
**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL**

**CARRERA EN TECNOLOGÍAS DE LA INFORMACIÓN**

**Tema:**

# METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TI MEDIANTE LA INTEGRACIÓN DE COBIT 5 E ITIL V4 PARA EL GOBIERNO DE TI DE FERRETERÍA "SU CASA"

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información

**ÁREA:** Software.

**LÍNEA DE INVESTIGACIÓN:** Normas y estándares.

**AUTOR:** Jorge Daniel Bonilla Pacheco

**TUTOR:** Ing. PhD. Julio Enrique Balarezo López

**Ambato – Ecuador**

**agosto - 2023**

## APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TI MEDIANTE LA INTEGRACIÓN DE COBIT 5 E ITIL V4 PARA EL GOBIERNO DE TI DE FERRETERÍA "SU CASA", desarrollado bajo la modalidad Proyecto de Investigación por el señor Jorge Daniel Bonilla Pacheco, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión,de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, agosto 2023

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Enrique Balarezo López, PhD.
TUTOR

## AUTORÍA

El presente trabajo de titulación titulado: METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TI MEDIANTE LA INTEGRACIÓN DE COBIT 5 E ITIL V4 PARA EL GOBIERNO DE TI DE FERRETERÍA "SU CASA", es absolutamente original, autentico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2023

Jorge Daniel Bonilla Pacheco

C.C. 1850592658

AUTOR

## DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como documento disponible para la lectura, y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, agosto 2023

Jorge Daniel Bonilla Pacheco

C.C. 1850592658

AUTOR

## APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Jorge Daniel Bonilla Pacheco, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la modalidad Proyecto de Investigación, titulado: METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TI MEDIANTE LA INTEGRACIÓN DE COBIT 5 E ITIL V4 PARA EL GOBIERNO DE TI DE FERRETERÍA "SU CASA", nos permitimos informar que el trabajo ha sido revisado ycalificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, agosto 2023

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
JOSE VICENTE MORALES LOZADA

PhD. José Vicente Morales Lozada
PROFESOR CALIFICADOR

Firmado electrónicamente por:
VICTOR HUGO GUACHIMBOSA VILLALBA

PhD. Víctor Hugo Guachimbosa Villalba
PROFESOR CALIFICADOR

## DEDICATORIA

*Deseo dedicar este proyecto a mis queridos padres, quienes han sido mi mayor apoyo a lo largo de mi vida. Su presencia y orientación han sido fundamentales para mi desarrollo personal y académico.*

*Agradezco sinceramente a mis padres por ser mis maestros más importantes. Desde mi infancia, han sido una fuente constante de inspiración y motivación. Me han enseñado importantes lecciones de vida y me han guiado por el camino correcto.*

*Su apoyo incondicional y compromiso con mi educación han sido una parte integral de mi éxito. Siempre han estado ahí para brindarme aliento y celebrar mis logros. Sus palabras de aliento y sabiduría han sido un motor para alcanzar mis metas.*

## AGRADECIMIENTO

*A la Universidad Técnica de Ambato, la institución que me recibió hace tantos años. Agradezco sinceramente a esta universidad por brindarme la oportunidad de adquirir conocimientos y crecer académicamente.*

*A mis estimados docentes, por compartir sus conocimientos a lo largo de mi carrera universitaria. Sus enseñanzas y orientación han sido fundamentales en mi formación académica y profesional. A través de su dedicación y compromiso, me han inspirado a alcanzar mis metas y superar desafíos.*

*A mi tutor, el Ingeniero Julio Balarezo, quiero agradecerle por su valiosa guía y consejos durante el desarrollo de este proyecto. Su experiencia y conocimiento han sido de gran ayuda para llevar a cabo esta investigación. Sus aportes y sugerencias han enriquecido mi trabajo y me han impulsado a dar lo mejor de mí.*

## ÍNDICE GENERAL DE CONTENIDOS

## INDICE DE FIGURAS

## INDICE DE TABLAS

## INDICE DE ANEXOS

## RESUMEN EJECUTIVO

Las tecnologías de la información en la actualidad están presentes en empresas dedicadas a comercio o servicios, pues estas necesitan manejar de forma eficaz la información que generan con sus actividades. En un entorno de alta competitividad la información es el activo más importante de cualquier empresa, mismo que debe mantenerse seguro y disponible solo para los integrantes de la empresa.

El uso de las tecnologías de la información a nivel empresarial trae consigo beneficios como la automatización de procesos, mejora en las comunicaciones y agilitar la toma de decisiones. Sin embargo, también existen riesgos, los cuales de no ser detectados y mitigados a tiempo afectan negativamente en aspectos como la reputación, competitividad y confiabilidad de la empresa, lo que ha largo plazo representa pérdidas económicas importantes.

El presente proyecto tiene como finalidad proponer una metodología para la gestión de riesgos de TI mediante la integración COBIT 5 e ITIL v4 para el gobierno de TI de ferretería “Su Casa”, para lo que se diseñó una metodología en base a las mejores prácticas de las metodologías propuestas. El objetivo de la metodología es ofrecer una guía clara para la identificación, análisis y gestión de los riesgos de TI.



**Palabras clave:** Gestión de riesgos, metodología, COBIT 5, ITIL v4, integración, principios, gobierno de TI, prácticas de gestión de riesgos de TI.

## ABSTRACT

Information technology is currently present in companies dedicated to commerce or services, as they need to effectively handle the information generated through their activities. In a highly competitive environment, information becomes the most important asset for any company, which must be kept secure and available only to authorized personnel.

The use of information technology at the enterprise level brings benefits such as process automation, improved communications, and facilitating decision-making. However, there are also risks that, if not detected and mitigated in a timely manner, negatively affect aspects such as reputation, competitiveness, and reliability of the company, resulting in significant long-term economic losses.

The purpose of this project is to propose a methodology for managing IT risks through the integration of COBIT 5 and ITIL v4 for the IT governance of "Su Casa" hardware store. For which a methodology was designed based on the best practices of the proposed methodologies. The objective of the methodology is to provide a clear guide for the identification, analysis, and management of IT risks.



**Keywords:** Risk management, methodology, COBIT 5, ITIL v4, integration, principles, IT governance, IT risk management practices.

# CAPÍTULO I.-MARCO TEÓRICO

## 1.1 Tema de investigación

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE TI MEDIANTE LA INTEGRACIÓN DE COBIT 5 E ITIL V4 PARA EL GOBIERNO DE TI DE FERRETERÍA SU CASA.

### 1.1.1 Planteamiento del problema

Las micro y pequeñas empresas son actualmente la mayor fuente de empleos en América Latina, por lo cual la búsqueda de formas o métodos para su consolidación es un tema importante. Pese a la importancia económica, poca se investiga para encontrar factores que impiden la adopción de tecnologías de información en áreas de poco crecimiento económico. Es fundamental apuntalar el desarrollo de dichas empresas, para esto uno de los medios es la adopción de las Tecnologías de la Información (TI), su utilización permite a las organizaciones mantener información valiosa al alcance, adquirir más conocimiento, mejorar las relaciones necesarias para el negocio (clientes, proveedores), a más de aumentar la eficiencia y productividad. [1]

La transformación digital (TD) comenzó a mitad de los años noventa a raíz del nacimiento de internet. Posteriormente, a mediados de la década pasada la TD empezó a ganar notoriedad nuevamente, eventualmente se da la "ola" de la TD, impactando por ende a todo tipo de organizaciones. Empresas como la banca, telecomunicaciones y tecnologías de la información fueron las primeras en subirse a la ola de la TD, para otras empresas como la de "retail" o consumo masivo esto tomo más tiempo. Naturalmente existen empresas y organizaciones que no son nativas digitales, por lo cual es obligatorio para estas recurrir a la TD, esto con el fin de sobrevivir a la cuarta revolución industrial que lleva varios años en boga. [2]

Actualmente, en Ecuador existe un marco regulatorio y normativo reducido en cuanto a materia de informática. Debido a lo anterior, las mayores organizaciones a la hora

de recurrir o necesitar una guía relacionada estas prácticas se basan en: “The Institute of Internal Auditors” (IIA) e “Information System Audit and Control Association” (ISACA). Según la Constitución del Ecuador, el organismo designado es la Contraloría General del Estado (CGE), el cual funciona como un organismo técnico de control, con autonomía administrativa, presupuestaria y financiera, contando además con atribuciones para controlar ingresos, gastos, inversión, utilización de recursos, administración y custodia de bienes públicos. La CGE establece lineamientos relacionados a las TI y comunicación, basándose en su mayoría en estándares y practicas establecidas por organismos internacionales, siendo estas aplicables a empresas públicas y privadas con el fin de dar cumplimiento a las funciones otorgadas a la CGE. [3]

En el Ecuador no existe un marco regulatorio que abarque completamente la implementación de un gobierno de TI; para instituciones públicas, lo mandatorio es guiarse por las normas de control interno las cuales fueron publicadas en registro oficial en el año 2010. Por lo anterior, es necesario que el organismo encargado del control de los recursos públicos en los cuales se incluyen las TICs, lleve a cabo la actualización´ de las normas, a fin de alinearlas con los estándares actuales y las mejores prácticas que proponen los organismos internacionales, además de revisar e importar casos de éxitos de otros países en temas de gobierno corporativo y de TI, lo que implica una constante revisión y actualización de las mejores prácticas dentro de las normas emitidas por la CGE. Por otro lado, las organizaciones de capital privado se acogen a firmas auditoras externas, las cuales en su gran mayoría aportan conocimientos sobre los estándares actuales y las mejores prácticas.[4]

En ferretería “Su Casa”, que en adelante se denominara como la empresa, se evidencia el poco o nulo interés en el tema de las TI, pues sus procesos los llevan a cabo con ayuda de un sistema básico. Un aspecto importante a tener en cuenta es el tamaño de la empresa, pues esta es pequeña, con pocos empleados, lo que en consecuencia deriva en la poca atención al área de TI, incumplimiento con la ley y sobre todo riesgos para el negocio en general, no solo para el departamento de TI, la situación de la empresa es un patrón que se repite con frecuencia en la ciudad de Ambato, debido a que la

mayoría de las empresas encajan con el perfil expuesto, teniendo ligeras variantes en cuanto al rubro del negocio.

### 1.2 Antecedentes investigativos

Tras la revisión de múltiples fuentes bibliográficas de universidades del Ecuador y de Latinoamérica, se encontraron trabajos para apoyar el presente trabajo de investigación:

Según Jorge Luis Tigse Moposita[5]:

La implementación de un Plan de Gestión Informática basado en la Norma ISO 27001, permitió mejorar la seguridad de información combinando los procesos de negocio con la tecnología, considerando las ventajas que tiene esta norma, la cual se puede adaptar a la empresa al ser una entidad que maneja grandes cantidades de información de todas sus plantas.

Según Esteban Crespo Martínez [6]:

Para proponer una metodología de gestión de riesgos se analizaron comparativamente varias metodologías de amplia divulgación, como: Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III. Estas metodologías son internacionalmente utilizadas en la gestión del riesgo de información. ECU@Risk propone procesos para el inventario de activos de información, considerando como categorías principales i) edificaciones o instalaciones, ii) el hardware, iii) el software, iv) la información electrónica, v) la información en papel, vi) la infraestructura de comunicaciones, vii) los medios de almacenamiento extraíbles y viii) los recursos humanos; elementos con que toda organización del sector MPYME cuenta.

Jean Carlo Alfaro Campos [7]:

El marco de referencia COBIT 5 contempla prácticas de gobierno y gestión de tecnología de información que abarcan a las organizaciones de extremo a extremo, reconociendo las responsabilidades de la gestión de TI a todos los involucrados del negocio; y su enfoque permite la gestión de riesgos con responsabilidad más allá de

los gestores de TI. COBIT 5 para riesgos, es una guía adecuada para la creación de una metodología de gestión de riesgos, esta guía considera el uso de principios y mecanismos definidos por COBIT 5, para garantizar los aspectos necesarios de una adecuada gestión de riesgos de TI.

Ramiro Quezada Sarmiento, Jonathan Aguilar Alvarado, Karina García Galarza, Rodrigo Morocho Roman y Wilmer Rivas Asanza [8]:

Hay cuatro objetivos que impulsan el Gobierno de TI: el valor de TI y la alineación, la rendición de cuentas, la medición del desempeño y la gestión del riesgo. Cada uno de estos objetivos deben abordarse como parte del proceso de Gobierno de TI. La gestión de riesgos de TI es de suma importancia. Los riesgos de TI incluyen los riesgos de seguridad derivados de los hackers y ataques de denegación de servicio, riesgos de privacidad derivados de robos de identidad, la recuperación de desastres, de resiliencia de los sistemas de cortes, y los riesgos asociados con las fallas del proyecto.

Darwin Pillo Guanoluisa y Robert Enríquez Reyes [9]:

El marco referencial COBIT 5 es robusto, flexible e integrador, y permite a las organizaciones alinear sus objetivos estratégicos con TI apoyando el uso adecuado de recursos, disminución de costos y riesgos, con un modelo integral que cubre de extremo a extremo a las organizaciones. Además, tiene varios principios, prácticas, herramientas y modelos de análisis que permiten abordar aspectos críticos; por lo que constituyó una base sólida para el diseño del modelo de Gobierno de TI para Hospitales Públicos, con énfasis en la Seguridad de la Información.

### 1.3 Fundamentación teórica

#### COBIT 5

COBIT 5 proporciona un enfoque integral que ayuda a las empresas a lograr sus objetivos en el gobierno y gestión de tecnologías de la información. En términos simples, COBIT 5 ayuda a las empresas a obtener el máximo valor de sus inversiones en tecnología al equilibrar beneficios, riesgos y recursos. Este enfoque abarca toda la organización, desde el principio hasta el final, y considera tanto las responsabilidades

funcionales de TI como las preocupaciones de las partes interesadas internas y externas. COBIT 5 es adaptable y útil para organizaciones de diversos tamaños y ámbitos, ya sean comerciales, sin fines de lucro o del sector público.

COBIT 5 se basa en cinco principios claves (mostrados en la Figura 2.) para el gobierno y la gestión de las TI empresariales:

**Principio 1.**

Satisfacer las Necesidades de las Partes Interesadas—Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

**Principio 2.**

Cubrir la Empresa Extremo-a-Extremo—COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

**Principio 3.**

Aplicar un Marco de Referencia único integrado—Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

**Principio 4.**

Hacer Posible un Enfoque Holístico—Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

- Principios, Políticas y Marcos de Trabajo
- Procesos
- Estructuras Organizativas
- Cultura, Ética y Comportamiento
- Información
- Servicios, Infraestructuras y Aplicaciones
- Personas, Habilidades y Competencias

**Principio 5.**

Separar el Gobierno de la Gestión—— El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

- **Gobierno**

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

- **Gestión**

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO). Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas [10]

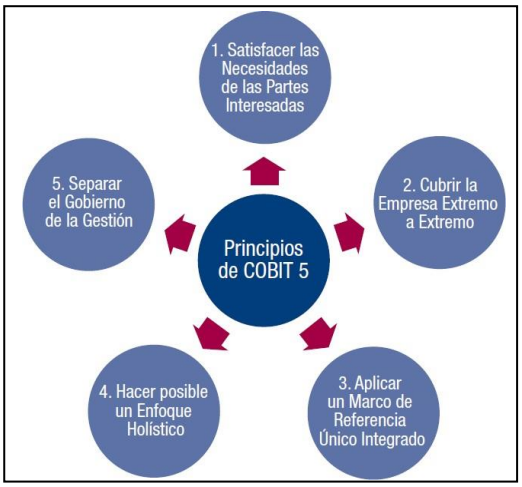


Figura 1: Principios de COBIT 5

**ITIL v4**

Information Technology Infraestructure Library, es una guía de 30 mejores prácticas para la gestión de servicios de TI, que permite proporcionar a las organizaciones un marco de orientación para emplear el potencial del avance tecnológico y para adecuarse a los nuevos retos de la gestión de servicios. Este marco de mejores prácticas permite diseñar un sistema coordinado, flexible e integrado para el gobierno y la gestión efectiva de los servicios referidos a tecnologías de la información de la organización. [10]

ITIL 4 proporciona un modelo operativo digital de extremo a extremo en la organización para la entrega y operación de productos y servicios habilitados por TI y permite que los equipos de TI continúen desempeñando un papel importante en la estrategia comercial del negocio. ITIL 4 también proporciona un enfoque integral de extremo a extremo que integra marcos como Lean, Agile y DevOps. [11]

- **Estructura y beneficios de ITIL 4:**

Los componentes clave del marco ITIL 4 son el Sistema de Valor del Servicio (SVS) y el Modelo de cuatro dimensiones. El SVS representa cómo los diversos componentes y actividades de la organización trabajan juntos para facilitar la creación de valor mediante servicios habilitados por TI. El SVS facilita la integración y coordinación y proporciona una dirección fuerte, unificada y enfocada en el valor, para la organización.

