimensiones de un activo son la disponibilidad(D), integridad(I), disponibilidad(D).

Tabla 5
Dimensiones De Valoración De Los Activos

Dimensión	Descripción
Disponibilidad	Que importancia tendría el activo al no estar disponible para las personas autorizadas.
Integridad	Que importancia tendría si el activo sufriera modificaciones o daños.
Confidencialidad	Que importancia tendría si personas no autorizadas conociera la información del activo.

Fuente: Elaboración propia

Este mismo criterio de valoración se utilizará para las amenazas y los riesgos.

2.4.1.3. Identificación de amenazas

Después de identificar los activos, se procede a realizar la identificación y el análisis de las amenazas que afectan a los activos informáticos de las empresas, las amenazas son daños que causan a las empresas y saber cuan probable es que se materialice.

2.4.1.4. Valoración de las amenazas

Una vez identificada las amenazas, se procede a la valoración de los promedios de impacto de las amenazas que lleguen afectar a los activos y así identificar que tan dañino puede ser las amenazas sobre los activos, las amenazas se les da valores en sus 3 dimensiones que son la disponibilidad, integridad y confidencialidad y los criterios serian con la escala de 0 a 10 siendo 10 como máximo y 0 mínimo.

La fórmula para establecer el promedio de las amenazas es la siguiente:

Promedio de amenaza= la suma de las 3 dimensiones (D+I+C) * la importancia de un activo en %

2.4.1.5. Determinación de los niveles de riesgos

El nivel de riesgo es una estimación del daño causado al activo producido por la materialización de las amenazas afectando la operatividad de la empresa.
Conociendo la importancia de los activos, el promedio de las amenazas que están expuestas sobre un activo, los niveles de riesgo con los mismos criterios de valoración de la Figura 10 podremos determinar el nivel de riesgo.

La fórmula para el cálculo del riesgo es la siguiente:

Riesgo=Probabilidad * la suma de todos los promedios de las amenazas de cada uno de los activos

Tabla 6

Tabla de probabilidad

Nivel	Criterio
5	Muy Alto
4	Alto
3	Posible
2	Bajo
1	Raro

Fuente: Elaboración propia

2.4.2. Fase 2: Plan de contingencia

Cumpliendo con el objetivo específico (**c**) que es la elaboración de un plan de contingencia se realizó una comparativa con la metodología OCTAVE y la propuesta basada con la norma ISO/IEC 27001:2013, se optó por la norma ISO/IEC 27001:2013 debido a la que más se ajusta a las necesidades de la empresa por su simplicidad y su rápida ejecución.

Una vez evaluado los riesgos y se han identificado las amenazas potenciales que afectan a los activos, el siguiente paso es elaborar un plan de contingencia que ayudara a que los procesos críticos de la empresa continúen funcionando ante algún posible fallo en los sistemas tecnológicos y les permitirá seguir operando, aunque sea al mínimo de sus actividades.

El plan de contingencia consta de 4 etapas que son las siguientes:

2.4.2.1. Primera etapa: Planificación

En esta primera etapa es donde se revisa el estado actual de los sistemas tecnológicos y en donde se identifican los procesos más críticos de la empresa, para ello se realiza lo siguiente:

- Revisión del estado actual de los sistemas informáticos
- Inventarios de los activos más críticos

2.4.2.2. Segunda etapa: Revisión de riesgos

En esta segunda etapa es donde se realiza un estudio de los riesgos de los sistemas informáticos con su respectiva valoración de interrupción de servicios.

Para realizar el análisis de los riesgos se utilizará la metodología MAGERIT v3, el cual se podrá identificar los activos de mayor riesgo y de gran impacto. En el análisis de riesgos se podrá medir cualitativo las pérdidas que se podría tener en caso de algún siniestro.

- Listar y valorar los activos informáticos involucrados en cada proceso

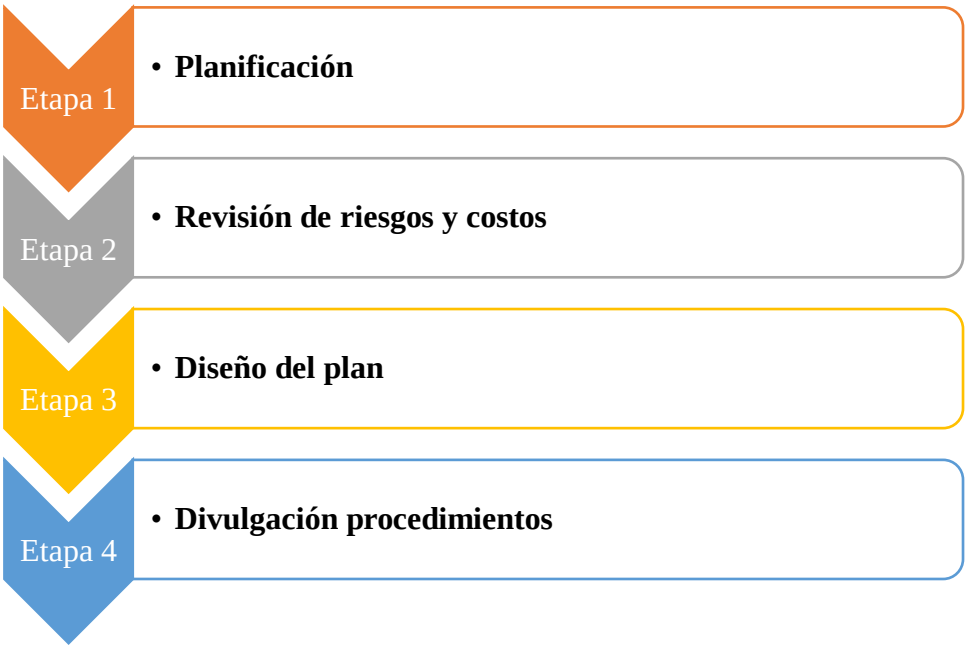
2.4.2.3. Tercera etapa: Diseño del plan

En esta tercera etapa se diseña los pasos o procedimientos y se genera el plan de contingencia en caso de algún siniestro.

2.4.2.4. Cuarta etapa: Divulgación procedimientos

En la cuarta etapa se define como se va a realizar la divulgación de los procedimientos al departamento de TI.

Figura 8
Etapas de la metodología del plan de contingencia de TI



Fuente: Elaboración Propia

CAPITULO III

MARCO METODOLÓGICO

3.1. Ubicación

La presente investigación, se realizó en la provincia de Tungurahua, cantón Ambato, en la empresa Importadora Alvarado Vásconez Cía. Ltda., tiene una trayectoria de 60 años en el mercado, ubicada en la Av. Panamericana norte Km. 7½ y Samanga, se establece en el mercado de autopartes y Repuestos para todo tipo de vehículos de todas las marcas a nivel nacional, beneficiando al desarrollo y progreso de las personas con el incremento de fuentes de empleo a las microempresas de la localidad que ha impulsado la economía local e incluso fuera de ellas.

3.1.1. Misión

Somos el proveedor de Línea y Servicios Automotrices preferido de mayoristas, minoristas y público en general, por nuestra disponibilidad de productos, variedad y asesoría de nuestro personal.

3.1.2. Visión

Ser el mayor distribuidor de Línea y Servicios Automotrices del Ecuador, con presencia en la zona Andina, reconocidos por la calidad de su gestión y su equipo humano.

3.2. Equipos y materiales

En esta investigación se utilizó los siguientes recursos:

Tabla 7

Equipos Y Materiales

Orden	Descripción	Unidad	Cantidad	Costo unitario(usd)	Costo Total(usd)
1	Computador	unidad	1	$1200	$1200
2	Impresora	unidad	1	$250	$250
3	Internet	horas	600	$0.10	$60
4	Hojas	unidad	1	$30	$30
				Costo total:	**$1.540**

Fuente: Elaboración propia

3.3. Tipo de investigación

3.3.1. Investigación Aplicada

Se utilizará la investigación aplicada debido a que se realizará los pasos necesarios para aplicar la metodología seleccionada correctamente.