Para garantizar un enfoque holístico en la gestión de servicios, ITIL 4 define cuatro dimensiones de la gestión de servicios:

- Organizaciones y personas
- Información y tecnología
- Asociados y proveedores

- Flujos de valor y procesos [11]

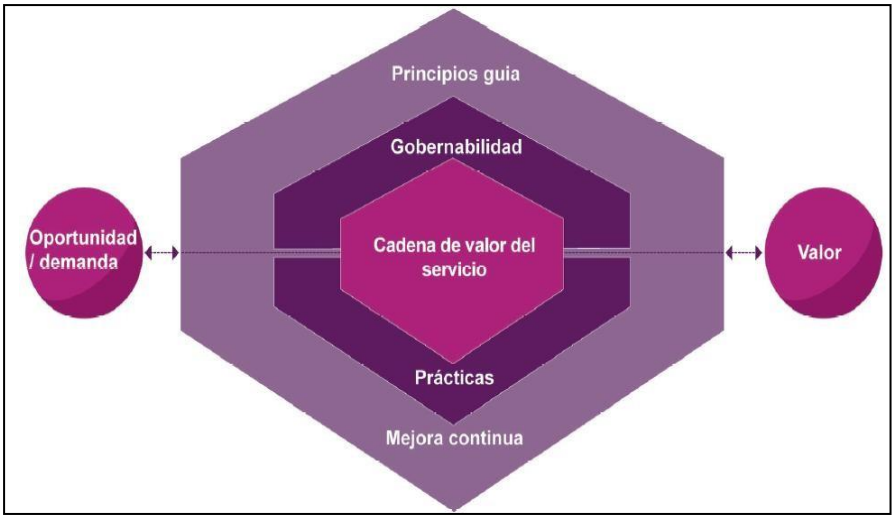



Figura 2: Estructura del Sistema de Valor del servicio (SVS)

**Riesgos de TI**

El Riesgo de TI (Risk TI) es el riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de la TI dentro de la empresa. Este riesgo consiste en los eventos relacionados con la TI que pueden potencialmente impactar al negocio. Cada evento puede ser visto como riesgo y oportunidad. [12]

Según Capterra.mx el riesgo de TI es la posible amenaza que supone un fallo o un mal uso, intencionado o no, de la estructura y equipos de TI de la empresa. Este riesgo puede provenir de hackers, ataques de phishing o incluso de robos de datos que pueden llevar a cabo los propios empleados. [13]

**Operaciones de TI**

Valuit Solutions [14] define las Operaciones de TI como una disciplina que busca integrar eficientemente tres factores: personas, procesos y tecnología, con el propósito de que estos estén alineados con los objetivos de negocio de la compañía.

Según Servicenow [15]las Operaciones de TI o ITOps pueden incluir todo, desde las operaciones de red hasta la supervisión de los componentes virtuales y físicos del entorno de TI de una empresa.

**Gestión de TI**

La gestión de TI según el IBM [16], se refiere al seguimiento y la administración de los sistemas de tecnología de la información de una organización: hardware, software y redes. La gestión de TI se centra en cómo hacer que los sistemas de información funcionen de manera eficiente.

En el sitio web de Redhat [17]se define la gestión de la TI como la coordinación de todos los recursos, los sistemas, las plataformas, las personas y los entornos de TI.

**Gobiernos de TI**

El Gobierno de TI es definido por (IT Governance Institute) como una parte integral del gobierno corporativo y consiste en el liderazgo de las estructuras y procesos organizativos que aseguran que las TI de la organización sostengan y extiendan la estrategia y los objetivos de la organización.

Weill define al Gobierno de TI como "La especificación del marco sobre los derechos y responsabilidades de decisión para alentar el comportamiento deseable del uso de las TI". [4]

La norma ISO/IEC 38500:2008 Corporate Governance of Information Technology (ISO/IEC, 2008) define el gobierno de las TI como "el sistema por el que se dirige y controla la utilización actual y futura de la tecnología de la información".

**Metodología para la gestión de riesgos de TI**

Una metodología para la gestión de riesgos de TI define los pasos a seguir para gestionar los riesgos de tecnología de información, de manera que se facilite la toma de decisiones oportuna ante eventos que limiten o afecten los objetivos de TI y que puedan impactar el logro de los objetivos del negocio. [7]

**Activos de TI**

El concepto base de ITIL v4 sobre activos de TI se refiere a cualquier componente valioso que puede contribuir a la entrega de un producto o servicio de TI, la gestión de los mismos es planificar y administrar el ciclo de vida de todos los activos de TI. Esto

a su vez ayuda a la organización a:

- Maximizar el valor para los clientes
- Controlar costos y presupuestos
- Hacer frente a los riesgos
- Tomar decisiones en términos de compra y reutilización
- Cumplir con los requisitos vigentes y prometidos

**Roles del personal de TI**

El concepto de rol según ITIL es un conjunto de actividades y responsabilidades asignada a una persona o un grupo. Una persona o grupo puede desempeñar simultáneamente más de un rol. Existen cuatro roles genéricos:
Gestor del Servicio: es el responsable de la gestión de un servicio durante todo su ciclo de vida: desarrollo, implementación, mantenimiento, monitorización y evaluación.
Propietario del Servicio: es el último responsable, tanto de cara al cliente, como de cara a la organización de TI que presta el servicio específico.
Gestor del Proceso: es el responsable de la gestión de toda la operativa asociada a un proceso en particular.
Propietario del Proceso: es el último responsable frente a la organización TI de que el proceso cumple sus objetivos. Debe estar involucrado en su fase de diseño, implementación y cambio, asegurando en todo momento que se dispone de las métricas necesarias para su correcta monitorización, evaluación y eventual mejora. [18]

**Contexto de la organización**

Según la norma ISO 9000 el contexto de la organización se define como combinación de cuestiones internas y externas que pueden tener un efecto en el enfoque de la organización para el desarrollo y logro de sus objetivos. [19]

El contexto de la organización puede definirse como el medio en que se desenvuelve la empresa tanto a nivel interno de la misma como en su entorno, dicho medio afecta positiva o negativamente los productos, servicios, metas y en general, el desarrollo de las actividades de la organización.[20]

## Gestión de seguridad de la información

El propósito de la práctica de gestión de la seguridad de la información es proteger la información que necesita la organización para llevar a cabo su negocio. Esto incluye comprender y gestionar los riesgos para la confidencialidad, la integridad y la disponibilidad de la información, así como otros aspectos de la seguridad de la información, como la autenticación (asegurarse de que alguien sea quien dice ser) y el no repudio (asegurarse de que alguien no pueda negar que tomo una acción).[21]

## ISO-31000.2018

Titulada como "Gestión del riesgo: Directrices", es una norma internacional desarrollada por la Organización Internacional de Normalización (ISO), la cual establece marcos, principios y procesos para la gestión de riesgos en organizaciones, su objetivo es proporcionar un enfoque sistemático y estructurado para identificar, evaluar y tratar riesgos.

Esta norma es aplicable en cualquier tipo de organización, se utiliza para la gestión en una amplia gama de áreas, como seguridad, finanzas, salud, etc. [22]

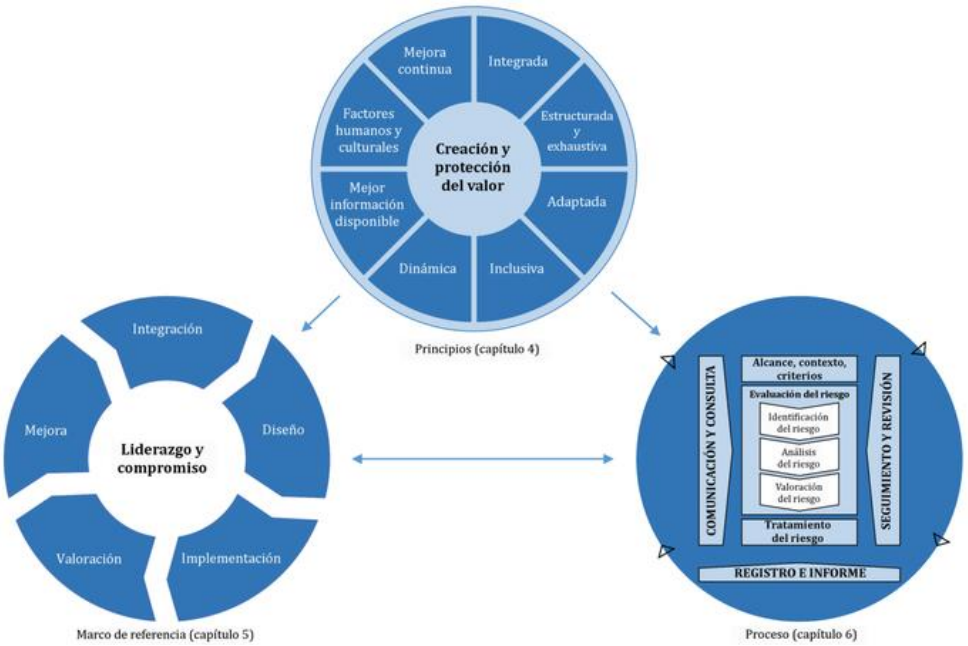



Figura 3: Principios, marco de referencia y proceso

## 1.4 Objetivos

### 1.4.1 Objetivo general

Diseñar una metodología para la gestión de riesgos de TI mediante la integración de COBIT 5 e ITIL v4 para el Gobierno de TI de ferretería “Su casa”

### 1.4.2 Objetivos específicos

- Evaluar los procesos relacionados a gestión de riesgos que se llevan a cabo en la empresa y su impacto en el Gobierno de TI, aplicando las metodologías COBIT 5 e ITIL v4.
- Integrar la metodología para la gestión de riesgos de TI mediante COBIT 5 e ITIL v4 para el Gobierno de TI de ferretería “Su casa”, con base en los resultados de la evaluación de los procesos.
- Proponer un plan de gestión de riesgos de TI utilizando la metodología integrada COBIT 5 e ITIL v4 para el Gobierno de TI de ferretería “Su casa”

# CAPITULO II.- METODOLOGÍA

## 2.1 Materiales

Dada la naturaleza de la investigación para la recolección de datos se aplicó entrevistas a miembros clave y una ficha de observación en busca de información relacionada al funcionamiento de las TI en la empresa. Para el apartado documental se realizaron fichas bibliográficas para resumir los aspectos más importantes de las metodologías propuestas.

## 2.2 Métodos

### 2.2.1 Modalidad de la Investigación

- **Investigación de campo**

Se aplico esta modalidad debido a que la empresa como objeto de estudio funcionó como fuente de la información base que permita encaminar la investigación.

- **Investigación bibliográfica – documental**

Se aplico la modalidad bibliográfica – documental debido a la necesidad de recurrir a múltiples fuentes de información bibliográfica y empresarial para desarrollar la solución propuesta.

### 2.2.2 Población y muestra

La población que formo parte de la investigación, es el personal de ventas y despacho, el personal de contabilidad y el gerente de la empresa.

| Población | Número | Porcentaje |
|---|---|---|
| Gerente | 1 | 9.09% |
| Personal de contabilidad | 4 | 36.36% |
| Personal de ventas y despacho | 6 | 54.55% |
| Total | 11 | 100.00% |

Tabla 1:Población y muestra

Elaborado por: Jorge Bonilla

La población no supera las 100 personas, por lo que fue necesario obtener muestras representativas y por ende se trabajó con toda la población.

### 2.2.3. Recolección de la información

Las guías de entrevista de los anexos 4.1, 4.2 muestran información sobre la infraestructura de TI de la empresa, como es utilizada para las actividades de la empresa y los roles del personal, la guía de entrevista del anexo 4.3 expone los aspectos más importantes sobre el sistema de facturación utilizado en la empresa. La ficha de observación presentada en el anexo 4.4 complementa la información relacionada a la infraestructura de TI y su uso, además de mostrar a breves rasgos como gestionan el inventario ofimático.

Los anexos 4.5 al 4.18 resumen información relacionada a la gestión de riesgos de TI tanto de ITIL v4 como en COBIT 5, exponen los aspectos y prácticas más relevantes.

### 2.2.4. Procesamiento y análisis de datos

- Una vez recolectada la información sobre el estado de la empresa y las metodologías propuestas, se determina que:
- La empresa no cuenta con políticas para la gestión de TI y sus riesgos.
- El conocimiento con el que cuenta la empresa sobre la gestión de riesgos de TI es prácticamente nulo.
- Al observar las actividades de la empresa se evidencia que el personal de la empresa está conformado en su totalidad por usuarios comunes.
- La gestión de TI en la empresa es deficiente, esto debido a la falta de conocimientos sobre la importancia de la seguridad de sus activos de TI.
- Existen múltiples brechas de seguridad en el sistema informático de la empresa, las cuales son causadas por el poco conocimiento de los integrantes y la poca inversión en el área de TI.
- La empresa no cuenta con procesos ni servicios documentados formalmente.
- Uno de los mayores problemas de la empresa es la dependencia completa de personal externo para afrontar inconvenientes relacionados a las TI.
- De acuerdo a las metodologías seleccionadas la gestión de riesgos de TI tiene como objetivo principal aprovechar las oportunidades y crear valor para las

partes involucradas.

- El origen de los riesgos de TI en ambas metodologías está ligado a la existencia de activos de TI y su uso para el negocio con el fin de crear valor.
- La seguridad de la información es un punto clave para ambas metodologías, debido a que se trata del activo más importante para la organización.
- A pesar de los enfoques diferentes de las metodologías, estas se complementan, ya que ITIL v4 se orienta a servicios y COBIT 5 se orienta a procesos, siendo estos últimos partes integral de los servicios.
- Los miembros de la organización son un punto clave para ambas metodologías, puesto que dejan en claro la necesidad de definir los roles necesarios para la gestión de TI, haciendo énfasis en la directiva o ejecutivo de la empresa como los miembros clave para una adecuada gestión de riesgos de TI.
- Para ambas metodologías la creación de valor consiste en la entrega de productos que generen beneficios a la organización.
- Ambas metodologías facilitan la mejora continua, debido a que ayudan a la organización a adoptar prácticas que permitan a la misma adaptarse a los cambios constantes del entorno comercial.

# CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

## 3.1 Análisis y discusión

Luego de la recolección de la información necesaria se procedió a integrar las metodologías, identificar los procesos críticos de la empresa e identificar, evaluar y analizar los riesgos relacionados.

### 3.1.1 Comparación de metodologías

| **Principio** | **ITIL v4** | **COBIT 5** |
|---|---|---|
| **Enfoque de la gestión de riesgos de TI** | • Se enfoca en garantizar la calidad de los servicios de TI.<br>• Este enfoque puede variar en función del paradigma de transformación de la empresa.<br>• La creación de valor está orientada a los clientes | • El enfoque está dirigido a lograr los objetivos empresariales y a la creación de valor para el negocio<br>• Busca la mejora de los resultados del negocio, la toma de decisiones y la estrategia global. |
| **Cobertura de la gestión de riesgos de TI** | • Cubre cada fase del ciclo de vida del servicio.<br>• Asegura el éxito de la organización en un medio con reglas cambiantes | • Cubre la gestión de riesgos de TI en todo el espectro de la gestión de TI.<br>• Cubre y gestiona todos las funciones y procesos necesario para gobernar y gestionar la información corporativa. |
| **Procesos y prácticas** | • Se orientan al análisis, gestión y monitoreo de riesgos resultantes de la implementación de servicios. | • Los procesos y practicas están orientados a la evaluación, gestión, monitoreo y análisis de riesgos ligados a los activos de TI.<br>• Se enfocan en el dominio de "Gestión de seguridad" |
| **Integración con otros procesos y prácticas.** | • Se lleva a cabo mediante la integración de gestión de riesgos en cada aspecto del ciclo de vida del servicio. | • Se realiza a través de la definición de objetivos y métricas alineados a los objetivos empresariales.<br>• Se integra además con otros |

| | | |
|---|---|---|
| | | marcos de gobierno y prácticas de seguridad y complimiento. |
| **Mejora continua** | • Se logra a través de la aplicación de ciclo de mejora continua de servicio. | • Se ejecuta mediante el ciclo de vida del gobierno y gestión de TI, esto incluye la definición de objetivos y métricas, evaluación de desempeño, identificación de áreas de mejora e implementación de mejoras en los procesos y prácticas de gestión de TI |
| **Enfoque de gobierno de TI** | • No cuenta con un enfoque explícito de gobierno de TI | • El gobierno de TI es un elemento clave para la gestión de riesgos de TI. |
| **Implementación de la gestión de riesgos de TI** | • Se enfoca en proteger los activos dentro de una organización.<br>• Se centra en la entrega de prototipos o productos y servicios mínimos viables. | • Se enfoca en el gobierno y gestión de TI de toda la organización.<br>• Abarca todo el espectro de TI de la organización. |
| **Conclusiones:** Existen múltiples diferencias entre ambas metodologías, pues ITIL v4 proporciona lineamientos generales sobre el ciclo de vida de los servicios de TI y como la gestión de riesgos de TI impacta en cada fase del mismo, mientras que COBIT 5 se enfoca a prácticas y procesos detallados, los cuales están orientados a todo el espectro de TI de la organización, representando una guía práctica para llevar a cabo la gestión de riesgos de TI.<br>En resumen, ITIL v4 presenta una guía de que hacer para gestionar riesgos de TI, mientras que COBIT 5 muestra el cómo hacerlo, la combinación de ambos modelos permite alcanzar las metas empresariales de mejor forma. | | |

Tabla 2: Comparación de metodologías

Elaborado por: Jorge Bonilla

### 3.1.2 Similitudes entre metodologías

| **Principio** | **ITIL v4** | **COBIT 5** |
|---|---|---|
| **Marco de referencia de gestión de riesgos** | Garantiza la continuidad del negocio y la creación de valor para sus clientes.<br>Cuenta con prácticas para la gestión de riesgos de TI dentro del ciclo de vida del servicio<br>Adopta principios de otras metodologías. | Ayuda a la empresa con la creación de valor<br>Cuenta con prácticas y catalizadores (procesos) para la gestión de riesgos de TI que cubren todo el espectro de la gestión de TI.<br>Se alinea con otros estándares y buenas prácticas de TI |

| | | |
|---|---|---|
| **Enfoque de la gestión de riesgos de TI** | El enfoque se resume a identificar, evaluar y gestionar los riesgos de TI que representen un posible impacto para la calidad de los servicios.<br>Busca que los beneficios potenciales valgan más para la empresa que el costo de abordar el riesgo. | Ayuda a la empresa alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas.<br>Mantiene el equilibrio entre la generación de beneficios y la optimización de niveles de riesgo<br>Permite a las TI ser gobernadas y gestionadas de modo holístico |
| **Gestión de riesgos de TI** | La gestión consiste en recursos organizaciones diseñados para llevar a cabo un trabajo o lograr un objetivo.<br>Se incluye la gestión de riesgos de TI en cada etapa del ciclo de vida del servicio. | Proporciona a la empresa una forma para solucionar la complejidad y desafíos que se originan durante las implementaciones<br>Incluye la gestión de riesgos en cada fase del ciclo de vida de la gestión de TI. |
| **Procesos y prácticas** | Incluye prácticas de gestión de riesgos de TI en procesos como la gestión de cambio, gestión de incidentes y gestión de problemas. | Dentro de los procesos de gestión de riesgos de TI se incluyen prácticas como la gestión y monitoreo de riesgos. |
| **Integración con otros procesos y prácticas.** | Se integra fácilmente con prácticas como la gestión del cambio y la gestión de problemas. | La gestión de riesgos forma parte de procesos como la gestión de la seguridad de la información y gestión de la continuidad del negocio. |
| **Mejora continua** | Uno de los objetivos es la mejora continua de los servicios. | La mejora continua se lleva a cabo mediante el monitoreo y evaluación constante de los riesgos, así como la implementación de medidas de mitigación y mejora. |
| **Implementación de la gestión de riesgos de TI** | Propone un proceso de gestión de riesgos de TI que abarca la identificación de riesgos, evaluación de riesgos, selección e implementación de controles, revisión y mejora continua | Propone procesos de gestión de riesgos en toda la organización, incluye la definición de políticas y procedimientos, además de roles y responsabilidades. |

| |
|---|
| **Conclusiones:** ITIL v4 y COBIT 5 reconocen la importancia de la gestión de riesgos de TI como elemento crucial para lograr los objetivos de la empresa mediante la implementación de procesos y servicios de TI así como la mejora continua de los mismos, además de proporcionar un enfoque claro para identificar y evaluar los riesgos de TI, manteniendo el equilibrio entre el beneficio potencial y el costo de asumir riesgos, también comparten practicas orientadas a la integración con otros procesos de gestión de TI. |

Tabla 3: Similitudes entre metodologías

Elaborado por: Jorge Bonilla

### 3.1.3 Integración de principios

| **Principio** | **Metodologías** | |
|---|---|---|
| **Establecer el contexto** | **ITIL v4** | **COBIT 5** |
| Identificar y comprometerse con las partes interesadas de la empresa, documentar la comprensión de los requerimientos, realizar la estimación del actual y futuro diseño del gobierno de TI de la empresa. | No | Si |
| **Actividades** | | |
| 1. Análisis e identificación de factores internos y externos del entorno, tendencias de negocio con potencial para influir en la gestión de riesgos de TI. | | |
| 2. Definir la relevancia de TI y su rol en relación al negocio. | | |
| 3. Considerar regulaciones externas, obligaciones legales y contractuales, determinar cómo aplicarlas en la gestión de riesgos de TI. | | |
| 4. Alinear uso y procesamiento ético de la información y su impacto en las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa. | | |
| 5. Establecer los principios guía para la toma de decisiones sobre riesgos de TI. | | |
| 6. Analizar la cultura empresarial para toma de decisiones de TI. | | |
| 7. Establecer niveles para delegación de autoridad, incluyendo reglas de umbrales, para las decisiones de TI. | | |
| **Principio** | **Metodologías** | |
| **Identificación de riesgos** | **ITIL v4** | **COBIT 5** |
| Identificar y recopilar datos relevantes sobre los riesgos potenciales, esto incluye probabilidad y gravedad de los mismos | Si | Si |
| **Actividades** | | |
| 1. Establecer un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, este puede incluir la frecuencia esperada e impacto potencial. | | |
| 2. Registrar datos relevantes del entorno de operación interno y externo de la empresa que puedan influir en la gestión del riesgo de TI. | | |
| 3. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI. | | |

| | | |
|---|---|---|
| 4. Determinar las causas de los eventos de riesgo y su impacto en la frecuencia del evento y la magnitud de perdida. | | |
| **Principio** | **Metodologías** | |
| **Evaluación de riesgos:** | **ITIL v4** | **COBIT 5** |
| Determinar la tolerancia al riesgo de la organización y establecer criterios para la aceptación o el rechazo de los riesgos. | Si | Si |
| **Actividades** | | |
| 1. Determinar y documentar la capacidad de riesgo y el apetito de riesgo que la empresa está dispuesta a asumir para cumplir sus objetivos. | | |
| 2. Determinar los servicios TI y recursos de infraestructuras de necesarios para los procesos de negocio. Identificar vulnerabilidades. | | |
| 3. Evaluar factores de riesgo TI previo a la toma de decisiones estratégicas pendientes. | | |
| 4. Analizar costo-beneficio de las actividades ante riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar | | |
| **Principio** | **Metodologías** | |
| **Análisis de riesgos:** | **ITIL v4** | **COBIT 5** |
| Proceso de comprender la naturaleza del riesgo y determinar el impacto del mismo. | No | Si |
| **Actividades** | | |
| 1. Considerar todos los factores de riesgo y su impacto en el negocio. Definir el alcance del análisis de riesgos basado en el análisis costo-beneficio. | | |
| 2. Plantear escenarios de riesgo de TI, que incluyan escenarios compuestos o amenazas coincidentes | | |
| 3. Determinar la frecuencia y magnitud de pérdida o ganancia bajo escenarios de riesgos de TI. | | |
| **Principio** | **Metodologías** | |
| **Planificación de la gestión de riesgos:** | **ITIL v4** | **COBIT 5** |
| Consiste en las políticas, planes, procesos y herramientas utilizados para preparase y reducir el impacto del riesgo en la empresa | Si | Si |
| **Actividades** | | |
| 1. Definir un inventario de actividades de control que se alineen con el apetito y tolerancia de riesgo. | | |
| 2. Determinar si cada unidad organizativa supervisa el riesgo dentro de sus niveles de tolerancia individuales. | | |
| 3. Generar propuestas para reducir el riesgo, o proyectos que den paso a oportunidades estratégicas empresariales, considerando costo/beneficio y su impacto en el perfil de riesgo actual. | | |
| 4. Generar planes con pasos específicos a seguir cuando un evento de riesgo cause un incidente significativo a nivel operativo. | | |

| | | |
|---|---|---|
| 5. Clasificar los incidentes en base a exposiciones reales y a la capacidad de riesgo. Comunicar los impactos en el negocio a los responsables de actualizar el perfil de riesgo. | | |
| 6. Aplicar plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo. | | |
| **Principio** | **Metodologías** | |
| **Comunicación y consulta:** | **ITIL v4** | **COBIT 5** |
| Trabajar con las partes interesadas y coordinar de extremo a extremo la entrega de servicios TI y soluciones proporcionadas al negocio. | Si | Si |
| **Actividades** | | |
| 1. Comunicar cambios y actividades de transición, los cuales incluyen proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación. | | |
| 2. Recopilar información relacionada a cambios e incidentes TI y comunicarla a las partes interesadas. La comunicación puede ser por medio de informes o reuniones periódicas. | | |
| 3. Coordinar y comunicar actividades operativas, roles y responsabilidades al personal correspondiente. | | |
| 4. Generar un plan de comunicación que defina contenido, frecuencia y destinatarios de la información relacionada a los servicios, incluyendo el estado del valor entregado y los riesgos identificados. | | |
| **Principio** | **Metodologías** | |
| **Monitoreo y revisión:** | **ITIL v4** | **COBIT 5** |
| Conjunto de procesos clave cuya finalidad es supervisar y evaluar el desempeño de los procesos de TI, identificar desviaciones, tomar acciones correctivas y garantizar el cumplimiento de los objetivos establecidos. | No | Si |
| **Actividades** | | |
| 1. Definir los objetivos y criterios de monitoreo y revisión, esto incluye el rendimiento de los procesos de TI, cumplimiento de controle, entre otros. | | |
| 2. Recopilar datos relevantes para evaluar el desempeño de los procesos de TI, esto puede incluir métricas, KPIs, entre otros | | |
| 3. Analizar los datos recopilados en busca de patrones, tendencia, posibles desviaciones y áreas de mejora. | | |
| 4. Evaluar la efectividad de los controles implementados en los procesos de TI, asegurando su funcionamiento adecuado para mitigar riesgos. | | |
| 5. Establecer un cronograma de revisiones periódicas. | | |
| 6. Tomar acciones correctivas y preventivas ante posibles desviaciones o deficiencias, esto puede implicar mejoras en los procesos. | | |
| 7. Comunicar los resultados del monitoreo y revisión a las partes interesadas. | | |

Tabla 4: Integración de principios

Elaborado por: Jorge Bonilla

### 3.1.4 Diagramas de procesos

**Proceso de adquisición:**

**Descripción:**

La adquisición de mercadería es el uno de los pilares de la actividad comercial de la empresa, los productos se adquieren de múltiples distribuidoras y el método de contacto con las mismas puede variar entre llamadas, correos electrónicos o con intermediarios como agentes de ventas. Luego de la solicitud y recepción de la mercadería, esta es ingresada al inventario de la empresa, para lo cual es necesaria una revisión previa de las unidades solicitadas y el estado de las mismas, cumplido este paso ingresan a bodega y al sistema.

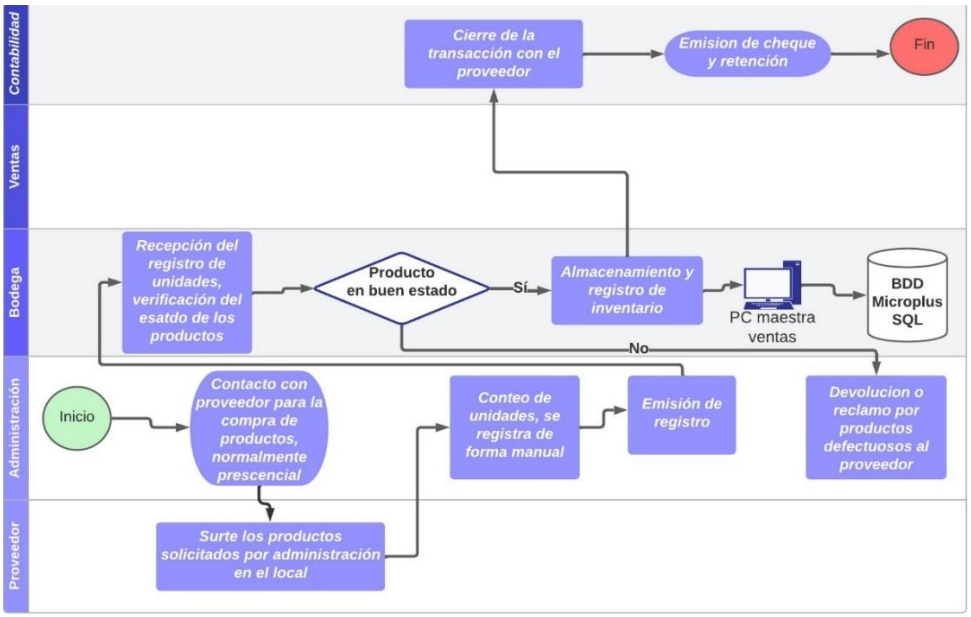



Figura 4: Proceso de adquisición

Elaborado por: Jorge Bonilla

**Identificación de activos de TI en este proceso:**

- Pc maestro ventas
- Servidor sistema de facturación

- BD sistema de facturación.
- Modem
- Switch
- Cables de red

**Proceso de ventas**

**Descripción:**

La actividad principal de la empresa y razón de su existencia, el personal encargado de las ventas interactúa constantemente con los clientes y las terminales designadas para dicha actividad, todo el proceso se lleva a cabo de forma personalizada y todos los datos generados se almacenan directamente en el servidor.

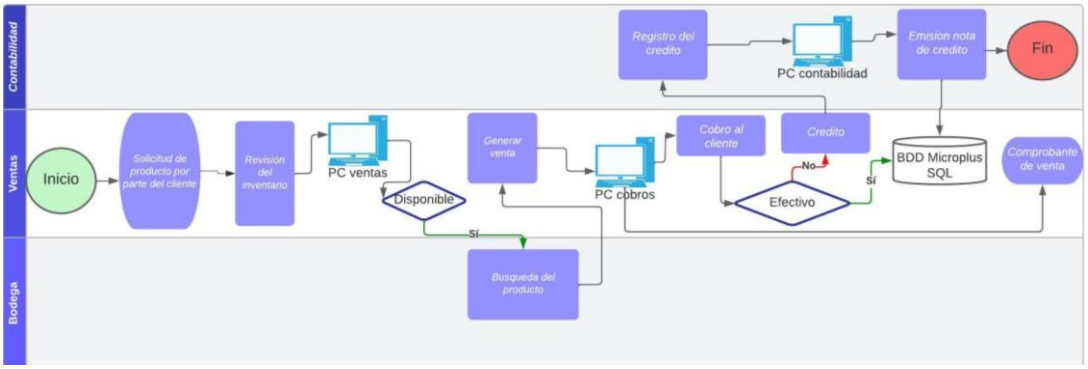



Figura 5: Proceso de ventas

Elaborado por: Jorge Bonilla

**Identificación de activos de TI en este proceso:**

- PCs ventas
- PC cobros
- PC contabilidad
- Servidor sistema de facturación
- BD sistema de facturación.
- Modem

- Switch
- Cables de red

**Proceso de facturación.**

**Descripción:**

La generación de facturas es el resultado de toda actividad comercial, la empresa cuenta con un departamento contable que se encarga de dar seguimiento a las transacciones, esto con ayuda del inventario ofimático designado para dicha labor.