3.3.2. Investigación Bibliográfica

La investigación será bibliográfica o documental, la cual nos permitirá conocer y profundizar en diferentes teorías relacionadas a nuestro tema de investigación basándonos en fuentes de información como libros, artículos científicos y tesis que nos ayudaran a tener un panorama más claro al problema de investigación.

3.3.3. Investigación de Campo

La investigación será de campo, la cual se acudirá a las instalaciones de la empresa para recopilar información de los activos informáticos, los procesos que cuenta actualmente el área de TI para determinar que metodología de análisis de riesgo se implementará para cumplir con los objetivos propuestos y el respectivo plan de contingencia.

3.3.4. Investigación Correlacional

La investigación será correlacional debido a que se va a realizar un tratamiento sobre los procesos en busca de menorar los riesgos informáticos.

3.3.5. Investigación Cuali-cuantitativo

Esta investigación tendrá el enfoque cuali-cuantitativo, debido a que se realizará una valoración de los activos informáticos para medir el nivel de riesgo y se realizará una entrevista al coordinador de TI.

3.4. Hipótesis de investigación

Con la implementación de la metodología de gestión de riesgo MAGERIT V3 y la ISO 31000 en la empresa Importadora Alvarado se reducirá los niveles de riesgo en los activos más críticos y se diseñará un plan de contingencia a los procesos críticos en caso de alguna amenaza se materialice, la empresa pueda seguir operando.

3.5. Población o muestra

La población o muestra de esta investigación es a los activos de mayor impacto tecnológicos del departamento de TI de la IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA., con un total de 27 activos asignando una valoración a la integridad, disponibilidad y confidencialidad en base a los criterios de valoración según la metodología MAGERIT v3, con este levantamiento de información se concluye el objetivo específico (**a**).

3.5.1. Identificación de activos

Tabla 8

Activos Tecnológicos

Ítem	Activo	Dimensiones			Importancia
		D	I	C	
A1	Switch T1600G-28TS	7	5	6	3
A2	Switch TL-SF1024	7	5	6	3
A3	Switch SF100-16	2	2	4	3
A4	Switch Core	9	6	8	9
A5	Switch Core SG- 500	9	6	6	7
A6	Firewall PA-820	9	8	8	9

A7	Servidor de Active Directory	9	5	7	9
A8	Servidor de File Server	5	9	9	8
A9	Servidor Wms - Iav	9	9	9	9
A10	Servidor Base datos - Compers	8	9	8	7
A11	Servidor Aplicaciones - Compers	8	5	8	7
A12	Central Telefónica - NS1000	6	5	5	5
A13	Correo Office 365	9	8	9	8
A14	BladeSystem Onboard Administrator C3000	9	5	8	10
A15	Storage P2000 CA	9	5	8	9
A16	Storage P2000 CB	9	5	8	9
A17	ProLiant BL460c Gen8 ESX1	9	5	9	10
A18	ProLiant BL460c Gen8 ESX2	9	5	9	10
A19	ProLiant BL460c Gen8 ESX3	9	5	9	10
A20	Servicio de internet	9	7	7	8
A21	Servidor Aplicativo - Web transaccional	9	8	9	9
A22	Servidor Base de datos - Web transaccional	9	8	9	9
A23	Antivirus	5	5	8	6
A24	Servidor Base datos Iav - GP	9	9	9	9
A25	Servidor Aplicaciones Iav - GP	9	8	8	8
A26	Servidor de Active Directory - Aws	9	7	7	8
A27	Servidor Postmaster - GP	7	5	7	5

Fuente: Elaboración propia

3.6. Recolección de información

Para la recolección de información se acudirá a la empresa para el levantamiento de información de los activos del departamento de TI.

Además, este trabajo de investigación se aplicó la observación directa porque se pone en contacto con el personal de TI y se acudirá a revisar la metodología que más se ajuste mediante investigaciones previas de otras empresas.

3.7. Procesamiento de la información y análisis estadístico

Para el procesamiento de la información y análisis estadísticos se utilizará los siguientes instrumentos:

1. Lectura de artículos relacionados al tema de investigación
2. Análisis y revisión de la información recogida
3. Entrevista al coordinador de TI
4. Listado de activos más críticos de la empresa
5. Revisión de la metodología

Finalmente, para le recolección de datos sobre los valores de criticidad de los indicadores de riesgo para los activos informáticos se utilizará la herramienta MAGERIT versión 3.0 y la norma ISO 31000, la cual se busca dar una solución a la problemática de la empresa.

3.8. Variables respuesta o resultados alcanzados

Con la información recopilada se pudo obtener los activos más críticos, las amenazas que afectarían a los activos y así obtener el nivel de riesgo.

Nuestras variables de respuesta son las amenazas que tienen el nivel de riesgo medio, alto y muy alto, lo cual se tratara mediante un plan de contingencia para poder actuar de mejor manera reduciendo los tiempos de inactividad y así asegurar el nivel de servicio.

Tabla 9

Análisis Estadístico

Variables	**Definición**	**Indicador**	**Técnica/instrumento**
Condiciones inadecuadas de	Deficiencia en la climatización:	Planes de mantenimiento	Entrevista/Observación

temperatura o humedad	excesivo calor o excesivo frio	preventivos y correctivos	
Acceso no autorizado	Acceso a los recursos sin autorización	Políticas de seguridad que los usuarios deben conocer	Entrevista/Observación
Avería de origen físico o lógico	Fallos en los equipos o en los programas	Planes de mantenimiento preventivos o propuesta de renovación de equipos tecnológicos	Entrevista/Observación
Errores del administrador	Equivocaciones no intencionadas	Propuestas de cursos o capacitaciones al personal	Observación
Suplantación de la identidad del usuario	Ingreso a los sistemas por un usuario autorizado	Políticas de caducidad de contraseñas.	Observación
Caída del sistema por agotamiento de recursos	Pocos recursos cuando se trabaja con cargas elevadas	Presupuesto para la adquisición de nuevos recursos.	Observación
Denegación de servicio	Intento malicioso de sobre carga de tráfico	Adquisición de herramientas para mantener protegidos.	Observación

Fuente: Elaboración propia

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Resultados Pre-Implementación

Para conocer la situación actual de la empresa Importadora Alvarado sobre riesgos, amenazas e incidentes informáticos, se realizó una entrevista al coordinador de TI, quién supo manifestar los siguientes datos relevantes para el desarrollo del proyecto.

4.1.1. Entrevista al coordinador de TI

Pregunta 1: ¿Qué daños en los activos tecnológicos ha tenido la empresa Importadora Alvarado en los últimos años?

La respuesta del entrevistado a la pregunta fue: la empresa últimamente ha tenido apagado de algunos Blade (donde se alojan las máquinas virtuales) debido a que el aire acondicionado presenta fallos físicos en el cuarto de equipos.

Pregunta 2: De lo mencionado anteriormente, ¿Cuenta con respaldos de los activos tecnológicos que han tenido problemas?

La respuesta del coordinado fue: Los Blade que presentan apagones debido al aire acondicionado y donde se encuentran las máquinas virtuales no se tiene respaldos, debido a que si se presenta algún daño físico o lógico la empresa sufriría la paralización de algunas de sus actividades.

Pregunta 3: ¿Tienen identificados los activos tecnológicos por niveles de importancia y de criticidad?

La respuesta del entrevistado nos indicó: La empresa actualmente no cuenta con un registro de valoración de activos para poder identificar los activos más críticos y de mayor impacto que cuenta la empresa.