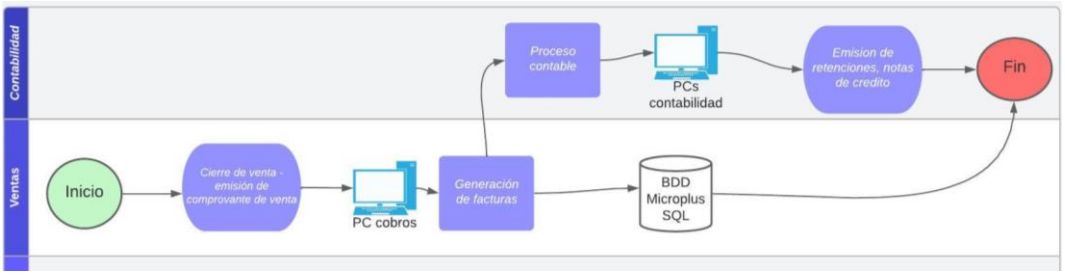



Figura 6: Proceso de facturación

Elaborado por: Jorge Bonilla

**Identificación de activos de TI en este proceso:**

- PC cobros
- PC contabilidad
- Servidor sistema de facturación
- BD sistema de facturación.
- Modem
- Switch
- Cables de red

**Proceso de transacciones**

**Descripción:**

Actividad desarrollada por el personal del departamento contable, se encargan de verificar las transacciones y llevar las cuentas de la empresa, incluyendo actividad bancaria y deberes tributarios.


Figura 7: Proceso de transacciones

Elaborado por: Jorge Bonilla

**Identificación de activos de TI en este proceso:**

- PC contabilidad
- Servidor sistema de facturación
- BD sistema de facturación.
- Modem
- Switch
- Cables de red

**Proceso de reembolso**

**Descripción:**

Actividad que se lleva a cabo bajo solicitud de los clientes, los cuales deben contar con una factura con datos, mismos que se utilizan para verificar la compra en el sistema y una vez comprobada la validez se emite una nota de crédito por la diferencia.

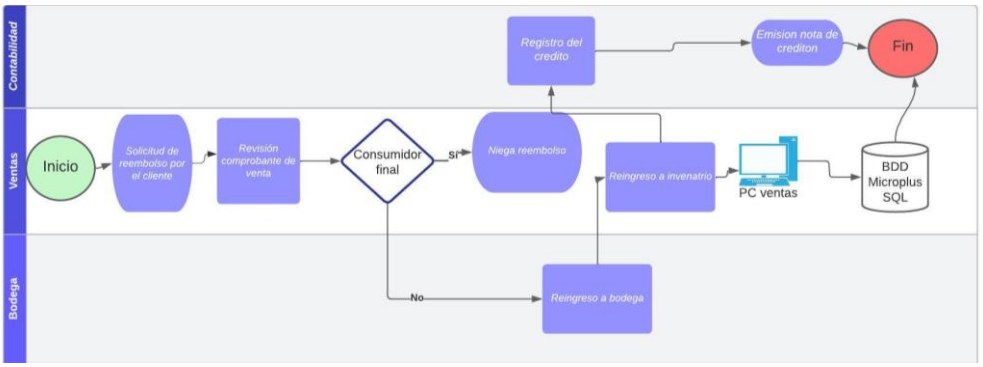



Figura 8: Proceso de reembolso

Elaborado por: Jorge Bonilla

**Identificación de activos de TI en este proceso:**

- PCs ventas
- Servidor sistema de facturación
- BD sistema de facturación.

- Modem
- Switch
- Cables de red

**Proceso de seguridad.**

**Descripción:**

Salvaguardar la integridad de la empresa y sus bienes es una actividad fundamental, el sistema de seguridad de la empresa consta de 17 cámaras IP activas las 24 horas del día, las grabaciones se almacenan en un CPU independiente el cual cuenta con capacidad para almacenar 3 semanas de grabaciones, el almacenamiento se limpia automáticamente una vez este llega a su máxima capacidad. Dos personas tienen acceso al sistema de seguridad desde la PC de cobros y celulares.

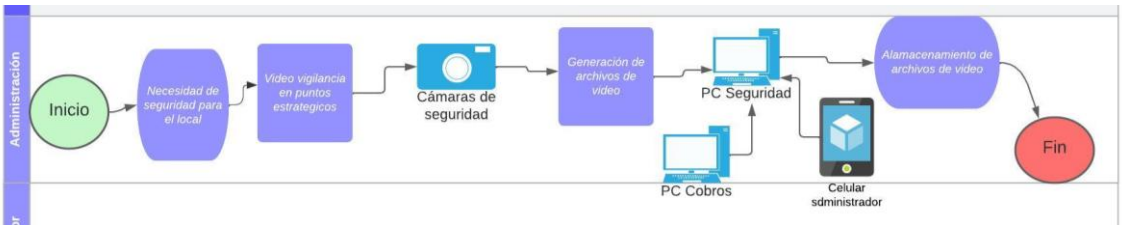



Figura 9: Proceso de seguridad

Elaborado por: Jorge Bonilla

**Identificación de activos de TI en este proceso:**

- PCs seguridad
- Cámaras IP
- Modem
- Cables de red

### 3.1.5 Identificación de riesgos

**Descripción general:**

**R1.**Errores humanos leves: Cualquier error menor en el ingreso de datos, errores tipográficos, errores de consulta o errores de archivado que causan dificultades leves en las operaciones de la empresa

**R2.**Errores humanos moderadores: Cualquier error relacionado a perdida o borrado de archivos importantes, inserción de datos erróneos o configuraciones de servidores causan dificultades menores.

**R3.**Errores humanos graves: Cualquier error significativo para las operaciones de TI, como el borrado de una o más BD, errores en la gestión de usuarios, falta de medidas de seguridad en la red implican dificultades mayores que pueden detener las operaciones de la empresa por periodos prolongados junto al impacto económico moderado.

**R4.**Errores humanos críticos: Cualquier error severo que comprometa la integridad parcial o total del sistema, estos causan dificultades graves que detienen las operaciones por periodos prolongados e implican un impacto económico grave para la empresa.

**R5.**Robo o perdida de periféricos: Implica costos y dificultades para las operaciones de la empresa.

**R6.**Robo o perdida de CPU'S y sus componentes: Implica pérdidas económicas y dificultades para las operaciones de la empresa, además de la perdida y exposición de datos sensibles.

**R7.**Daños físicos de periféricos: Implican costos y dificultades para las operaciones de la empresa.

**R8.**Daños físicos de CPU'S y sus componentes: Implican pérdidas económicas y dificultades para las operaciones de la empresa, compromete la reputación de la empresa.

**R9.**Fallos de periféricos: Causados por desgaste, fallos de diseño, errores humanos, causando interrupciones en el funcionamiento de los dispositivos o daños, que a su vez implica dificultades para las operaciones de la empresa.

**R10.** Fallos de CPU'S y sus componentes: Causados por desgaste, fallos de diseño, errores humanos, implica dificultades para las operaciones de la empresa, perdida de datos y perjuicio económico.

**R11.** Virus: Implica la perdida de información y la ralentización de los servicios de TI.

**R12.** Ransomware: Implica el robo de datos sensibles y extorsión a los propietarios de los mismos, provocando pérdidas económicas y el cese de las operaciones de la empresa.

**R13.** Spyware: Recopila toda clase de información de los usuarios objetivo y lleva a cabo seguimiento de sus actividades con fines extorsivos, ralentiza el sistema donde está instalado con ayuda de otros tipos de malware y deja el camino listo para otros tipos de ataque, todo esto afecta operativa y económicamente a la empresa.

**R14.** Fallos de software: Errores de programación, configuraciones o instalaciones incorrectas implican brechas de seguridad, perdida de datos, fallas en el funcionamiento y daños de los equipos.

**R15.** Fallos de actualización: Incompatibilidad, errores de actualización, vulnerabilidades no resueltas implican errores, mal funcionamiento, impacto negativo en la productividad y perdidas de datos.

**R16.** Acceso no autorizado: La falta de controles de acceso, credenciales débiles o permisos mal configurados implican brechas de seguridad para los datos y el sistema.

**R17.** Ataques de denegación de servicio (DoS): Atacantes externos inundan la red con tráfico, ralentizando la red.

**R18.** Interceptación de datos: Ante ausencia de cifrado en el sistema y cables de red desprotegidos, los datos están expuestos, facilitando a los atacantes su extracción mediante suplantación de identidad.

**R19.** Interferencia electromagnética: Las interferencias electromagnéticas afectan la calidad de la señal de los cables de red, provocando perdidas de datos o errores de transmisión.

**R20.** Cableado defectuoso o dañado: Cables defectuosos o dañados pueden provocar interrupciones en la comunicación y afectar la disponibilidad de la red.

**R21.** Espionaje físico: Un atacante físicamente cercano puede utilizar dispositivos de monitoreo (sniffers) para interceptar y capturar información.

**R22.** Ataques de reenvió de tráfico: En base a ataques de suplantación de direcciones ARP los atacantes redirigen el tráfico de la red hacia ellos, permitiendo manipular la comunicación entre los dispositivos conectados al switch.

**R23.** Ataque de inundación de switch: Los atacantes envían gran cantidad de tráfico hacia el switch con el objetivo de causar fallos en el mismo o volverlo inaccesible.

**R24.** Ataques de envenenamiento ARP (Addres Resolution Protocol): Mediante tramas de red corruptas se altera la tabla de direcciones MAC del switch, permitiendo a los atacantes asociar su dirección MAC con una IP legitima de la red, permitiendo interceptar información.

**R25.** Fallas del suministro eléctrico: Las fallas del suministro eléctrico tienen un impacto significativo en la red, provocando desde la interrupción de los servicios de TI hasta fallos y daños en el inventario ofimático.

**R26.** Fallas del servicio de internet: Causadas por fallas en la infraestructura de la red o problemas con el proveedor implican interrupciones parciales o totales en los servicios de TI.

**R27.** Vacunadores: La presencia de extorsionistas afecta directamente al área financiera de las empresas y por ende a la disponibilidad de recursos económicos para gestionar el área de TI.

**R28.** Desastres naturales: Los desastres naturales implican desde cortes prolongados de electricidad hasta daño o destrucción del inventario ofimático, causando suspensión de los servicios de Ti y la perdida de datos.

**R29.** Incendios: Representas daños directos a la infraestructura de la red y al inventario ofimático en general, implica además la perdida de datos sensibles.

**R30.** Software sin licencia: La utilización de software sin licencia implica problemas legales y sanciones económicas para quien lo utilice, además de representar fallas en la seguridad del sistema informático de la empresa y comprometer la integridad de los datos sensibles.

**R31.** Acceso no autorizado a la data center: El acceso no autorizado puede ser físico o remoto, esto compromete la integridad de los datos sensibles almacenados en el data center y la seguridad del sistema en general.

**R32.** Riesgo de estática: Las descargas de estática afectan a los dispositivos electrónicos en términos de rendimiento y durabilidad, causan perdidas de datos y en casos extremos provocar incendios.

### 3.1.6 Matriz de riesgos

La presente tabla muestra las posibles consecuencias de los riesgos identificados en cada proceso de la empresa.

| Procesos / Riesgos | Adquisición | Ventas | Facturación | Transacciones | Reembolso | Seguridad |
|---|---|---|---|---|---|---|
| **R1** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |
| **R2** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |
| **R3** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |
| **R4** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. | Brechas de en el sistema de seguridad. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | Ralentización de los reembolsos. | |
| **R5** | Ralentización del ingreso de nuevos productos. Robo o perdida de información de inventario. | Ralentización en la generación de nuevas ventas. Robo o perdida de información de ventas. | Ralentización en la generación de nuevas facturas. Robo o perdida de información de facturación. | Ralentización en el proceso contable. Robo o perdida de información contable. | Ralentización de los reembolsos. Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Reducción del alcance de la videovigilancia. |
| **R6** | Ralentización del ingreso de nuevos productos. Robo o perdida de información de inventario. | Ralentización en la generación de nuevas ventas. Robo o perdida de información de ventas. | Ralentización en la generación de nuevas facturas. Robo o perdida de información de facturación. | Ralentización en el proceso contable. Robo o perdida de información contable. | Ralentización de los reembolsos. Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Reducción del alcance de la videovigilancia. |
| **R7** | Ralentización del ingreso de nuevos productos. | Ralentización en la generación de nuevas ventas. | Ralentización en la generación de nuevas facturas. | Ralentización en el proceso contable. | Ralentización de los reembolsos. | Brechas en el sistema de seguridad. Reducción del alcance de la videovigilancia. |
| **R8** | Ralentización del ingreso de nuevos productos. Perdida de datos sobre productos. | Ralentización en la generación de nuevas ventas. Perdida de datos sobre ventas. | Ralentización en la generación de nuevas facturas. Perdida de datos de facturación. | Ralentización en el proceso contable. Perdida de datos contables. | Ralentización de los reembolsos. Dificultad para acceder a los datos de ventas | Brechas en el sistema de seguridad. Reducción del alcance de la videovigilancia. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **R9** | Ralentización del ingreso de nuevos productos. | Ralentización en la generación de nuevas ventas. | Ralentización en la generación de nuevas facturas. | Ralentización en el proceso contable. | Ralentización de los reembolsos. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia. |
| **R10** | Ralentización del ingreso de nuevos productos. Perdida de datos sobre productos. | Ralentización en la generación de nuevas ventas. Perdida de datos sobre ventas. | Ralentización en la generación de nuevas facturas. Perdida de datos de facturación. | Ralentización en el proceso contable. Perdida de datos contables. | Ralentización de los reembolsos. Dificultad para acceder a los datos de ventas | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia. |
| **R11** | Perdida de información de inventario. | Ralentización en la generación de nuevas ventas. Perdida de información de ventas. | Ralentización en la generación de nuevas facturas. Perdida de información de facturación. | Ralentización en el proceso contable. Perdida de información contable. | Ralentización de los reembolsos. Perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia. |
| **R12** | Robo o perdida de información de inventario. | Ralentización en la generación de nuevas ventas. Robo o perdida de información de ventas. | Ralentización en la generación de nuevas facturas. Robo o perdida de información de facturación. | Ralentización en el proceso contable. Robo o perdida de información contable. | Ralentización de los reembolsos. Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Perdida de registros de videovigilancia. |
| **R13** | Robo o perdida de información de inventario. | Ralentización en la generación de nuevas ventas. | Ralentización en la generación de nuevas facturas. | Ralentización en el proceso contable. Robo o perdida de información contable. | Ralentización de los reembolsos. Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | | | Perdida de registros de videovigilancia. |
| **R14** | Fallos o perdida de información de inventario. | Ralentización en la generación de nuevas ventas. | Ralentización en la generación de nuevas facturas. | Ralentización en el proceso contable. | Ralentización de los reembolsos. | Registros corruptos de videovigilancia. |
| **R15** | Fallos o perdida de información de inventario. | Ralentización en la generación de nuevas ventas. | Ralentización en la generación de nuevas facturas. | Ralentización en el proceso contable. | Ralentización de los reembolsos. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia. |
| **R16** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Seguimiento de las actividades por terceros |
| **R17** | Fallas al generar registros por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | |
| **R18** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **R19** | Fallas al generar registros por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | Registros corruptos de videovigilancia. |
| **R20** | Fallas al generar registros por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia |
| **R21** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | |
| **R22** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Seguimiento de las actividades por terceros |
| **R23** | Fallas al generar registros por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **R24** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia |
| **R25** | Fallas al generar registros por baja o nula disponibilidad de red. Fallos o perdida de información de inventario. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia. |
| **R26** | Fallas al generar registros por baja o nula disponibilidad de red. Fallos o perdida de información de inventario. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | Brechas en el sistema de seguridad. Registros corruptos de videovigilancia. |
| **R27** | Dificultades para adquirir suministros. | Reducción de ventas por inseguridad. | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **R28** | Perdida de información de inventario.<br>Perdida de inventario ofimático designado. | Perdida de información de ventas.<br>Perdida de inventario ofimático designado. | Perdida de información de facturación.<br>Perdida de inventario ofimático designado. | Perdida de información contable.<br>Perdida de inventario ofimático designado. | Perdida de información de notas de crédito.<br>Perdida de inventario ofimático designado. | Perdida de registros de videovigilancia.<br>Perdida de inventario ofimático designado. |
| **R29** | Perdida de información de inventario.<br>Perdida de inventario ofimático designado. | Perdida de información de ventas.<br>Perdida de inventario ofimático designado. | Perdida de información de facturación.<br>Perdida de inventario ofimático designado. | Perdida de información contable.<br>Perdida de inventario ofimático designado. | Perdida de información de notas de crédito.<br>Perdida de inventario ofimático designado. | Perdida de registros de videovigilancia.<br>Perdida de inventario ofimático designado. |
| **R30** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad.<br>Registros corruptos de videovigilancia. |
| **R31** | Robo o perdida de información de inventario. | Robo o perdida de información de ventas. | Robo o perdida de información de facturación. | Robo o perdida de información contable. | Robo o perdida de información de notas de crédito. | |
| **R32** | Fallas al generar registros por baja o nula disponibilidad de red. | Ralentización en la generación de nuevas ventas por baja o nula disponibilidad de red | Ralentización en la generación de nuevas facturas por baja o nula disponibilidad de red. | Ralentización en el proceso contable por baja o nula disponibilidad de red. | Ralentización de los reembolsos por baja o nula disponibilidad de red. | Brechas en el sistema de seguridad.<br>Registros corruptos de videovigilancia. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Fallos o perdida de información de inventario. | | | | | |

Tabla 5: Matriz de riesgos

Elaborado por: Jorge Bonilla

### 3.1.7 Matriz de elementos

La presente tabla muestra los elementos del inventario ofimático de la empresa afectados por cada riesgo identificado, las casillas en color azul señalan los elementos afectados.

| Elementos / Riesgos | Servidor sistema de facturación | BD sistema de facturación | PCs contadoras | PC secretaria | PC cobros | PCs ventas | Modem | Switches | Cables de red | Cámaras IP | PC videovigilancia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **R1** | | | | | | | | | | | |
| **R2** | | | | | | | | | | | |
| **R3** | | | | | | | | | | | |
| **R4** | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **R5** | | | | | | | | | | | |
| **R6** | | | | | | | | | | | |
| **R7** | | | | | | | | | | | |
| **R8** | | | | | | | | | | | |
| **R9** | | | | | | | | | | | |
| **R10** | | | | | | | | | | | |
| **R11** | | | | | | | | | | | |
| **R12** | | | | | | | | | | | |
| **R13** | | | | | | | | | | | |
| **R14** | | | | | | | | | | | |
| **R15** | | | | | | | | | | | |
| **R16** | | | | | | | | | | | |
| **R17** | | | | | | | | | | | |
| **R18** | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **R19** | | | | | | | | | | | |
| **R20** | | | | | | | | | | | |
| **R21** | | | | | | | | | | | |
| **R22** | | | | | | | | | | | |
| **R23** | | | | | | | | | | | |
| **R24** | | | | | | | | | | | |
| **R25** | | | | | | | | | | | |
| **R26** | | | | | | | | | | | |
| **R27** | | | | | | | | | | | |
| **R28** | | | | | | | | | | | |
| **R29** | | | | | | | | | | | |
| **R30** | | | | | | | | | | | |
| **R31** | | | | | | | | | | | |
| **R32** | | | | | | | | | | | |

Tabla 6: Matriz de elementos

Elaborado por: Jorge Bonilla

### 3.1.8 Calificaciones de probabilidad y nivel de impacto

La tabla a continuación muestra los resultados de aplicar la metodología Delphi, muestra la probabilidad y el nivel de impacto de cada riesgo en una escala de 1 a 5, la información se obtuvo con ayuda de personal clave de la empresa y 2 consultores externos.

| Riesgo ID | Encargado de TI | | Contadora | | Investigador | | Consultor 1 | | Consultor 2 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto |
| **R1** | 2 | 1 | 1 | 1 | 3 | 1 | 4 | 1 | 4 | 3 |
| **R2** | 1 | 2 | 1 | 1 | 2 | 1 | 4 | 2 | 3 | 3 |
| **R3** | 3 | 2 | 2 | 2 | 2 | 3 | 3 | 4 | 4 | 4 |
| **R4** | 3 | 4 | 2 | 2 | 2 | 4 | 2 | 5 | 3 | 5 |
| **R5** | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 3 |
| **R6** | 1 | 3 | 1 | 1 | 2 | 3 | 2 | 4 | 2 | 4 |
| **R7** | 2 | 3 | 2 | 2 | 4 | 2 | 2 | 1 | 2 | 2 |
| **R8** | 2 | 3 | 3 | 3 | 4 | 3 | 3 | 3 | 2 | 4 |
| **R9** | 1 | 2 | 1 | 1 | 4 | 1 | 2 | 1 | 2 | 1 |
| **R10** | 2 | 2 | 1 | 1 | 4 | 3 | 3 | 2 | 2 | 3 |
| **R11** | 1 | 2 | 1 | 1 | 3 | 3 | 5 | 4 | 5 | 4 |
| **R12** | 1 | 3 | 1 | 1 | 3 | 4 | 5 | 4 | 5 | 5 |
| **R13** | 1 | 3 | 1 | 1 | 4 | 3 | 5 | 4 | 5 | 4 |
| **R14** | 1 | 3 | 2 | 2 | 2 | 2 | 4 | 3 | 4 | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **R15** | 2 | 4 | 3 | 1 | 2 | 3 | 1 | 3 | 1 | 2 |
| **R16** | 1 | 3 | 1 | 1 | 1 | 3 | 4 | 4 | 4 | 5 |
| **R17** | 1 | 4 | 3 | 3 | 2 | 4 | 3 | 3 | 2 | 3 |
| **R18** | 1 | 3 | 1 | 1 | 2 | 2 | 3 | 4 | 4 | 4 |
| **R19** | 1 | 3 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 2 |
| **R20** | 1 | 2 | 1 | 1 | 2 | 2 | 4 | 1 | 5 | 2 |
| **R21** | 1 | 2 | 1 | 1 | 1 | 3 | 1 | 2 | 3 | 3 |
| **R22** | 1 | 2 | 1 | 1 | 1 | 4 | 1 | 4 | 2 | 4 |
| **R23** | 1 | 3 | 1 | 1 | 1 | 4 | 1 | 3 | 2 | 4 |
| **R24** | 1 | 2 | 1 | 1 | 1 | 4 | 3 | 3 | 4 | 4 |
| **R25** | 2 | 2 | 1 | 1 | 3 | 5 | 2 | 4 | 3 | 5 |
| **R26** | 1 | 2 | 2 | 2 | 2 | 4 | 2 | 5 | 2 | 3 |
| **R27** | 1 | 1 | 1 | 1 | 1 | 3 | 4 | 5 | 4 | 5 |
| **R28** | 1 | 3 | 1 | 1 | 3 | 4 | 3 | 5 | 3 | 5 |
| **R29** | 1 | 4 | 1 | 1 | 2 | 3 | 1 | 5 | 2 | 5 |
| **R30** | 1 | 1 | 1 | 1 | 3 | 3 | 5 | 5 | 5 | 5 |
| **R31** | 1 | 5 | 1 | 1 | 2 | 4 | 2 | 5 | 3 | 5 |
| **R32** | 1 | 3 | 5 | 1 | 2 | 3 | 1 | 3 | 2 | 4 |

Tabla 7: Calificaciones de probabilidad y nivel de impacto

Elaborado por: Jorge Bonilla

### 3.1.9 Clasificación por niveles de riesgo

En base al promedio de los resultados de la tabla 7, se clasifican los riesgos en función de su calificación con ayuda de la tabla 9.

| Riesgo ID | Nombre riesgo | Probabilidad | Nivel de impacto | Calificación | Nivel de riesgo |
|---|---|---|---|---|---|
| **R13** | Spyware | 4 | 3 | 4;3 | Alto |
| **R31** | Acceso no autorizado a la data center | 2 | 5 | 2;5 | Alto |
| **R3** | Errores humanos graves | 3 | 3 | 3;3 | Medio |
| **R4** | Errores humanos críticos | 2 | 4 | 2;4 | Medio |
| **R6** | Robo o perdida de CPUs y sus componentes | 2 | 3 | 2;3 | Medio |
| **R8** | Daños físicos de CPU'S y sus componentes | 3 | 3 | 3;3 | Medio |
| **R11** | Virus | 3 | 3 | 3;3 | Medio |
| **R12** | Ransomware | 3 | 4 | 3;4 | Medio |
| **R15** | Fallos de actualización | 2 | 3 | 2;3 | Medio |
| **R17** | Ataques de denegación de servicio (DoS) | 2 | 3 | 2;3 | Medio |
| **R18** | Interceptación de datos | 2 | 3 | 2;3 | Medio |
| **R22** | Ataques de reenvió de tráfico | 1 | 4 | 1;4 | Medio |
| **R25** | Fallas del suministro eléctrico | 2 | 4 | 2;4 | Medio |
| **R26** | Fallas del servicio de internet | 2 | 3 | 2;3 | Medio |
| **R28** | Desastres naturales | 3 | 4 | 3;4 | Medio |
| **R29** | Incendios | 1 | 4 | 1;4 | Medio |
| **R30** | Software sin licencia | 3 | 3 | 3;3 | Medio |
| **R32** | Riesgo de estática | 2 | 3 | 2;3 | Medio |
| **R1** | Errores humanos leves | 3 | 1 | 3;1 | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| **R2** | Errores humanos moderados | 2 | 2 | 2;2 | Bajo |
| **R5** | Robo o perdida de periféricos | 1 | 2 | 1;2 | Bajo |
| **R7** | Daños físicos de periféricos | 2 | 2 | 2;2 | Bajo |
| **R9** | Fallos de periféricos | 2 | 1 | 2;1 | Bajo |
| **R10** | Fallos de CPU'S y sus componentes | 2 | 2 | 2;2 | Bajo |
| **R14** | Fallos de software | 2 | 2 | 2;2 | Bajo |
| **R16** | Acceso no autorizado | 1 | 3 | 1;3 | Bajo |
| **R19** | Interferencia electromagnética | 1 | 2 | 1;2 | Bajo |
| **R20** | Cableado defectuoso o dañado | 2 | 2 | 2;2 | Bajo |
| **R21** | Espionaje físico | 1 | 2 | 1;2 | Bajo |
| **R23** | Ataque de inundación de switch | 1 | 3 | 1;3 | Bajo |
| **R24** | Ataques de envenenamiento ARP (Addres Resolution Protocol) | 1 | 3 | 1;3 | Bajo |
| **R27** | Vacunadores | 1 | 3 | 1;3 | Bajo |

Tabla 8: Clasificación por niveles de riesgo

Elaborado por: Jorge Bonilla

### 3.1.10 Matriz priorización de riesgos

La presente matriz muestra como clasificar los riesgos en base a la calificación probabilidad / impacto, las cuales se representan en escalas de 1 a 5, donde la probabilidad se limita entre 1 a 100% y el impacto se mide desde “muy leve” hasta “critico”.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Impacto** | **5** | **Critico** | | R31 | | | |
| | **4** | **Grave** | R22, R29 | R4, R25 | R12, R28 | | |
| | **3** | **Moderado** | R16, R23, R24, R27 | R6, R15, R17, R18, R26, R32 | R3, R8, R11, R30 | R13 | |
| | **2** | **Leve** | R5, R19, R21 | R2, R7, R10, R14, R20 | | | |
| | **1** | **Muy leve** | | R9 | R1 | | |
| | | | **1% - 20%** | **21% - 40%** | **41% - 60%** | **61% - 80%** | **81% - 100%** |
| | | | **1** | **2** | **3** | **4** | **5** |
| | | | **Probabilidad** | | | | |

Tabla 9: Matriz priorización de riesgos

Elaborado por: Jorge Bonilla

### 3.1.11 Problemas de TI clasificados

La presente tabla muestra un listado de los problemas relacionados a cada riesgo identificado, se basa en el orden de la tabla 7.

| Riesgo ID | Nombre riesgo | Problemas | Nivel de riesgo |
|---|---|---|---|
| R13 | Spyware | • Bajo rendimiento<br>• Corrupción de datos<br>• Perdida de datos<br>• Inconsistencia de datos | Alto |
| R31 | Acceso no autorizado a la data center | • Corrupción de datos<br>• Perdida de datos<br>• Inconsistencia de datos<br>• Accesos no autorizados a la base de datos<br>• Problemas de rendimiento de la base de datos | Alto |
| R3 | Errores humanos graves | • VLAN mal configurada | Medio |
| R4 | Errores humanos críticos | • Problemas de seguridad (modem)<br>• Problemas de seguridad (switch) | Medio |
| R6 | Robo o perdida de CPUs y sus componentes | • Robo o perdida de CPUs | Medio |
| R8 | Daños físicos de CPU'S y sus componentes | • Sobrecalentamiento<br>• Error de arranque de CPU<br>• Fallos de ventiladores | Medio |

| | | | |
|---|---|---|---|
| | | • Fallos de la fuente de poder<br>• Ruido excesivo del ventilador<br>• Fallas de la tarjeta madre<br>• Puertos inoperables<br>• Fallas de procesador<br>• Procesador incompatible<br>• Fallos de disco duro<br>• Fallos de memoria RAM<br>• Fallos de tarjeta gráfica<br>• Fallos de la fuente de poder<br>• Fallos de la tarjeta de red | |
| R11 | Virus | • Pantallazo azul<br>• Bloqueo del sistema<br>• Bajo rendimiento de CPU<br>• Corrupción de datos<br>• Perdida de datos<br>• Inconsistencia de datos | Medio |
| R12 | Ransomware | • Pantallazo azul<br>• Bloqueo del sistema<br>• Bajo rendimiento<br>• Perdida de datos<br>• Inconsistencia de datos | Medio |
| R15 | Fallos de actualización | • Fallas de la BIOS<br>• Bajo rendimiento de CPU<br>• Pantallazo azul<br>• Bloqueo del sistema | Medio |

| | | | |
|---|---|---|---|
| R17 | Ataques de denegación de servicio (DoS) | • Problemas de conectividad de switch<br>• Bajo rendimiento de puertos<br>• Bajo rendimiento de switch<br>• Sobrecarga de CPU de switch<br>• Sobrecarga de búfer<br>• Desbordamiento de búfer | Medio |
| R18 | Interceptación de datos | • Corrupción de datos<br>• Perdida de datos<br>• Inconsistencia de datos<br>• Accesos no autorizados a la base de datos<br>• Problemas de rendimiento de la base de datos<br>• Fallos de seguridad de switch | Medio |
| R22 | Ataques de reenvió de tráfico | • Problemas de conectividad<br>• Direcciones MAC duplicadas<br>• Bajo rendimiento de puertos<br>• Tabla incompleta<br>• Tabla llena<br>• Direcciones duplicadas<br>• Bajo rendimiento<br>• Sobrecarga de CPU<br>• Fallos de seguridad<br>• Sobrecarga de búfer<br>• Desbordamiento de búfer | Medio |
| R25 | Fallas del suministro eléctrico | • Fallos de la fuente de poder<br>• Sobrecalentamiento<br>• Error de arranque de CPU | Medio |

| | | | |
|---|---|---|---|
| R26 | Fallas del servicio de internet | • Conexión a internet inestable por fallas del modem<br>• Baja velocidad por fallas de interfaces del modem<br>• Problemas de configuración del modem<br>• Problemas de seguridad del modem<br>• Problemas de incompatibilidad del modem<br>• Conexión a internet inestable por fallas de procesador<br>• Baja velocidad por fallas de procesador del modem<br>• Memoria insuficiente<br>• Corrupción de datos<br>• Actualizar firmware<br>• Fallos de firmware<br>• Configuración incorrecta<br>• Problemas de compatibilidad<br>• Problemas persistentes<br>• Tabla de enrutamiento incorrecta<br>• Problemas de IP<br>• Actualizar firmware<br>• Configuración incorrecta<br>• Bloqueo de puertos necesarios<br>• Restricciones de acceso<br>• Actualizar firmware<br>• Fallas de procesamiento | Medio |

| | | | |
|---|---|---|---|
| | | • Problemas de compresión de video<br>• Fallas de procesamiento de imagen | |
| R28 | Desastres naturales | • Daños físicos del revestimiento del cable de red<br>• Daños físicos de la cubierta exterior del cable de red<br>• Robo o perdida de CPUs<br>• Robo o perdida de periféricos | Medio |
| R29 | Incendios | • Daños físicos del revestimiento del cable de red<br>• Daños físicos de la cubierta exterior del cable de red<br>• Robo o perdida de CPUs<br>• Robo o perdida de periféricos | Medio |
| R30 | Software sin licencia | • Pantallazo azul<br>• Bloqueo del sistema<br>• Bajo rendimiento de CPU | Medio |
| R32 | Riesgo de estática | • Problemas de interferencia<br>• Problemas de atenuación | Medio |
| R1 | Errores humanos leves | • Cable mal ponchado<br>• Problemas de longitud de cable<br>• Cableado incorrecto<br>• Conector flojo o suelto<br>• Oxidación o corrosión | Bajo |
| R2 | Errores humanos moderados | • Problemas de configuración del modem<br>• Problemas de seguridad del modem | Bajo |

| | | | |
|---|---|---|---|
| | | • Baja calidad de imagen por fallos de sensor de imagen<br>• Fallas de enfoque de cámara IP<br>• Problema de viñeteado de cámara IP<br>• Problemas de condensación en la lente de cámara IP | |
| R5 | Robo o perdida de periféricos | • Robo o perdida de periféricos | Bajo |
| R7 | Daños físicos de periféricos | • Pixeles muertos<br>• Problemas de retroalimentación<br>• Problemas de encendido<br>• Pantalla sin imagen<br>• Parpadeo de pantalla<br>• Teclas atascadas<br>• Daños por líquidos<br>• Cable dañado<br>• Teclas pegadas o ruidosas | Bajo |
| R9 | Fallos de periféricos | • Pixeles muertos<br>• Imagen distorsionada<br>• Problemas de encendido<br>• Pantalla sin imagen<br>• Parpadeo de pantalla<br>• Fallos de color o imagen<br>• Resolución incorrecta<br>• Fallos de teclas<br>• Caracteres incorrectos<br>• Tiempo de respuesta prolongado | Bajo |