Pregunta 4: ¿Cuáles amenazas consideraría usted que podría tener sus activos tecnológicos en su empresa?

La respuesta del coordinador fue la siguiente: Las amenazas que consideramos importantes son los desastres naturales, el phishing por medio de correos electrónicos, la fuga de información y daños inesperados en los servidores más antiguos.

Pregunta 5: ¿Cuentan con planes de contingencia en caso de que alguna amenaza llegara a materializarse?

El coordinador de TI nos indicó: El departamento de TI actualmente no cuenta con planes de contingencia para poder estar preparados o prevenidos en caso de algún imprevisto llegara a ocasionarse.

Pregunta 6: ¿Cuentan con equipos tecnológicos que ya hayan cumplido su ciclo de vida?

La respuesta del entrevistado fue: En el data center de la empresa cuentan con equipos que ya superan su clico de vida como el Blade y unos switchs que están comenzando a dar alertas de diferente tipo.

4.2.Discusión

Estos resultados concuerdan con los de Huefle Arévalo (2021) quien en su investigación se refirió que implementar la metodología MAGERIT permitirá identificar las amenazas y los riesgos potenciales a los que están expuestos mediante los 3 pilares que son la confidencialidad, disponibilidad y la integridad, lo cual podrán establecer estrategias para reducir las amenazas a la que están sometido los activos informáticos.

Por su parte Burgos Gordón (2020) señalo que con un plan de contingencia se puede tener un control sobre los activos informaticos logrando cuando se presente algun siniestro por diferentes circunstancias puedan establecer controles y tomar las medidas necesarias para proteger los activos informaticos. Con estas medidas la empresa pueda seguir operando al minimo de sus actividades.

4.3. Aplicación de la metodología

Para la evaluación de riesgos se aplicó la fase 1 donde contiene una secuencia de tareas, con el objetivo de alcanzar los resultados necesarios para el diseño del plan de contingencia de los activos tecnológicos de la Importadora Alvarado aplicado en la fase 2.

Se utilizará la metodología MAGERIT v3 con la norma ISO31000 bajo un enfoque cualitativo que nos permite avanzar con rapidez y utiliza una escala de valores para identificar las amenazas que fueron ocurridos o que podrían ocurrir.

4.3.1. Fase 1: Análisis de riesgos

4.3.1.1. Identificación de activos

La identificación de activos más críticos dentro del departamento de tecnología se estableció con el coordinador de TI, considerando la lista de activos de la metodología MAGERIT v3 establecida en la tabla 4.

Tabla 10

Identificación De Activos De Importadora Alvarado

Item	Activos	Tipo de activo	Ubicación	Responsable	Descripción
A1	Switch T1600G-28TS	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch de capa de acceso
A2	Switch TL-SF1024	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch de capa de acceso
A3	Switch SF100-16	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch de capa de acceso
A4	Switch Core	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch core central
A5	Switch Core SG-500	[COM] Redes de	Rack Bodega	Analista de infraestructura	Switch de capa de acceso

		comunicaciones			
A6	Firewall PA-820	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Firewall de seguridad perimetral
A7	Servidor de Active Directory	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server de Active directory
A8	Servidor de File Server	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server de File Server
A9	Servidor Wms - Iav	[SW] Aplicaciones (software)	Data Center Edificio	Analista de aplicaciones	Windows Server Sistema de bodega
A10	Servidor Base datos - Compers	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server Sistema de bodega - Corpal
A11	Servidor Aplicaciones - Compers	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server de base de datos - Corpal
A12	Central Telefónica - NS1000	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Central telefónica
A13	Correo Office 365	[S] Servicios	Data Center Edificio	Analista de infraestructura	Correos de office 365
A14	BladeSystem Onboard Administrator C3000	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Chasis donde se incorporan los Blades
A15	Storage P2000 CA	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	San de Almacenamiento de datos 1
A16	Storage P2000 CB	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	San de Almacenamiento de datos 2
A17	ProLiant BL460c Gen8 ESX1	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Blade 1 con SO Vmware
A18	ProLiant BL460c Gen8 ESX2	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Blade 2 con SO Vmware

A19	ProLiant BL460c Gen8 ESX3	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Blade 3 con SO Vmware
A20	Servicio de internet	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Servicio de internet
A21	Servidor Aplicativo - Web transaccional	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor Ubuntu server donde se encuentra la aplicación web
A22	Servidor Base de datos - Web transaccional	[SW] Aplicaciones (software)	Data Center Edificio	Analista de aplicaciones	Servidor Aurora donde se aloja la base de datos de la web
A23	Antivirus	[SW] Aplicaciones (software)	Proveedor externo Sophos	Analista de infraestructura	Servidor de Sophos
A24	Servidor Base datos Iav - GP	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor Sql Server de Microsoft GP
A25	Servidor Aplicaciones Iav - GP	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor de aplicaciones de Microsoft GP
A26	Servidor de Active Directory - Aws	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor replica de Active Directory en la nube
A27	Servidor Postmaster - GP	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor de autoposting para la contabilización automática de facturas

Fuente: Elaboración propia

4.3.1.2. Valoración de activos

Se valoriza a los activos más importantes de la empresa con la ayuda del coordinador de TI dando criterios a sus 3 dimensiones: disponibilidad(D), integridad(I), confidencialidad(C), ya que son los más importantes para valoración de los activos.

Para la valoración de los activos se utilizó los criterios de valoración de la figura 10.

Tabla 11

Valoración De Activos De Importadora Alvarado

Item	Activos	Dimensiones			Importancia
		D	I	C	
A1	Switch T1600G-28TS	7	5	6	5
A2	Switch TL-SF1024	7	5	6	5
A3	Switch SF100-16	2	2	4	3
A4	Switch Core	9	6	8	9
A5	Switch Core SG- 500	9	6	6	7
A6	Firewall PA-820	9	8	8	9
A7	Servidor de Active Directory	9	5	7	9
A8	Servidor de File Server	5	9	9	8
A9	Servidor Wms - Iav	9	9	9	9
A10	Servidor Base datos - Compers	8	9	8	7
A11	Servidor Aplicaciones - Compers	8	5	8	7
A12	Central Telefónica - NS1000	3	3	3	3
A13	Correo Office 365	9	8	9	8
A14	Blade System Onboard Administrator C3000	9	5	8	10
A15	Storage P2000 CA	9	5	8	9
A16	Storage P2000 CB	9	5	8	9
A17	ProLiant BL460c Gen8 ESX1	9	5	9	10

A18	ProLiant BL460c Gen8 ESX2	9	5	9	10
A19	ProLiant BL460c Gen8 ESX3	9	5	9	10
A20	Servicio de internet	9	7	7	8
A21	Servidor Aplicativo - Web transaccional	9	8	9	9
A22	Servidor Base de datos - Web transaccional	9	8	9	9
A23	Antivirus	5	5	8	6
A24	Servidor Base datos Iav - GP	9	9	9	9
A25	Servidor Aplicaciones Iav - GP	9	8	8	8
A26	Servidor de Active Directory - Aws	9	7	7	8
A27	Servidor Postmaster - GP	2	2	2	2

Fuente: Elaboración propia

4.3.1.3. Identificación de amenazas

Es identificar todas las amenazas que atentan a los activos de TI con la ayuda del coordinador de tecnología y las observaciones realizadas en el departamento de TI, se utilizó el catálogo de amenazas publicadas en la metodología MAGERIT v3, el departamento de tecnología presenta las siguientes amenazas:

Tabla 12

Identificación De Amenazas De Importadora Alvarado

Categoría	**Amenaza**
[N] Desastres naturales	Desastres Naturales
	Corte del suministro eléctrico

[I] De origen industrial	Condiciones inadecuadas de temperatura o humedad
	Fallo de servicios de comunicaciones
	Avería de origen físico o lógico
	Errores del administrador
	Errores de configuración
	Alteración accidental de la información
	Vulnerabilidades de los programas (software)
[E] Errores y fallos no intencionados	Destrucción de información
	Errores de mantenimiento / actualización de programas (software)
	Caída del sistema por agotamiento de recursos
	Suplantación de la identidad del usuario
	Difusión de software dañino
	Acceso no autorizado
[A] Ataques intencionados	Divulgación de información
	Denegación de servicio
	Ingeniería social (picaresca)

Fuente: Elaboración propia

4.3.1.4. Valoración de las amenazas

Una vez identificada las amenazas que puedan afectar a los activos de TI se procede a la valoración de las amenazas, planteándonos preguntas como: ¿Qué daño causaría si personas no autorizadas llegaran a conocer?, ¿Qué problema causaría no tenerlo o no poder utilizarlo?, ¿Qué problema causaría que estuviera dañado o averiado?, para así dar valores a sus dimensiones: disponibilidad(D), integridad(I), confidencialidad(C).