| | | | |
|---|---|---|---|
| | | • Cursor con movimiento errático<br>• Clics inconsistentes o con retardo<br>• Desplazamiento irregular<br>• Mouse sin respuesta | |
| R10 | Fallos de CPU'S y sus componentes | • Pantallazo azul<br>• Bloqueo del sistema<br>• Bajo rendimiento | Bajo |
| R14 | Fallos de software | • Pantallazo azul<br>• Bloqueo del sistema<br>• Bajo rendimiento de CPU | Bajo |
| R16 | Acceso no autorizado | • Robo o perdida de CPUs<br>• Robo o perdida de periféricos<br>• Corrupción de datos<br>• Perdida de datos<br>• Inconsistencia de datos | Bajo |
| R19 | Interferencia electromagnética | • Problemas de interferencia por daños en el conductor de cobre<br>• Problemas de atenuación<br>• Problemas de interferencia por daños en cubierta exterior | Bajo |
| R20 | Cableado defectuoso o dañado | • Problemas de interferencia por daños en el conductor de cobre<br>• Problemas de atenuación<br>• Problemas de interferencia por pares mal trenzados | Bajo |

| | | | |
|---|---|---|---|
| | | • Problemas de longitud de cable<br>• Daños físicos del revestimiento del cable de red<br>• Oxidación o corrosión<br>• Daños físicos de la cubierta exterior del cable de red<br>• Problemas de interferencia por daños en cubierta exterior<br>• Problemas de flexibilidad | |
| R21 | Espionaje físico | • Corrupción de datos<br>• Perdida de datos<br>• Inconsistencia de datos<br>• Accesos no autorizados a la base de datos<br>• Problemas de rendimiento de la base de datos | Bajo |
| R23 | Ataque de inundación de switch | • Problemas de conectividad de switch<br>• Direcciones MAC duplicadas<br>• Bajo rendimiento de puertos de switch<br>• Tabla incompleta<br>• Tabla llena<br>• Direcciones duplicadas<br>• Bajo rendimiento de switch<br>• Sobrecarga de CPU de switch<br>• Fallos de seguridad de switch<br>• Sobrecarga de búfer<br>• Problema de latencia<br>• Desbordamiento de búfer | Bajo |

| | | | |
|---|---|---|---|
| R24 | Ataques de envenenamiento ARP (Addres Resolution Protocol) | • Problemas de conectividad de switch<br>• Direcciones MAC duplicadas<br>• Bajo rendimiento de puertos de switch<br>• Tabla incompleta<br>• Tabla llena<br>• Direcciones duplicadas<br>• Bajo rendimiento de switch<br>• Sobrecarga de CPU de switch<br>• Fallos de seguridad de switch<br>• Sobrecarga de búfer<br>• Problema de latencia<br>• Desbordamiento de búfer | Bajo |
| R27 | Vacunadores | • Robo o perdida de CPUs<br>• Robo o perdida de periféricos | Bajo |

Tabla 10: Problemas de TI clasificados

Elaborado por: Jorge Bonilla

# CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

## 4.1 Conclusiones

- La observación de los procesos empresariales que involucran el uso de las TI evidenciaron la poca atención y conocimiento sobre riesgos de TI. Además, se identificó una dependencia significativa de asistencia técnica de terceros para hacer frente a daños o incidentes con el inventario ofimático, esto representa una deficiente gestión de los recursos de TI y la ausencia de una metodología para la gestión de riesgos.
- De acuerdo con los objetivos planteados, se realizó el análisis bibliográfico para determinar los principios necesarios para la gestión de riesgos de TI, por lo que se identificaron semejanzas y diferencias entre las metodologías propuestas, determinando aspectos clave como el ciclo de vida para servicios de TI y la alineación del gobierno de TI con los objetivos empresariales para la creación de valor para las partes interesadas.
- El resultado de integrar las metodologías propuestas cuenta con principios y estructura similares a la norma ISO/IEC 31000.2018, cumpliendo con el objetivo de la creación de valor.
- El desarrollo de la metodología hibrida dio como resultado un procedimiento a la medida de las necesidades de la empresa, la combinación de los principios planteados, identificación de los riesgos potenciales y como solventarlos ayudo a establecer el listado de problemas relacionados al inventario ofimático de la empresa.

## 4.2 Recomendaciones

- Se recomienda capacitar al personal de la empresa en temas relacionados a ciberseguridad y uso de dispositivos a nivel básico, o en su defecto contratar a un profesional capacitado en el área de las TI para poner en práctica la metodología propuesta.
- Se sugiere mantener actualizada la lista de proveedores actuales y formular una lista de proveedores alternos, además de establecer convenios con los mismos para optimizar tiempo y costos.

- Se recomienda llevar un registro de incidentes y clasificarlos por su impacto en las actividades de la empresa, esto con el fin de ampliar el listado de problemas identificados y mejorar los tiempos de respuesta.
- Se recomienda dar seguimiento a la normativa legal relacionada a la protección de datos, esto para evitar sanciones y problemas legales.

## BIBLIOGRAFÍA


[1] M. de León-Sigg, S. Vázquez-Reyes, and J. L. Villa-Cisneros, "Factores que Afectan la Adopción de Tecnologías de Información en Micro y Pequeñas empresas: Un Estudio Cualitativo," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao,* no. 22, pp. 20–36, Jun. 2017, doi: 10.17013/risti.22.20-36.

[2] M. A. Fernández del Pomar, "La estructura organizacional, el agile mindset y el gobierno de TI para la transformación digital de las empresas," *Actas del II Congreso Internacional de Ingeniería de Sistemas* , pp. 107–126, Jun. 2019, Accessed: Nov. 09, 2022. [Online]. Available: https://hdl.handle.net/20.500.12724/11173

[3] R. De, T. Tecnolog´, D. Michellc, Z. Zambrano, D. José Vélez Román, and Y. D. Daza Alava, "INFORM´ATICAINFORM´ INFORM´ATICA Y SISTEMAS," 2017. [Online]. Available: http://creativecommons.org/licenses/BY-NC-ND/4.0/1.Introducción

[4] R. De, T. Tecnolog´, D. Michellc, Z. Zambrano, D. José Vélez Román, and Y. D. Daza Alava, "GOBIERNO DE TI – IMPLEMENTACI´ON EN ELECUADOR," Manabi, 2017. [Online]. Available: http://creativecommons.org/licenses/BY-NC-ND/4.0/1.Introducción

[5] J. L. Tigse Moposita and Mayorga Franklin Oswaldo, "PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001

PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.," Ambato, Jan. 2020. Accessed: Nov. 28, 2022. [Online]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/30696/1/Tesis_t1663si.PDF

[6] U. Enfoque, "Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs (ECU@Risk, a methodology for risk management applied to MSMEs)," no. 1, pp. 107–121, 2017, [Online]. Available: http://ingenieria.ute.edu.ec/enfoqueute/

[7] J. Carlo Alfaro Campos, I. Laura Alpízar Chaves, and C. Rica, "Metodología para la gestión de riesgos de TI basada en COBIT 5," 2017.

[8] R. Quezada Sarmiento, J. Aguilar Alvarado, K. García Galarza, R. Morocho Roman, and W. Rivas Asanza, "Servicio y Gestión de las Tecnologías de la Información en las empresas," *Revista Ciencia UNEMI*, vol. 11, no. 26, pp. 170–175, Jun. 2018, Accessed: Nov. 29, 2022. [Online]. Available: https://ojs.unemi.edu.ec/index.php/cienciaunemi/article/view/682/541

[9] D. Pillo-Guanoluisa and R. Enríquez-Reyes, "MASKANA, CEDIA 2017 TIC.EC Track Científico 41 Gobierno de TI con énfasis en seguridad de la información para hospitales públicos," Quito, 2017. Accessed: Nov. 29, 2022. [Online]. Available: https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1451/1125

[10] L. H. Carrasco Cortez and H. G. Abanto Cabrera, “UNIVERSIDAD PRIVADA ANTENOR ORREGO FACULTAD DE INGENIERÍA PROGRAMA DE ESTUDIO DE INGENIERÍA ‘MARCO DE DESARROLLO BASADO EN ITIL V4.0 PARA GESTIONAR LOS INCIDENTES Y REQUERIMIENTOS A CARGO DEL AREA DE SISTEMAS DE LA UNIVERSIDAD PRIVADA DE PIURA,’” Piura, 2022.

[11] AXELOS, “ITIL 4 Foundation Spanish (Latam).”

[12] “AEC - Risk IT.” https://www.aec.es/web/guest/centro-conocimiento/risk-it (accessed Nov. 30, 2022).

[13] “Definición: Riesgo de TI, Glosario TI - Capterra.” https://www.capterra.mx/glossary/676/it-risk (accessed Nov. 30, 2022).

[14] “Gestión de las operaciones de TI - Valuit Solutions.” https://www.valuit.co/gestion-operaciones-de-ti/ (accessed Nov. 30, 2022).

[15] “¿Qué son las operaciones de TI (ITOps)? - ServiceNow.” https://www.servicenow.com/es/products/it-operations-management/what-is-it-operations.html (accessed Nov. 30, 2022).

[16] “Qué es la gestión de la TI.” https://www.redhat.com/es/topics/management (accessed Nov. 29, 2022).

[17] “¿Qué es la gestión de TI?” https://www.ibm.com/es-es/topics/it-management (accessed Nov. 29, 2022).

[18] nombre Oltra Badenes and R. Francisco, “Procesos, Funciones y Roles en ITIL® (Information Technology Infrastructure Library).”

[19] “NORMA INTERNACIONAL Traducción oficial Official translation Traduction officielle,” 2015. [Online]. Available: www.iso.org

[20] “1 MANUAL CONTEXTO DE LA ORGANIZACIÓN - IMPLEMENTANDO SGI.” https://www.implementandosgi.com/estructura-alto-nive/manual-contexto-de-la-organizacion/ (accessed Nov. 30, 2022).

[21] AXELOS, *ITIL Foundation ITIL 4 Edition (Spanish PDF) - Carlos Rivas Istacuy _ Flip PDF en línea _ FlipHTML5*, 2º. TSO, 2019. Accessed: Apr. 26, 2023. [Online]. Available: http://www.axelos.com

[22] *NORMA INTERNACIONAL ISO 31000*. Accessed: May 05, 2023. [Online]. Available: https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486

# ANEXOS

La siguiente entrevista presenta información proporcionada por el gerente de la empresa, esto con el fin de comprender el punto de vista del alto mando de la empresa.

**Guía de entrevista**

**Objetivo:** Recolectar información sobre el funcionamiento del sistema informático.

**Sujeto de estudio:** Ferretería "Su Casa"

**Actividad comercial:** Comercialización de productos de ferretería, hogar, acabados y materiales de construcción

**Entrevistado:** Ramiro Naranjo **Cargo que ocupa:** Gerente

**Entrevistador:** Jorge Bonilla

**Fecha y hora de la entrevista:** 17/04/2023 15h00

| **Pregunta** | **Respuesta** | **Observaciones** |
|---|---|---|
| 1. ¿Han definido un presupuesto para la seguridad de la información? ¿Cuánto? | No lo han definido, la seguridad de la información no es tema que se tome a consideración. | Esto pone en riesgo los datos que no se han generado con el sistema de facturación. |

| | | |
|---|---|---|
| 2. ¿Han definido un presupuesto para la seguridad del inventario ofimático? ¿Cuánto? | No Lo han definido, cualquier gasto relacionado a TI va con los demás gastos de la empresa. | Esto da la posibilidad a gastos excesivos en TI, afectando económicamente a la empresa. |
| 3. ¿Los empleados han recibido capacitación relacionada a la seguridad de la información? | No la han recibido | La falta de conocimiento sobre el tema incrementa el riesgo para los datos de la empresa. |
| 4. ¿Los empleados han recibido capacitación relacionada al uso del inventario ofimático? | Si, pero solo cuando implementaron el sistema, los nuevos reciben guía de los demás empleados en base a conocimiento empírico en su mayoría. | El conocimiento empírico es fiable siempre y cuando se depure y lleve un registro del mismo, caso contrario este puede ser la base de múltiples problemas. |
| 5. ¿Cuál fue la última adquisición de equipo ofimático? ¿Por qué? | Impresora del departamento administrativo debido a fallas de los cartuchos. | |
| 6. ¿Cuentan con un procedimiento a la hora de adquirir nuevos equipos ofimáticos? | No cuentan, se adquieren según se va necesitando y por recomendación de un experto que contratan ocasionalmente. | A nivel empresarial es necesario mantener el control de sus adquisiciones, sean del tipo que sean. |
| 7. ¿Tienen planeado invertir en TI a corto, medio o largo plazo? | Si, para futuras expansiones del negocio. | |

| | | |
|---|---|---|
| 8. ¿Qué informes le gustaría recibir relacionados al manejo y gestión de la seguridad de TI de la empresa? | Informes trimestrales y que lo puedan entender los usuarios comunes. | |
| 9. ¿Cuáles son los archivos más importantes para el negocio?,¿Quién los gestiona? | Registros de compras, cuentas por cobrar y pagar, inventarios, estos son archivos XML que son gestionados por el personal administrativo.<br>Especificaciones:<br>Asistente Contable: retenciones<br>Contadora: facturas de ventas y compras, estados de cuenta, inventarios, bancos<br>Secretaria: cartas, estados de cuentas, conciliaciones bancarias, facturación, revisión de bancos | El personal que gestiona los archivos está conformado por usuarios comunes, esto representa una brecha de seguridad importante en cuanto seguridad de la información se refiere. |
| 10. ¿Cuál es el equipo más importante para el negocio?,¿Quién lo gestiona? | El servidor con el sistema de facturación, esta cuenta además con los todos los archivos generados en la empresa, es gestionado por gerencia. | La falta de procedimientos para respaldar la información es una brecha de seguridad importante. |
| 11. ¿Cuentan con seguro para el inventario ofimático? | No cuentan | |
| 12. ¿Cuentan con seguro para la | No cuentan | |

| | | |
|---|---|---|
| información? | | |
| 13. ¿Cuentan con proveedores fijos para adquirir nuevos equipos ofimáticos? | Si, cuentan con un proveedor | |
| **Conclusiones:** El gerente en cuanto a su rol se extralimita e interviene en aspectos para los cuales no está preparado, esto causa que se tomen decisiones poco efectivas en el apartado de TI, lo que a la larga puede causar daños irreversibles a la infraestructura de TI de la empresa, comprometiendo así la continuidad del negocio. | | |

Anexo 1: Guía de entrevista al gerente

Elaborado por: Jorge Bonilla

La siguiente entrevista presenta información sobre la administración de las TI de la empresa, esto con el fin de comprender el punto de vista de quienes utilizan la TI de la empresa.