Promedio= Importancia del activo en % * la suma de las dimensiones(D+I+C)

Tabla 13

Valoración De La Amenazas Con Los Promedios De Impacto

Item	Activo	Amenazas	Importancia Activo(A)	Dimensiones			Suma de las dimensiones(B)	Promedio (A%*B)
				D	I	C		
A1	Switch T1600G-28TS	Condiciones inadecuadas de temperatura o humedad	5	5	0	0	5	0.25
		Avería de origen físico o lógico		5	0	0	5	0.25
A2	Switch TL-SF1024	Condiciones inadecuadas de temperatura o humedad	5	3	0	0	3	0.15
		Avería de origen físico o lógico		3	0	0	3	0.15
A3	Switch SF100-16	Condiciones inadecuadas de temperatura o humedad	3	3	0	0	3	0.09
		Avería de origen físico o lógico		3	0	0	3	0.09
A4	Switch Core-Aruba	Condiciones inadecuadas de temperatura o humedad	9	6	0	0	6	0.54
		Acceso no autorizado		0	2	6	8	0.72
		Avería de origen físico o lógico		8	0	0	8	0.72
A5	Switch Core SG- 500	Corte del suministro eléctrico	7	5	0	0	5	0.35
		Acceso no autorizado		0	2	6	8	0.56
		Avería de origen físico o lógico		8	0	0	8	0.56
A6	Firewall PA-820	Condiciones inadecuadas de temperatura o humedad	9	9	0	0	9	0.81
		Acceso no autorizado		0	6	5	11	0.99
		Errores del administrador		7	3	5	15	1.35
A7	Servidor de Active Directory	Condiciones inadecuadas de temperatura o humedad	9	6	0	0	6	0.54
		Acceso no autorizado		0	3	6	9	0.81

		Avería de origen físico o lógico		8	0	0	8	0.72
A8	Servidor de File Server	Condiciones inadecuadas de temperatura o humedad	8	7	0	0	7	0.56
		Destrucción de información		9	0	0	9	0.72
		Divulgación de información		0	0	9	9	0.72
		Alteración accidental de la información		0	9	0	9	0.72
A9	Servidor Wms - Iav	Condiciones inadecuadas de temperatura o humedad	9	9	0	0	9	0.81
		Acceso no autorizado		0	7	8	15	1.35
		Destrucción de información		6	0	0	6	0.54
A10	Servidor Base datos - Compers	Condiciones inadecuadas de temperatura o humedad	7	6	0	0	6	0.42
		Acceso no autorizado		0	7	6	13	0.91
		Alteración accidental de la información		0	8	0	8	0.56
A11	Servidor Aplicaciones - Compers	Condiciones inadecuadas de temperatura o humedad	7	4	0	0	4	0.28
		Avería de origen físico o lógico		5	0	0	5	0.35
		Acceso no autorizado		0	5	6	11	0.77
A12	Central Telefónica - NS1000	Avería de origen físico o lógico	3	5	0	0	5	0.15
		Ingeniería social (picaresca)		3	7	8	18	1.44
A13	Correo Office 365	Difusión de software dañino	8	6	8	3	17	1.36
		Suplantación de la identidad del usuario		3	6	7	16	1.28
A14	BladeSystem Onboard	Condiciones inadecuadas de temperatura o humedad	10	9	0	0	9	0.9
		Fallo de servicios de comunicaciones		9	0	0	9	0.9

	Administrator C3000	Avería de origen físico o lógico		9	0	0	9	0.9
A15	Storage P2000 CA	Condiciones inadecuadas de temperatura o humedad	9	9	0	0	9	0.81
		Avería de origen físico o lógico		9	0	0	9	0.81
A16	Storage P2000 CB	Condiciones inadecuadas de temperatura o humedad	9	9	0	0	9	0.81
		Avería de origen físico o lógico		10	0	0	10	0.9
A17	ProLiant BL460c Gen8 ESX1	Condiciones inadecuadas de temperatura o humedad	10	10	0	0	10	1
		Caída del sistema por agotamiento de recursos		8	0	0	8	0.8
		Avería de origen físico o lógico		9	0	0	9	0.9
A18	ProLiant BL460c Gen8 ESX2	Condiciones inadecuadas de temperatura o humedad	10	10	0	0	10	1
		Caída del sistema por agotamiento de recursos		8	0	0	8	0.8
		Avería de origen físico o lógico		9	0	0	9	0.9
A19	ProLiant BL460c Gen8 ESX3	Condiciones inadecuadas de temperatura o humedad	10	10	0	0	10	1
		Caída del sistema por agotamiento de recursos		8	0	0	8	0.8
		Avería de origen físico o lógico		9	0	0	9	0.9
A20	Servicio de internet	Desastres Naturales	8	9	0	0	9	0.72
		Fallo de servicios de comunicaciones		8	0	0	8	0.64
A21	Servidor Aplicativo - Web transaccional	Avería de origen físico o lógico	9	9	0	0	9	0.81
		Acceso no autorizado		0	8	7	15	1.35
		Denegación de servicio		9	0	0	9	0.81

		Denegación de servicio		9	0	0	9	0.81
A22	Servidor Base de datos - Web transaccional	Caída del sistema por agotamiento de recursos	9	9	0	0	9	0.81
		Acceso no autorizado		0	8	9	17	1.53
		Divulgación de información		0	0	9	9	0.81
A23	Antivirus-Sophos	Manipulación de la configuración	6	5	6	6	17	1.02
		Suplantación de la identidad del usuario		5	6	6	17	1.02
		Avería de origen físico o lógico		7	0	0	7	0.63
A24	Servidor Base datos Iav - GP	Alteración accidental de la información	9	9	0	0	9	0.81
		Errores del administrador		8	9	9	26	2.34
		Avería de origen físico o lógico		5	0	0	5	0.4
A25	Servidor Aplicaciones Iav - GP	Suplantación de la identidad del usuario	8	4	4	6	14	1.12
		Acceso no autorizado		0	5	8	13	1.04
		Avería de origen físico o lógico		8	0	0	8	0.64
A26	Servidor de Active Directory - Aws	Errores del administrador	8	8	8	5	21	1.68
		Errores de configuración		0	6	0	6	0.48
A27	Servidor Postmaster - GP	Acceso no autorizado	2	0	2	2	4	0.08

Fuente: Elaboración propia

4.3.1.5. Determinación del riesgo

El riesgo es la medida del daño causado por la materialización de las amenazas sobre uno o más activos perjudicando gravemente a la empresa, conociendo la importancia de los activos del departamento de TI y las amenazas a las que están expuestas se procede al cálculo.

Tabla 14

Determinación Del Riesgo

Amenazas	Activos	Total de promedio de las amenaza	Suma de los promedios de las amenazas (Impacto)	Probabilidad (P)	Nivel de riesgo (P*I)	Nivel
Condiciones inadecuadas de temperatura o humedad	A1	0.25	3.5	4	14	Riesgo muy alto
	A2	0.15				
	A3	0.09				
	A4	0.54				
	A6	0.81				
	A7	0.54				
	A8	0.56				
	A11	0.28				
	A11	0.28				
Acceso no autorizado	A4	0.72	10.11	3	30.33	Riesgo muy alto
	A5	0.56				
	A6	0.99				
	A7	0.81				
	A9	1.35				
	A10	0.91				
	A11	0.77				
	A21	1.35				
	A22	1.53				
	A25	1.04				

	A27	0.08				
	A1	0.25				
	A2	0.15				
	A3	0.09				
	A4	0.72				
	A5	0.56				
	A7	0.72				
	A11	0.35				
	A12	0.15				
	A14	0.9				
Avería de origen físico o lógico	A15	0.81	11.59	3	34.77	Riesgo muy alto
	A16	0.9				
	A17	0.9				
	A18	0.9				
	A19	0.9				
	A21	0.81				
	A22	0.81				
	A24	0.63				
	A25	0.4				
	A26	0.64				
Corte del suministro eléctrico	A5	0.35	0.35	3	1.05	Riesgo Muy Bajo
	A6	1.35				
Errores del administrador	A24	2.34	5.37	3	16.11	Riesgo muy alto
	A26	1.68				
Destrucción de información	A8	0.72	1.26	2	2.52	Riesgo Muy Bajo
	A9	0.54				
Divulgación de información	A8	0.72	1.53	3	4.59	Riesgo Muy Bajo
	A22	0.81				

Alteración accidental de la información	A8 A24	0.72 0.81	1.53	3	4.59	Riesgo Muy Bajo
Ingeniería social (picaresca)	A13	1.44	1.44	3	4.32	Riesgo Muy Bajo
Difusión de software dañino	A13	1.36	1.36	3	4.08	Riesgo Muy Bajo
Suplantación de la identidad del usuario	A13 A25 A23	1.28 1.12 1.02	3.42	3	10.26	Riesgo alto
Fallo de servicios de comunicaciones	A14 A20	0.9 0.64	1.54	3	4.62	Riesgo Muy Bajo
Caída del sistema por agotamiento de recursos	A17 A22 A19	0.8 0.81 0.8	2.41	3	7.23	Riesgo medio
Desastres Naturales	A20	0.72	0.72	3	2.16	Riesgo Muy Bajo
Denegación de servicio	A21 A22	0.81 0.81	1.62	4	6.48	Riesgo medio
Manipulación de la configuración	A23	1.02	1.02	3	3.06	Riesgo Muy Bajo

Fuente: Elaboración propia

Tabla 15

Prioridad De Las Amenazas Según El Riesgo Obtenido

Amenaza	Prioridad			
	Muy bajo	**Medio**	**Alto**	**Muy alto**
Condiciones inadecuadas de temperatura o humedad				
Acceso no autorizado				
Avería de origen físico o lógico				
Corte del suministro eléctrico				
Errores del administrador				
Destrucción de información				
Divulgación de información				
Alteración accidental de la información				
Ingeniería social (picaresca)				
Difusión de software dañino				
Suplantación de la identidad del usuario				
Fallo de servicios de comunicaciones				
Caída del sistema por agotamiento de recursos				
Desastres Naturales				
Denegación de servicio				
Manipulación de la configuración				

Fuente: Elaboración propia

4.3.2. Fase 2: Plan de contingencia

En esta fase es donde se elaborará el plan de contingencia para los procesos más críticos de la empresa Importadora Alvarado, la cual se va a desarrollar siguiendo los cuatros etapas:

- Revisión del estado actual
- Revisión de riesgos
- Diseño del plan
- Divulgación de procedimientos

Para la elaboración del plan de contingencia se debe realizar un análisis de riesgos el cual busca establecer los activos informáticos que están expuestos a un mayor riesgo

en caso de que se materialice las amenazas, para el análisis de riesgos se utilizó la metodología MAGERIT v3.

4.3.2.1. Primera etapa: Planificación

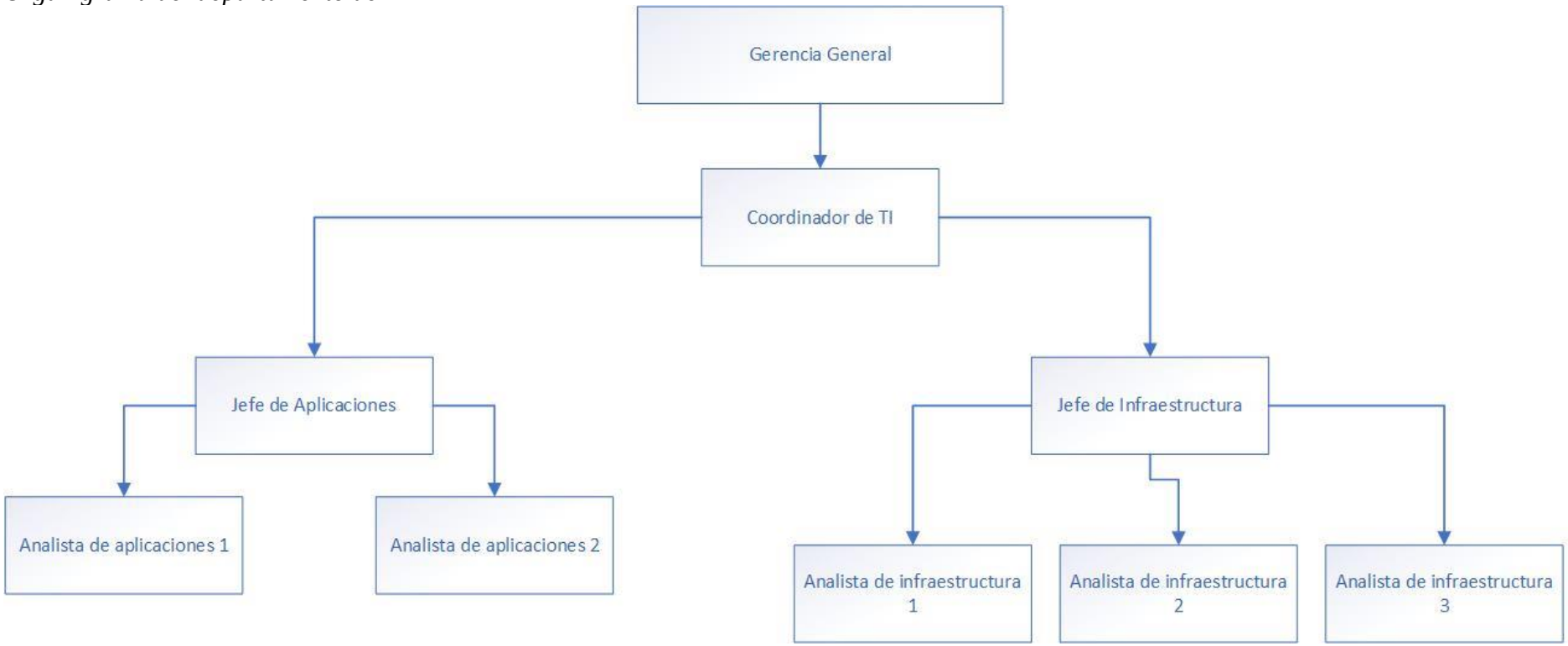
La infraestructura tecnológica de la empresa Importadora Alvarado está funcionando más de 10 años y se ha ido implementando con diferentes servicios tecnológicos de acuerdo a sus tres procesos principales que son: las ventas por internet, sistema de despachos y su ERP.