**Guía de entrevista**

**Objetivo:** Recolectar información sobre el funcionamiento del sistema informático.

**Sujeto de estudio:** Ferretería "Su Casa"

**Actividad comercial:** Comercialización de productos de ferretería, hogar, acabados y materiales de construcción

**Entrevistado:** Luis Miranda **Cargo que ocupa:** Encargado de sistemas.

**Entrevistador:** Jorge Bonilla

**Fecha y hora de la entrevista:** 15/04/2023 09h00

| **Pregunta** | **Respuesta** | **Observaciones** |
|---|---|---|
| 1. En resumen, ¿Cómo funciona el sistema que utilizan en la empresa? | • Todos usan con el mismo usuario en el sistema de facturación, es un cliente, son un total de 7 persona, puestos fijos a veces salen a despachar, utilizan las terminales de forma dinámica. A nivel de la red todos | El uso de múltiples sistemas operativos sin licencia deja muchas brechas de seguridad, no tienen claro como los archivos de venta recorren la red.<br>El encargado es capaz de solventar pequeños problemas técnicos, para |

| | | |
|---|---|---|
| | utilizan todo. Comparten la red entre ventas y administrativo, en el caso de administrativo cada empleado tiene su terminal con sus credenciales.<br>• Todas las terminales tienen acceso a servidor del sistema de facturación. El personal de venta solo puede ingresar ventas.<br>• Tanto el encargado como el gerente pueden realizar CRUD, si hay error durante el registro de una venta también pueden solventar,<br>• a administración entran las ventas<br>• El sistema de facturación es compatible con Windows 7,8 y 10.<br>• De cierta forma administración y ventas funcionan por separado<br>Todos los vendedores comparten un solo usuario para el sistema de facturación, además las contraseñas de los perfiles no son seguras. | problemas mayores requieren de apoyo externo.<br>Los vendedores comparten un solo usuario para el sistema de facturación, usuario que no cuenta con clave segura, esto es una brecha de seguridad importante<br>Todo el sistema depende de la conexión a internet, sin eso sus operaciones se detienen hasta que el servicio se restaure.<br>Tienen conexión con una sucursal, para esto utilizan software poco seguro, el cual puede permitir el acceso de terceros. |

| | | |
|---|---|---|
| 2. ¿Cuál es su rol en cuanto a la administración del sistema? | Es el encargado de supervisar todo el sistema | Posee pocos conocimientos sobre cómo funciona el sistema, en cuanto a sus conocimientos sobre informática son insuficientes y requiere ayuda de terceros con frecuencia. |
| 3. ¿En cuántas terminales está instalado el sistema? | • Son 6 terminales destinadas al sistema de facturación, de las cuales 1 es para el cobro,1 para supervisión de ventas, 3 para el ingreso de nuevas ventas y la última como servidor, en el departamento de administración cuentan con terminales, 1 para la secretaria que a su vez es la terminal principal de la red y los 2 restantes son para las contadoras.<br>• En la sucursal 2 utilizan un sistema provisto por Disensa | Las terminales destinadas a ventas tienen cierto grado de vulnerabilidad, estas se encuentran en el escaparate dejando totalmente expuestos los periféricos de cada una, aunque exista un sistema de vigilancia estos corren peligro de daño o perdida. |
| 4. ¿Cuántos usuarios tienen acceso al sistema? | • En total son 11 usuarios en la sucursal 1, 5 que cuentan con acceso a todo el sistema (gerente, encargado y personal administrativo), los 6 restantes tienen acceso parcial al sistema (generar ventas). | El gerente puede acceder a la BD y modificar las tablas, pero no cuenta con el conocimiento para hacerlo, lo que dadas las condiciones adecuadas puede causar problemas al negocio, el encargado puede llevar a cabo procesos CRUD que en general no representan |

| | | |
|---|---|---|
| | • En la sucursal 2 son 3 usuarios que se dedican únicamente a ventas. | una amenaza para la continuidad del negocio. |
| 5. ¿Qué tipos de archivos genera cada empleado en base a su perfil? | • Los vendedores y el gerente generan archivos XML a la hora de realizar ventas, además de reportes en PDF de las mismas.<br>•<br>• Personal administrativo genera archivos derivados del paquete de office (hojas de cálculo, docs. de Word)<br>• Adicional se generan archivos de video de las cámaras de seguridad, eso bajo el control del gerente. | Los archivos XML y PDF se generan sin mayor intervención de los usuarios, esto es un punto a favor en la gestión del sistema, en cuanto a los archivos de administración estos son generados 100% por el personal administrativo. |
| 6. ¿Dónde almacenan estos archivos? | En el mismo servidor donde este alojado el sistema de facturación. | Esto es muy riesgoso para la continuidad del negocio, puesto que mantener todos los archivos en un mismo almacenamiento, que además se encuentra en una ubicación poco segura. |

| | | |
|---|---|---|
| 7. ¿Existen procedimientos de respaldos de esos archivos? | • Lo llevan por impreso y lo respaldan en el servidor de facturación. | Llevar respaldo en físico aparte de ser poco práctico es riesgoso, este formato es más vulnerable a sufrir daños. |
| 8. ¿Cómo se estructura la red de la empresa? | Es una red LAN con topología de estrella escalonada, se divide en 2 secciones, cada una con su switch, en la planta baja se encuentra el departamento de ventas con sus respectivas terminales conexión al servidor destinado al sistema de facturación, en el primer piso está el departamento administrativo, donde se encuentra el modem que sostiene toda la red y las terminales para el personal administrativo. | Cuentan con poco conocimiento de cómo está estructurada la red, en caso de fallos a nivel estructural las operaciones se detienen hasta que la ayuda de un tercero llegue.<br>Los Wireless son un problema, son una posible entrada para intrusos. |
| 9. ¿Qué equipos de red utilizan? | • Cuentan con una sola línea de internet, el modem se encuentra en administración, el cual alimenta a toda la red, además de 2 switches, uno por cada departamento, que a su vez se conectan a un punto de acceso inalámbrico cada uno. | Estos equipos están ubicados en puntos accesibles para todos los empleados, esto implica un fallo de seguridad importante, además de que dichas ubicaciones no son las más optimas. |
| 10. ¿Cuál es la categoría del cable de red? | Cable UTP categoría 5 en la sucursal 1<br>Cable UTP categoría 6 en la sucursal 2 | Los cables se han dispuesto por el inmueble sin mayor cuidado, son propensos a recibir daño físico. |
| 11. ¿Cuentan con algún | El cableado es estructurado | |

| | | |
|---|---|---|
| procedimiento para manejar el cableado? | | |
| 12. ¿Cuántas veces al año se lleva a cabo mantenimiento de los equipos? | Se realizan 2 veces al año, manteniendo preventivo por acumulación de polvo | No están en capacidad de llevarlo a cabo por su cuenta, requieren ayuda externa |
| 13. ¿Qué sistema operativo usan en las terminales y en el servidor? | En las terminales de ventas y administración trabajan con los SO Windows 7,8 y 10, en el servidor destinado al sistema de facturación trabajan con Windows server 2012 | |
| 14. Enliste los softwares que utilizan en la empresa y detalle si cuentan o no con licencia. | • Paquete de office – sin licencia<br>• Adobe PDF – libre<br>• Any desk – libre<br>• Microplus SQL 2019 -licencia<br>• TeamViewer – libre<br>• EVA ERP(sistema facturación sucursal, proveedor Disensa) – licencia | La causa de que en su mayoría sea software libre o crackeado es económica, esto implica riesgos para los datos de la empresa. |

| | | |
|---|---|---|
| | • Software impresoras Epson – licencia<br>• Winrar – libre<br>• Zoom – libre<br>• FIRMAEC – libre (provee el gobierno)<br>• Antivirus Avast – libre<br>• SRI - DIMM – libre | |
| 15. ¿Cuentan con bitácora para registro de los incidentes del sistema? | No cuentan | Esto dificulta la investigación, pues no permite conocer en su totalidad el estado inicial de la empresa. |
| 16. ¿Cuál ha sido el mayor inconveniente relacionado al sistema? | Caída parcial de la red debido a switch defectuoso. | |
| 17. ¿Cuál es el inconveniente más común en el sistema? | Caídas de internet, imposibilita el uso del sistema de facturación y por ende de todo el sistema de la empresa. | La absoluta dependencia del sistema al internet es una problemática a tener en cuenta. Requiere de un proveedor de |

| | | |
|---|---|---|
| | | internet alterno para garantizar la continuidad del negocio. |
| 18. ¿Alguna vez el sistema sufrió fallas catastróficas? ¿Cómo las afrontaron? | Ninguno | Esto debido a que al tamaño de la empresa. |
| 19. ¿Cuál es el incidente más reciente?, ¿Cómo afecto esto a las operaciones de la empresa? | Fallo del servicio eléctrico durante una hora, detuvo las operaciones de la empresa. | Esto es un error que con el equipamiento adecuado se puede solventar. |
| 20. ¿Qué tan complejo es para los usuarios finales usar el sistema? | No tienen dificultades para usar el sistema, lo que más da problema es las impresiones en administración. | |
| 21. ¿Existe algún encargado para capacitar a nuevos usuarios? | No existe personal fijo, es un proceso autodidáctico, comparten conocimiento empírico. | Esto puede dar paso a omisiones sobre el uso del inventario ofimático y por ende a errores. |
| 22. ¿Qué medidas de seguridad usan para proteger el sistema y los datos de la empresa? | Cuentan con un sistema de video vigilancia en el local. | Esta medida es un punto positivo sobre la gestión del sistema de la empresa. |

| | | |
|---|---|---|
| 23. ¿Quién es el responsable de gestionar la BD? | El gerente cuenta con perfil de super usuario | La falta de personal calificado para gestionar la BD es un claro problema a la hora de mantener la seguridad del sistema. |
| 24. ¿Han sometido al sistema a análisis de riesgos de TI? (de ser el caso pedir la documentación resultante) | No lo han realizado | Esto refleja claramente el poco conocimiento sobre el sistema de la empresa. |
| 25. ¿Cuentan con procesos o políticas de manejo de TI? | No cuentan | Esto puede dar paso a problemas a la gestionar el inventario ofimático de la empresa. |
| 26. ¿Tienen documentados estos procesos? | No tienen | |
| 27. ¿Han definido un comité de TI?, de no ser el caso, ¿Quién toma las decisiones relacionadas a proyectos de TI? | No cuentan con un comité, las decisiones las toma el gerente | Este punto es preocupante, puesto que es implícito que las decisiones se toman únicamente desde un enfoque administrativo, dejando de lado el tema técnico que es necesario para la relación calidad – precio de las nuevas adquisiciones. |

| | | |
|---|---|---|
| 28. ¿Cuentan con planes de contingencia para afrontar riesgos de TI? | No cuentan | Esto implica un riesgo grave para la continuidad del negocio, debido a la incapacidad de afrontar incidentes por su cuenta siempre requerirán el apoyo de terceros. |
| **Conclusiones:** Tras llevar a cabo la entrevista se entiende que los integrantes de la empresa en general se pueden clasificar como usuarios comunes, puesto que entienden poco o nada sobre el sistema informático que utilizan y la evidente dependencia de terceros para solucionar problemas relacionados al mismo, esto es un problema que requiere de atención inmediata, ya que a pesar de que el sistema se mantiene en funcionamiento y la continuidad de la empresa no se ha visto en riesgo, hay una alta probabilidad de que el sistema sufra una falla catastrófica a medio o largo plazo debido a una gestión deficiente de los recursos de TI. | | |

Anexo 2: Guía de entrevista encargado de TI

Elaborado por: Jorge Bonilla

La siguiente entrevista presenta información sobre el sistema de facturación de la empresa, esto con el objetivo de comprender como trabaja la empresa en el área de ventas.

**Guía de entrevista**

**Objetivo:** Recolectar información sobre el funcionamiento del sistema informático.

**Sujeto de estudio:** Ferretería “Su Casa”

**Actividad comercial:** Comercialización de productos de ferretería, hogar, acabados y materiales de construcción

**Entrevistado:** Ing. Cristóbal Paredes **Cargo que ocupa:** Asistencia Sistema Contable (Servicios)

**Entrevistador:** Jorge Bonilla

**Fecha y hora de la entrevista:** 17/04/2023 14h00

| **Pregunta** | **Respuesta** | **Observaciones** |
|---|---|---|
| 1. En resumen, ¿Cómo funciona el sistema que brinda a la empresa? | Es un Software Contable para la Industria y Administrativo en base de datos que le ayuda a generar documentos electrónicos y a controlar Inventarios, clientes, proveedores, cxc, cxp, bancos, contabilidad, anexos y nómina. Trabaja con tecnología Cliente Servidor y se conecta mediante ODBC. | El servidor es el activo más valioso de la empresa, por ende, es el objetivo principal de los atacantes. |

| | | |
|---|---|---|
| 2. Describa a detalle el ciclo de vida del sistema que brinda a la empresa | Se instala la aplicación por cada maquina solo en el servidor se instala la aplicación y la BD. Se configura en el Windows ciertas condiciones y se conecta a la BD mediante ODBC en una RED LAN. | El sistema se mantiene dentro de la red, no es posible acceder a ella por medios inalámbricos lo que representa mejor seguridad. |
| 3. ¿El sistema está diseñado a medida para la empresa? | Es Software es un sistema Estándar no se ha hecho personalizaciones adicionales. | Es un software seguro, además de contar con licencia. |
| 4. ¿La instalación del sistema es centralizada o en el escritorio de cada cliente? | Se instala la aplicación por máquina. | Esto garantiza la continuidad de las operaciones, si una terminal cae no afecta a las demás. |
| 5. ¿Cuál es el motor de base de datos que utiliza el sistema? | El sistema es de Base de Datos, utilizamos la base de Sybase Central SQL Anywhere 12. | |
| 6. ¿Con que tecnología está programado el back end? | Cliente – Servidor conector OBDC | |
| 7. ¿Con que tecnología está programado el front end? | Cliente – Servidor conector OBDC | |
| 8. ¿Con que sistemas operativos | Cualquier versión de SO de Windows | Esto representa posibles brechas de seguridad, el uso de SO antiguos o |

| | | |
|---|---|---|
| es compatible el sistema? | | sin soporte es de las mejores formas para infiltrarse a una red. |
| 9. ¿Para cuantos usuarios está diseñado el sistema? | Es multiusuario ilimitado a todos usuarios que estén en RED LAN | |
| 10. ¿Cuántas interfaces tiene el sistema?, describa la funcionalidad de cada una dividir o borrar | Módulos varios, pero Interfaces 1 adicional para el módulo de Facturación Electrónica. Existe el Generador (genera en archivos xml los documentos) y el firmador (Captura esos movimientos y firma y envía al Web Service del SRI) | |
| 11. ¿Qué tipo de archivos procesa el sistema? | XML, TXT, XLS, DOC, DBF | |
| 12. ¿Cuántas bases de datos maneja el sistema?, describa cada una | Una sola BD, contiene toda la información de los módulos. | El uso de una sola BD implica riesgo para toda la información de la empresa |
| 13. ¿El sistema cuenta con controles para el ingreso de datos? | Si mantiene información como por ejemplo Usuario, fecha, hora en cada módulo. | |

| | | |
|---|---|---|
| 14. ¿El sistema cuenta con medidas de seguridad? | Si la BD tiene seguridades de ingreso además de los Backups y control de usuarios | |
| 15. ¿El sistema está seguro contra inyecciones SQL? | Si, cuenta con usuario y clave para ingreso a la BD | |
| 16. ¿Cuál es el método de autenticación del sistema? | Usuario y clave | |
| 17. ¿El sistema ha pasado por pruebas de seguridad?, ¿Cuáles?, ¿Las ha superado? | No responde | |
| 18. ¿Cuentan con un plan de continuidad para el sistema? | Hay Backups se los puede recuperar y reinstalar el sistema, pero los Backups están dentro del mismo disco duro no hay de forma externa. | Mantener el respaldo en el mismo almacenamiento de la base operativa solo ocupa más espacio, no funciona como medida de seguridad. |
| 19. ¿El sistema cuenta con un protocolo de respaldo automático? | De nuestra parte hemos indicado que saquen respaldos, pero ya es responsabilidad de la empresa ir sacando en otro medio | Señal clara de la gestión poco eficiente de los recursos de TI. |

| | | |
|---|---|---|
| 20. ¿Cómo retoman las operaciones en caso de inconvenientes? | Hay varios casos, pero uno de ellos es instalar la BD en otra maquina diferente al servidor y activar para que los otros clientes se conecten a la BD | |
| 21. ¿Cuál es su tiempo de respuesta ante fallos del sistema? | A más tardar 24 horas. En la mayoría de casos es inmediata. | |

Anexo 3:Guía de entrevista proveedor sistema de facturación

Elaborado por: Jorge Bonilla

La siguiente matriz de observación presenta información sobre las actividades y procesos de la empresa, la observación se realizó en base practicas comunes de ITIL v4 y COBIT 5.