La cual ha dado lugar a que su infraestructura por su tiempo de vida útil a comenzado a dar alertas de fallos lógicos y a tener firmware desactualizados, lo que se avisto en la necesidad de elaborar un plan de contingencia que ayudara a la empresa a estar preparados en caso de algún siniestro a los activos informáticos y recobrar rápidamente sus operaciones.

Para verificar el estado actual de los sistemas informáticos se tendrá la siguiente información:

- Organigrama del departamento de TI en la Figura 9.
- Inventario de los activos más críticos en la Tabla 16.
- Arquitectura de la infraestructura tecnológica en el Figura 10.

Figura 9
Organigrama del departamento de TI



Fuente: Elaboración propia

Tabla 16

Inventario De Activos De Ti

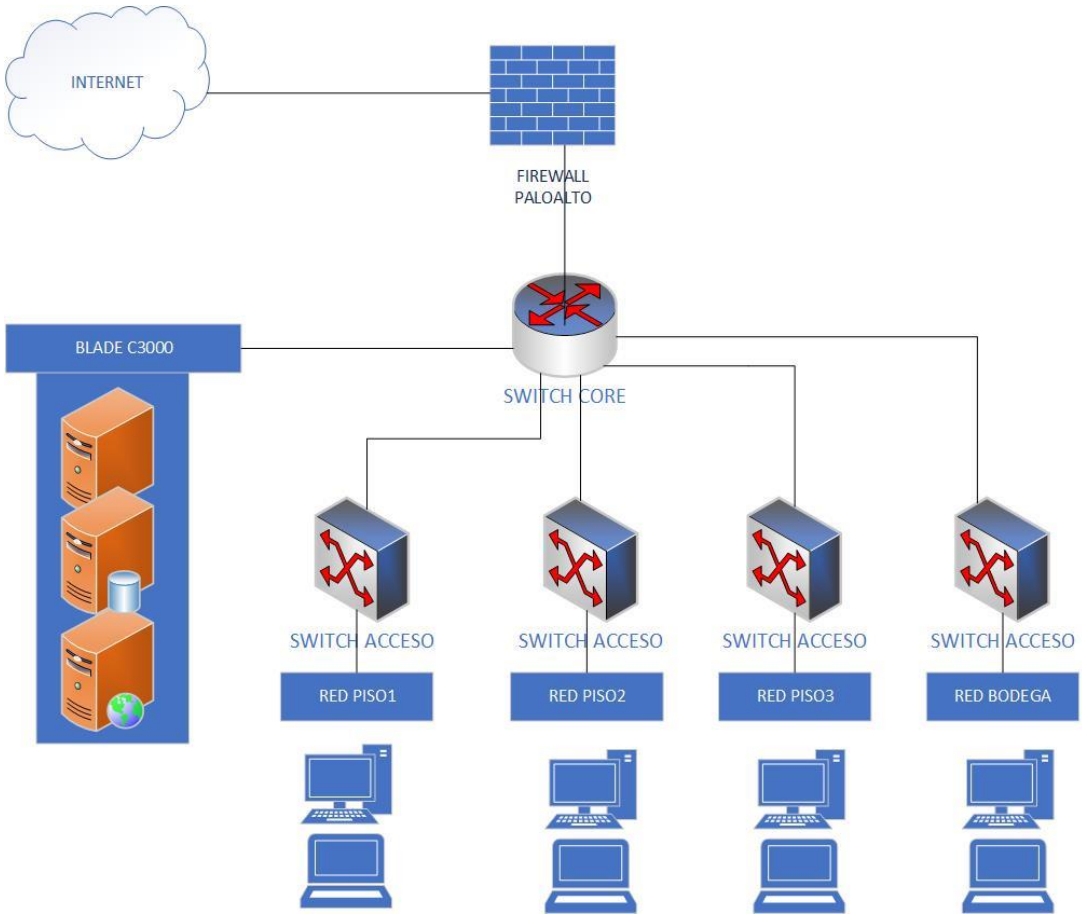
Ítem	Activos	Tipo de activo	Ubicación	Responsable	Descripción
A1	Switch T1600G-28TS	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch de capa de acceso
A2	Switch TL-SF1024	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch de capa de acceso
A3	Switch SF100-16	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch de capa de acceso
A4	Switch Core	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Switch core central
A5	Switch Core SG-500	[COM] Redes de comunicaciones	Rack Bodega	Analista de infraestructura	Switch de capa de acceso
A6	Firewall PA-820	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Firewall de seguridad perimetral
A7	Servidor de Active Directory	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server de Active directory
A8	Servidor de File Server	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server de File Server
A9	Servidor Wms - Iav	[SW] Aplicaciones (software)	Data Center Edificio	Analista de aplicaciones	Windows Server Sistema de bodega
A10	Servidor Base datos - Compers	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server Sistema de bodega - Corpal
A11	Servidor Aplicaciones - Compers	[SW] Aplicaciones (software)	Data Center Edificio	Analista de infraestructura	Windows Server de base de datos - Corpal

A12	Central Telefónica - NS1000	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Central telefónica
A13	Correo Office 365	[S] Servicios	Data Center Edificio	Analista de infraestructura	Correos de office 365
A14	BladeSystem Onboard Administrator C3000	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Chasis donde se incorporan los Blades
A15	Storage P2000 CA	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	San de Almacenamiento de datos 1
A16	Storage P2000 CB	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	San de Almacenamiento de datos 2
A17	ProLiant BL460c Gen8 ESX1	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Blade 1 con SO Vmware
A18	ProLiant BL460c Gen8 ESX2	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Blade 2 con SO Vmware
A19	ProLiant BL460c Gen8 ESX3	[HW] equipos informáticos (hardware)	Data Center Edificio	Analista de infraestructura	Blade 3 con SO Vmware
A20	Servicio de internet	[COM] Redes de comunicaciones	Data Center Edificio	Analista de infraestructura	Servicio de internet
A21	Servidor Aplicativo - Web transaccional	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor Ubuntu server donde se encuentra la aplicación web
A22	Servidor Base de datos - Web transaccional	[SW] Aplicaciones (software)	Data Center Edificio	Analista de aplicaciones	Servidor Aurora donde se aloja la base de datos de la web
A23	Antivirus	[SW] Aplicaciones (software)	Proveedor externo Sophos	Analista de infraestructura	Servidor de Sophos
A24	Servidor Base datos Iav - GP	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor Sql Server de Microsoft GP

A25	Servidor Aplicaciones Iav - GP	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor de aplicaciones de Microsoft GP
A26	Servidor de Active Directory - Aws	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor replica de Active Directory en la nube
A27	Servidor Postmaster - GP	[SW] Aplicaciones (software)	Proveedor externo Amazon Aws	Analista de aplicaciones	Servidor de autoposting para la contabilización automática de facturas

Fuente: Elaboración propia

Figura 10
Arquitectura de red



Fuente: Elaboración propia

4.3.2.2. Segunda etapa: Revisión de riegos

En esta etapa se busca identificar las vulnerabilidades enfocados solo para casos de siniestros en los activos tecnológicos, además se realizará la valoración por la interrupción del servicio.

Para el análisis de riesgos se utilizó la metodología MAGERIT v3 para identificar los activos tecnológicos que están expuestos a un mayor riesgo y los que producirían un gran impacto en caso de materializarse las amenazas, lo que nos llevó a desarrollar los siguientes pasos:

- Identificar los activos tecnológicos
- Valoración de los activos
- Identificación de las amenazas
- Valoración de las amenazas
- Determinación del riesgo

- **Identificación de activos tecnológicos**

La identificación de activos se encuentra en la fase 1, en el numeral 4.3.1.1

- **Valoración de los activos**

La valoración de los activos se encuentra en la fase 1, en el numeral 4.3.1.2

- **Identificación de amenazas**

La identificación de amenazas se encuentra en la fase 1, en el numeral 4.3.1.3

- **Valoración de las amenazas**

La valoración de las amenazas se encuentra en la fase 1, en el numeral 4.3.1.4

- **Determinación del riesgo**

La determinación del riesgo se encuentra en la fase 1, en el numeral 4.3.1.5

4.3.2.3. Tercera etapa: Diseño del plan

En esta etapa se procede a elaborar los procedimientos y se genera el plan de contingencia en caso de presentarse un siniestro.

4.3.2.3.1. Procedimientos de reanudación

Son los primeros procedimientos a ejecutar para recuperar los procesos más críticos de la empresa después de una contingencia, los cuales se cuentan con:

- Procesos críticos en el Anexo B
- Cuadro de evaluación Anexo C

- **Procedimientos recuperación ERP – Sistema empresarial contable**

Para el óptimo funcionamiento de esta aplicación se necesita que este implementada en 3 servidores los cuales son:

- Servidor de base de datos
- Servidor de aplicaciones ERP
- Servidor de Postmaster

Para restablecer el servidor de base de datos se debe realizar los siguientes pasos:

- Levantar la imagen del servidor de base de datos
- Descargar el backup ubicado en el repositorio de respaldos S3
- Restaurar el backup (.slq) en el motor de base de datos Sql Server
- Realizar pruebas de validación que no haya tenido ningún error al momento de importar

Para restablecer el servidor de aplicaciones ERP se debe realizar los siguientes pasos

- Levantar la imagen del servidor de aplicaciones

- Transferir la carpeta GP2018 ubicado en el repositorio de backup
- Reemplazar en la ubicación C:/GP2018 para actualizar los desarrollos implementados
- Revisar la cadena de conexión que este apuntando al servidor de base de datos ubicado en la herramienta ODBC de Windows – System DNS – Dynamics GP2018

Para restablecer el servidor de Postmaster se debe realizar los siguientes pasos:

- Levantar la imagen del servidor de aplicaciones
- Transferir la carpeta GP2018 ubicado en el repositorio de backup
- Reemplazar en la ubicación C:/GP2018
- Revisar la cadena de conexión que este apuntando al servidor de base de datos ubicado en la herramienta ODBC de Windows – System DNS – Dynamics GP2018

- **Procedimiento recuperación de la Web Transaccional**

Para el óptimo funcionamiento de esta aplicación se requiere que este implementado en 3 servidores, los cuales son:

- Servidor Linux Ubuntu Server
- Motor de base de datos Aurora
- Servidor de WebServices

Para restablecer el servidor de Ubuntu Server se debe realizar los siguientes pasos:

- Levantar la imagen del Servidor Ubuntu
- Transferir la carpeta IAVWT ubicado en el repositorio de backup
- Reemplazar en la ubicación /var/www/html/IAVWT para mantener actualizado los desarrollos implementados
- Validar que esté funcionando la página ingresando a ventas.iav.com.ec

Para restablecer el motor de base de datos Aurora se debe realizar los siguientes pasos:

- Levantar la imagen del motor de base de datos Aurora
- Subir el respaldo de la base de datos ubicado en el repositorio de backup

Para restablecer el servidor de los WebServices se debe realizar los siguientes pasos:

- Levantar la imagen del servidor de WebServices
- Transferir la carpeta WEBWMS ubicado en el repositorio de backup
- Reemplazar en la ubicación C:/Publicaciones/WebServices para mantener actualizado los desarrollos implementados
- Iniciar el IIS
- Verificar que estén funcionando ingresando en un navegador 18.225.117.52/WEBWMS

- **Procedimiento recuperación de WMS – Sistema de bodega**

  Para el óptimo funcionamiento de esta aplicación se requiere que este implementado en 1 servidor el cual contiene el motor de base de datos y la aplicación, el cual es:

- Servidor Wms y de la aplicación

Para restablecer el servidor de wms se debe realizar los siguientes pasos:

- Levantar la imagen del servidor
- Descargar el backup ubicado en el repositorio de respaldos S3
- Restaurar el backup (.slq) en el motor de base de datos Sql Server
- Transferir la carpeta WMSiav ubicado en el repositorio de backup
- Reemplazar en la ubicación E:\PUBLICACIONES\WMSiav
- Iniciar el IIS

- **Procedimiento recuperación del servicio de Internet**

Para el óptimo funcionamiento de este servicio se requiere lo siguiente:

- Verificar con el proveedor de internet para ver cuál es la causa de la caída del internet
- Después de verificar la causa, decir al proveedor que reenvíen el tráfico de internet por la otra fibra de backup
- Realizar el cambio en el Firewall perimetral para que salgan los usuarios por el internet de backup
- Comprobar el internet con los usuarios

4.3.2.3.2. Estructura organizacional para la contingencia

Es donde se define la estructura organizacional para formar un comité de contingencia, el cual se encargará de llevar las acciones en una emergencia con planes ya definidos.

Para definir la estructura organizacional que se encargue de restablecer los sistemas a la normalidad en caso de algún siniestro, deben existir dos equipos que actúen directamente.

Primer equipo: Tendrá la tarea enfrentar el siniestro
Segundo equipo: Tendrá la tarea de salvar los recursos tecnológicos

A continuación, se presentan a los miembros para que puedan ayudar con la recuperación de los sistemas.

- **Comité de emergencia tecnológica**

Son los responsables de coordinar las actividades en caso de un siniestro, lo cual está conformado por:

- Coordinador de TI

- Ingeniero de infraestructura
- Ingeniero de redes y comunicaciones
- Ingeniero de aplicaciones

Los miembros de este comité deben realizar las siguientes tareas:

- Generar el inventario de activos afectados y el cuadro de evaluación de activos tecnológicos.
- Realizar un análisis de la situación actual y determinar en base al plan de contingencia en que paso se debe empezar.
- Gestionar lo más pronto posible la recuperación y puesta en marcha de los servicios tecnológicos

- **Ingeniero de infraestructura**

El ingeniero de infraestructura se encarga de los servidores y del almacenamiento dentro de la empresa.

Consta de las siguientes funciones:

- Administración de los servidores Linux y Windows
- Administración de los backup de las bases de datos y de los servidores
- Administración del sistema de almacenamiento
- Administrar la central telefónica

Realiza las siguientes tareas:

- Se procede a verificar el estado de los servidores en el cuadro de evaluación de activos.
- Revisar los servidores para determinar su estado actual, si esta todo correctamente se procede a encender los servidores.

- Verificar el estado de la central telefónica, si no presenta ningún problema se procede a encender

- **Ingeniero de redes y comunicaciones**

Se encarga de la red y de la transmisión de la información

Tiene las siguientes funciones:

- Administrar la red de área local – Switch
- Administrar los enlaces de conectividad
- Administrar el Firewall
- Administrar el Internet

Realiza las siguientes tareas:

- Revisar los switches de borde y de acceso.
- Verificar si hay red en las estaciones de trabajo.
- Comprobar que el firewall esté funcionando correctamente.
- Verificar que no tengan puertos dañados los switch, caso contrario reconfigurar o cargar el archivo de configuración.
- En caso de no tener internet verificar la fibra óptica o los equipos del proveedor.
- Reportar el incidente al proveedor de internet el cual debe restablecer el servicio lo más ante posible.

- **Ingeniero de aplicaciones**

Se encarga de las bases de datos que cuenta la empresa y de las aplicaciones

Tiene las siguientes funciones:

- Administración de las bases de datos MYSQL y SQL SERVER

- Administrar las aplicaciones: ERP, WMS y la WEB TRANSACCIONAL

Realiza las siguientes tareas:

- Restaurar las bases de datos con el ultimo backup obtenido.
- Verificar que no tengan ningún error la importación.
- Para la aplicación del ERP, realizar lo escrito en el numeral 4.3.2.3.1.
- Para la aplicación de WMS, realizar lo escrito en el numeral 4.3.2.3.1.
- Para la aplicación de la WEB TRANSACCIONAL, realizar lo escrito en el numeral 4.3.2.3.1.

4.3.2.4. Cuarta etapa: Divulgación de procedimientos

Una vez cumplido el plan de contingencia para la empresa Importadora Alvarado, se procede a realizar la divulgación y la capacitación al personal del departamento de TI sobre los procedimientos del plan de contingencia.

- **Plan de comunicación y divulgación**

Para la divulgación se va a realizar una capacitación por temarios que se muestra en la siguiente tabla:

Tabla 17

Temario Para La Divulgación Del Plan De Contingencia

Temario	Horas	Funcionarios
Conceptos básicos	2	Departamento de TI
Procesos críticos	2	Departamento de TI
Revisión de riesgos	2	Departamento de TI
Procedimientos de reanudación	3	Departamento de TI
Beneficios	2	Departamento de TI

Fuente: Elaboración propia

- **Medios de comunicación**

Para la divulgación del plan de contingencia al departamento de TI se puede realizar con diferentes recursos como:

- Charlas
- Manual de usuario con los procedimientos del plan de contingencia
- Brochures

CAPÍTULO V

CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS (OPCIONAL)

5.1 Conclusiones

- La investigación se evaluó los riesgos informáticos y se diseñó un plan de contingencia para el área de tecnología de la empresa IMPORTADORA ALVARADO VÁSCONEZ CIA. LTDA, ubicada en la ciudad de Ambato.

- Se realizó el levantamiento de información de los activos tecnológicos de la empresa, para posteriormente identificar los activos más críticos dependiendo su nivel de importancia, las amenazas a las que están expuestos y los riesgos con sus respectivas valoraciones.

- En base a los requerimientos levantados de las diferentes metodologías de gestión de riesgos se determinó la metodología MAGERIT V3.0 y la norma ISO 3100 como la óptima para la valoración de los activos en la Importadora Alvarado, el cual establecido todo el modelo tendrán medidas preventivas para poder minimizar los riesgos de mayor impacto de la empresa.

- Se elaboró un plan de contingencia de los activos más críticos para el área de TI, donde puedan obtener una guía en caso de alguna amenaza se materialice y poder actuar de manera rápida logrando reducir los tiempos de respuesta.

5.2 Recomendaciones

- Se recomienda mantener actualizado periódicamente los riesgos y las amenazas ya que pueden sufrir cambios o alterar con el pasar del tiempo, sobre todo cuando se integre un nuevo activo tecnológico a la empresa para no dejar ningún activo sin considerarlo.

- Se recomienda que el departamento de TI se relacione con la metodología MAGERIT y la ISO 31000 para un monitoreo constante de la seguridad de los activos y otras tecnologías que la empresa tenga a futuro.

- Capacitar al personal del departamento de TI en el plan de contingencia de los activos, para que se encuentren preparados en caso de presentar algún incidente y puedan reducir el tiempo de respuesta.

5.3 Bibliografía

Bernal, D. (2021). *Implementación de la gestión de riesgos TI para una empresa dental en la Ciudad de Lima –2021*. Universidad Tecnológica del Perú. https://repositorio.utp.edu.pe/handle/20.500.12867/4430

Burgos Gordón, C. A. (2020). *Plan de contingencia informático para el área de TI en base a la norma de calidad ISO 27001: 2013 para la Fundación Cultural y Educativa Ambato-Unidad Educativa Atenas*. Universidad Técnica de Ambato. Facultad de Ingenier{\'\i}a en Sistemas~….

Cabrejos Torres, R. (2020). *Influencia de la metodolog{\'\i}a Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC*.

Carmona Torres, L. D. (2021). *Implementación de una Metodolog{\'\i}a de Gestión de Riesgos alineada a la ISO 27005 y Magerit para el proceso "OSE" de una empresa de facturación electrónica en la ciudad de Lima-2021*.

Guzmán Morán, O. D. (2019). *Diseño de un modelo de sistema para la gestión de riesgos con base a la norma ISO 31000 y MAGERIT versión 3.0 en la empresa*

BlueBox. Universidad de Guayaquil Facultad de Ciencias Administrativas.

Huefle Arévalo, A. B. (2020). *Implementación de la gestión de riesgos de TI en la empresa Mapusys*.

Lopez Rimari, R. P. (2020). *Metodolog{\'\i}as para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura*.

Mayorga Guacon, G. D. (2022). *Evaluación de riesgos de la infraestructura en la empresa logban basado en la norma ISO31000.* Babahoyo: UTB-FAFI. 2022.

Ministerio de Administraciones Públicas de España. (2012). *Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Metodo*. https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Montalbán, E. A. R., Gómez, R. J. M., & Borré, D. A. F. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Aglala*, *11*(1), 227–245.

Suastegui Jaramillo, L. E. (2022). *Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19.*

5.4 Anexos

Anexo 1

Entrevista al coordinador de TI

Nombre del encuestador: _____Ciudad: _____

Lugar donde se aplica: _____

Fecha: _____

Estimado entrevistado:

El motivo de la siguiente entrevista es conocer sobre los riesgos informáticos en el departamento de TI.

Nombre de entrevistado: _____Edad: ____Genero: _____

Cargo: _____Tiempo en la función: _____

1. ¿Qué daños en los activos tecnológicos ha tenido la empresa Importadora Alvarado en los últimos años?

2. De lo mencionado ¿Cuál considera que fue el daño más perjudicial para la empresa?

3. ¿En el caso de suscitarse un desastre natural, cuenta con un registro de los principales activos tecnológicos que le permita retomar las actividades normales?

4. ¿Tienen identificados los activos tecnológicos por niveles de importancia y de criticidad?

5. ¿Cuentan con planes de contingencia en caso de que algún activo critico se dañe?

6. ¿Tienen identificados las amenazas que posee cada activo en su empresa?

7. Actualmente, ¿Cuenta con respaldos de los activos críticos?

8. En caso de sufrir un ataque informático cuentan con procedimientos para mitigar el impacto

9. ¿Cuentan con metodologías o norma ISO de gestión de riesgos?

10. ¿Qué tiempo promedio se demoraron en restaurar en una inactividad de la empresa?

Anexo 2

Procesos críticos

Activo	Área responsable	Tiempo max duración
Base de datos – Sql server – Mysql - Aurora	Todas las áreas	2 hora
Software ERP – Sistema de contabilidad empresarial	Todas las áreas	4 horas
Sistema WMS – Sistema de bodega	Bodega	4 horas
Sistema web transaccional	Ventas	4 horas
Correo electrónico	Todas las áreas	1 día
Internet	Todas las áreas	1 día
Compers - Sistema de nomina	RRHH	1 día
Firewall – Sistema perimetral	Todas las áreas	2 día

Anexo 3

Cuadro de evaluación de activos

Activo	Funciona	No funciona	Observación
Switch T1600G-28TS			
Switch TL-SF1024			
Switch SF100-16			
Switch Core-Aruba			
Switch Core SG-500			
Firewall PA-820			
Servidor de Active Directory			
Servidor de File Server			
Servidor Wms - Iav			
Servidor Base datos - Compers			
Servidor Aplicaciones - Compers			
Central Telefónica - NS1000			
Correo Office 365			
BladeSystem Onboard Administrator C3000			
Storage P2000 CA			
Storage P2000 CB			

ProLiant BL460c Gen8 ESX1	
ProLiant BL460c Gen8 ESX2	
ProLiant BL460c Gen8 ESX3	
Servicio de internet	
Servidor Aplicativo - Web transaccional	
Servidor Base de datos - Web transaccional	
Antivirus-Sophos	
Servidor Base datos Iav - GP	
Servidor Aplicaciones Iav - GP	
Servidor de Active Directory - Aws	
Servidor Postmaster - GP	