**Matriz de observación**

**Objetivo:** Recolectar información sobre el funcionamiento del sistema informático.

**Sujeto de estudio:** Ferretería "Su Casa"

**Actividad comercial:** Comercialización de productos de ferretería, hogar, acabados y materiales de construcción

| No | Aspectos a evaluar | Cumple | Cumple parcialmente | No cumple | Observaciones |
|---|---|---|---|---|---|
| **1** | Identifican los riesgos de TI y establecen un proceso para evaluarlos y gestionarlos. | | | **X** | Poco o nada entienden de los riesgos que corre el sistema y de la amenaza potencial que estos representan para la continuidad del negocio. |
| **2** | Establecen un marco de gestión de riesgos de TI. | | | **X** | No cuentan con ningún plan para afrontar vulnerabilidades del sistema, toman acción cuando el sistema sufre fallos. |
| **3** | Gestionan los riesgos de TI en todas las fases del ciclo de vida del servicio. | | **X** | | Cámaras de seguridad salvaguardan la integridad de los equipos ofimáticos, mantienen a la vista los equipos durante la jornada, poca protección de los equipos, sobre todo periféricos. |
| **4** | Realizan análisis de riesgos para identificar los puntos vulnerables de la organización. | | | **X** | A nivel de empresa desconocen las vulnerabilidades del sistema y no consideran necesario un análisis de las mismas. |

| | | | | | |
|---|---|---|---|---|---|
| **5** | Establecen medidas de control para reducir la probabilidad y el impacto de los riesgos de TI. | | | **X** | El plan de acción es solicitar soporte técnico cuando existe algún fallo. |
| **6** | Establecen un plan de continuidad del negocio y de recuperación ante desastres para minimizar la interrupción de los servicios de TI. | | | **X** | Dado que jamás lo han requerido no consideran que sea necesario. |
| **7** | Realizan pruebas de seguridad y continuidad del negocio para garantizar la efectividad de los planes establecidos. | | | **X** | |
| **8** | Gestionan los riesgos relacionados con la privacidad de los datos y cumplir con las regulaciones y leyes aplicables. | | **X** | | Mantienen la confidencialidad dentro de la empresa, no se divulga información relacionada a la empresa sin antes se apruebe por la administración. |
| **9** | Llevan a cabo capacitaciones para el personal en la gestión de riesgos de TI | | | **X** | Lo hicieron únicamente cuando el sistema fue implementado, para nuevos usuarios se recurre a la experiencia del resto del personal. |
| **10** | Desarrollan y mantienen un plan de gestión de riesgos de TI. | | | **X** | A raíz del desconocimiento de los riesgos de TI la ausencia de un plan de es evidente. |
| **11** | Gestionan la disponibilidad y las solicitudes de parte de los usuarios para el acceso a los servicios | **X** | | | El sistema de la empresa satisface los requerimientos de la misma, existen suficientes recursos de TI para solventar la demanda del negocio. |

| |
|---|
| **Conclusiones:** El sistema en cuanto a su funcionamiento es más cercano a lo domestico que a lo empresarial, esto debido al tamaño de la empresa y su actividad comercial, sin embargo, de aumentar el tamaño de la empresa se volverá necesario mejorar el sistema en todos los aspectos, incluido el apartado de gestión de riesgos de TI, debido a que la demanda del negocio incrementa al igual que las amenazas potenciales, que en la actualidad se limitan a errores de gestión y mal uso de los dispositivos. |

Anexo 4: Ficha de observación

Elaborado por: Jorge Bonilla

Las siguientes fichas bibliográficas presentan información fundamental sobre el tema propuesto, contienen los lineamientos generales sobre gestión de riesgos de TI de las metodologías propuestas.

| Identificación del texto |
|---|
| Autor(es): AXELOS Limited<br>Título: ITIL 4 Foundation Material - Participante<br>Editorial: ITpreneurs<br>Palabras clave: seguridad de la información, confidencialidad, integridad, disponibilidad, autenticidad, vulnerabilidades, amenazas, riesgos, controles de seguridad, gestión de riesgos, cumplimiento normativo, incidentes de seguridad |
| **Síntesis de contenido** |
| **Práctica: Gestionar la seguridad de la información**<br>Esta práctica tiene como objetivo asegurar que los activos de información de la organización estén protegidos. Para ello, es necesario establecer controles de seguridad adecuados que garanticen la confidencialidad, integridad, disponibilidad y autenticidad de la información. Se deben identificar las vulnerabilidades y amenazas existentes, evaluar los riesgos y aplicar los controles de seguridad adecuados. Además, se deben cumplir con los requisitos legales y normativos aplicables y responder adecuadamente ante incidentes de seguridad que puedan surgir. |
| **Conclusión** |
| El activo más importante para las organizaciones en la información, sin esta el negocio no puede existir, la prioridad en la gestión de riesgos es mantener segura y disponible la información de forma que la organización pueda acceder a ella sin mayores inconvenientes. |
| **Aporte al proyecto** |
| Esto permite tener clara la importancia de la seguridad de la información cuando de servicios de TI se trata y como esto afecta a la organización. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 5: Ficha bibliográfica N°1

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: ITIL 4 Foundation Material - Participante<br>Editorial: ITpreneurs<br>Palabras clave: proveedores, socios, contratos, acuerdos de nivel de servicio, colaboración, comunicación, gestión de riesgos, mejora continua, satisfacción del cliente |
| **Síntesis de contenido** |
| **Práctica: Gestionar las relaciones**<br>Esta práctica tiene como objetivo establecer y gestionar las relaciones con los proveedores y socios de la organización. Es necesario establecer contratos y acuerdos de nivel de servicio adecuados, así como fomentar la colaboración y la comunicación efectiva. La gestión de riesgos y la mejora continua deben estar presentes en todas las relaciones, y se debe garantizar la satisfacción del cliente en todo momento. |
| **Conclusión** |
| No existe individuo u organización capaz de desarrollarse de forma aislada, debido a esto es importante mantener buenas relaciones con todas las partes involucradas, así se evitan brechas de seguridad y se promueve el desarrollo. |
| **Aporte al proyecto** |
| Esto ayuda a comprender que una buena práctica en cuanto a gestión de riesgos de TI es mantener buenas relaciones con todas las partes interesadas, permitiendo mantener una buena comunicación en cuanto a necesidades y requerimientos de TI se trata. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 6: Ficha bibliográfica N°2

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: ITIL 4 Foundation Material – Participante<br>Editorial: Itpreneurs<br>Palabras clave: continuidad del servicio, interrupciones, crisis, planes de continuidad, evaluación de impacto en el negocio, gestión de riesgos, estrategias de recuperación, pruebas y mantenimiento |
| **Síntesis de contenido** |
| **Práctica: Gestionar la continuidad del servicio**<br>Esta práctica tiene como objetivo garantizar que los servicios de la organización puedan continuar operando en caso de interrupciones o crisis. Para ello, se deben establecer planes de continuidad, evaluar el impacto de los incidentes en el negocio, identificar las estrategias de recuperación adecuadas y realizar pruebas y mantenimiento regularmente. La gestión de riesgos es esencial para identificar y mitigar los riesgos asociados a la interrupción del servicio. |
| **Conclusión** |
| Un plan de contingencia es necesario para evitar interrupciones durante las actividades de la organización, esto a su vez crea una imagen de solidez para la organización ante los clientes manteniendo la fidelidad de los mismos |
| **Aporte al proyecto** |
| Este apartado aclara la necesidad de contar con planes de contingencia que ayuden a la organización a mantener los servicios y por ende la continuidad del negocio. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 7: Ficha bibliográfica N°3

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: Digital and IT Strategy<br>Editorial: TSO<br>Palabras clave: avance tecnológico, riesgos, vulnerabilidades, practicas, oportunidades. |
| **Síntesis de contenido** |
| **Gestión del riesgo estratégico:**<br>El avance tecnológico representa oportunidades que pueden impulsar una organización o destruirla, todo depende de cómo se gestionen los riesgos tanto a nivel táctico como estratégico, logrando combatir amenazas y vulnerabilidades asegurando el éxito de la organización.<br>Riesgo se define como todo evento con potencial de causar daño, perdida o dificultar el logro de objetivos, otra forma de definirlo es como la incertidumbre del resultado, pudiendo ser estos positivos o negativos, donde los resultados positivos se los conoce como oportunidades.<br>La gestión de riesgos tiene como objetivo asegurar que la organización comprenda los riesgos y los enfrente de forma efectiva, para lo cual se recurre a las siguientes practicas:<br>• Realizar análisis ambientales para identificar y enmarcar los riesgos<br>• Determinar y documentar la capacidad de riesgo y el apetito de riesgo de la organización<br>• Documentar las políticas de gestión de riesgos<br>• Identificar, analizar y evaluar los riesgos<br>• Determinar el tratamiento de riesgo apropiado<br>• Identificar los desencadenantes y los propietarios del riesgo<br>• Garantizar que las estrategias de riesgo se implementen de manera adecuada. |
| **Conclusión** |
| Dadas las condiciones de la actualidad, en las que la tecnología evoluciona cada día más rápido, es necesario que las organizaciones aprendan como adaptarse a los cambios constantes y en ocasiones bruscos del medio en el que se desenvuelven, por ello llevar a cabo la gestión de riesgos es un pilar fundamental para mantener la continuidad del negocio y lograr los objetivos planteados como organización. |
| **Aporte al proyecto** |
| Contar con la capacidad de identificar riesgos y oportunidades es un aspecto importante para formular una estrategia efectiva para la gestión de riesgos de TI. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 8: Ficha bibliográfica N°4

Elaborado por: Jorge Bonilla

| Identificación del texto |
|---|
| Autor(es): AXELOS Limited<br>Título: Digital and IT Strategy<br>Editorial: TSO<br>Palabras clave: Tecnología, riesgos, paradigma, procesos, modelos |
| **Síntesis de contenido** |
| **Manejo de riesgos en organizaciones digitales:**<br>La gestión de riesgos depende en gran medida de del paradigma de transformación de la organización. En el caso de la organización recurre a un paradigma basado en procesos puede comenzar evaluando su estado actual y que desea a futuro identificando los riesgos que implica esta transición, mientras que con un paradigma basado en modelos inicia identificando casos comerciales potenciales y sus riesgos asociados, entre otros escenarios tenemos:<br>• Uso de nueva tecnología, esta puede quedar obsoleta rápidamente<br>• Nuevo modelo de negocio<br>• Tecnología en etapa temprana de desarrollo<br>• Uso de nuevas tecnologías por parte de empleados y clientes generando fallos<br>• Uso de Internet de las cosas (IoT), puede exponer los datos<br>• La amenaza constante de ciberdelincuentes, que por lo general encuentran y explotan vulnerabilidades rápidamente.<br>Además, hay que tener en cuenta que los activos en una organización digital deben protegerse en todas partes, además de un compromiso de todos los interesados, logrando mitigar los riesgos. |
| **Conclusión** |
| Para una organización es importante mantenerse en el tiempo y expandirse, esto implica riesgos que se originan por múltiples razones, es por esto que lo más importante a la hora de gestionar riesgos es proteger los activos e involucrar a todas las partes interesadas, minimizando así las brechas de seguridad y garantizando la continuidad del negocio. |
| **Aporte al proyecto** |
| Esto ayuda a identificar el contexto de la organización con la que se trabaja, facilitando así el diseño de una metodología para gestión de riesgos de TI. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 9: Ficha bibliográfica N°5

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: Digital and IT Strategy<br>Editorial: TSO<br>Palabras clave: Tecnología, riesgos, modelo de negocio, probabilidad, beneficio, resultados, relación, datos |
| **Síntesis de contenido** |
| **Identificación de riesgos y oportunidades:**<br>La tecnología brinda oportunidades que pueden o no beneficiar a la organización, es por ello que la gestión de riesgos es necesaria para determinar que oportunidades traerán beneficios. La gestión de riesgos permite estratégicamente a los lideres a:<br>• Identificar los riesgos positivos y negativos de cada oportunidad<br>• Establecer la probabilidad de riesgos positivos y negativos<br>• Indicando lo que la organización debería hacer para evitar riesgos negativos<br>• Indicar qué acción es más probable que asegure un resultado positivo<br>• Evaluar el resultado neto de todos los riesgos negativos y positivos.<br>Para comprender y gestionar riegos se usan marcos como: PESTLE, VUCA, TECOP, OODA, etc.<br>**Riesgos disruptivos:**<br>Tipo de riesgo con potencial de alterar el modelo de negocio de la organización, surge por la adopción de nuevas tecnologías por parte de la competencia, alterando así la dinámica de la industria, o en otros casos agotar los recursos sin lograr un avance significativo.<br>**Riegos de innovación:**<br>Innovar conlleva riesgos, por ello el desarrollo y prueba se lo lleva a cabo en entornos controlados, evaluando los nuevos productos y mantenerse competitivos.<br>**Riesgos de ciberseguridad:**<br>Estos surgen en función del tamaño de la organización y los datos que estas acumulen, a mayor volumen de información mayor interés por porte de ciberdelincuentes.<br>**Riesgos de participación:**<br>Estos surgen a partir de relaciones débiles con las partes interesadas, ya sean estas internas o externas, creando brechas de seguridad que bloquean al área de TI |
| **Conclusión** |
| Cuando un riesgo aparece el cómo se lo afronta lo convierte en oportunidad, esto no significa que todo riesgo tiene potencial de oportunidad, si no se identifican correctamente los resultados pueden ser catastróficos para la organización, siendo el mejor de los casos un cambio en el modelo de negocio. |
| **Aporte al proyecto** |
| Poder identificar la clase de riesgo a la que se enfrenta la organización facilita también la identificación de oportunidades con potencial de traer beneficios a la organización. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 10: Ficha bibliográfica N°6

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: Digital and IT Strategy<br>Editorial: TSO<br>PALABRAS CLAVE: riesgos, impacto, costo |
| **Síntesis de contenido** |
| **Registro de riesgos:**<br>Es el producto de la identificación de riesgos exitosa, una lista de riegos identificados y ordenados por su prioridad, estado actual y su historial es deber del alto ejecutivo, facilitando así trabajos de auditoría.<br>**Análisis de riesgos:**<br>Este puede ser cualitativo o cuantitativos, cuando se habla de cualitativo se refiere a la probabilidad de ocurrencia de un riesgo y su impacto, mientras que el cuantitativo se centra en asignar un valor monetario.<br>**Disparadores de riesgo:**<br>Se refiere a eventos con el potencial de convertir un riesgo en problema, o causar que el riesgo cambie de categoría. |
| **Conclusión** |
| Para lograr una gestión de riesgos adecuada es fundamental llevar la documentación pertinente, además de esto tener claro la clase de riesgo y lo que este puede causar, así como los factores que los crean o desencadenan. |
| **Aporte al proyecto** |
| Comprender los pasos posteriores a la identificación de riesgos es un punto clave para el buen funcionamiento y gestión de servicio de TI en una organización, permitiendo a esta responder de forma adecuada a los riesgos de TI. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 11: Ficha bibliográfica N°7

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: Digital and IT Strategy<br>Editorial: TSO<br>Palabras clave: riesgos, actitud, postura, capacidad de riesgo, apetito de riesgo |
| **Síntesis de contenido** |
| **Mentalidad y cultura informadas sobre el riesgo:**<br>El aspecto más importante sobre la gestión de riesgos es el cómo reacciona la organización ante los riesgos, esto implica definir la postura y la actitud antes los mismos. Cuando de postura se habla de cómo la organización identifica, analiza, planifica responde y gestiona el riesgo, esto incluye determinar la capacidad y apetito de riesgo de la organización.<br>La actitud hace referencia a cómo responde la organización a los riesgos, esta actitud va desde la aversión, pasando por la búsqueda y tolerancia de riesgos, hasta llegar a la neutralidad, siendo esta ultima la actitud ideal ante los riesgos. |
| **Conclusión** |
| El resultado de una organización solida es la actitud frente a los riesgos, a mayor resiliencia mejor mentalidad a nivel organizacional a la hora de enfrentar y neutralizar riesgos, logrando así mantener la continuidad del negocio y permanecer en el tiempo. |
| **Aporte al proyecto** |
| Entender el rol que juega el ejecutivo de la organización en relación a los riesgos de TI es un punto importante a la hora de diseñar una metodología para gestión de riesgos de TI, pues está en manos del alto mando encaminar a todas las partes de la organización hacia un modelo sostenible en lo que a TI se refiere. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 12: Ficha bibliográfica N°8

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): AXELOS Limited<br>Título: Digital and IT Strategy<br>Editorial: TSO<br>Palabras clave: riesgos, actitud, postura, capacidad de riesgo, apetito de riesgo |
| **Síntesis de contenido** |
| **Gestión de riesgos:**<br>La meta de la práctica de la gestión de riesgos es asegurar que la organización comprenda y maneje los riesgos de manera efectiva, esto con fin de garantizar la sostenibilidad continua de la organización y crear valor para sus clientes. La gestión de riesgos es una parte integral de todas las actividades de la organización.<br>Para ello se sigue la siguiente cadena de valor:<br>• Plan: Contar con una estrategia e insumos necesarios para afrontar los riesgos.<br>• Mejorar: Cualquier iniciativa de mejora debe ser controlada y evaluada por la gestión de riesgos.<br>• Comprometerse: Identificar las partes interesadas clave y optimizar su participación en función del apetito por riesgo o perfiles de riesgo.<br>• Diseño y transición: Productos y servicios deben ser diseñados para abordar riesgos priorizados. Cuando un nuevo producto o servicio es presentado, trae consigo nuevos riesgos que deben ser evaluados antes de aprobar el cambio.<br>• Obtener/construir: La gestión de riesgos debe informar las decisiones sobre la obtención o creación de nuevos productos, servicios o componentes de servicios.<br>• Entregar y apoyar: Consiste en garantizar que la entrega de productos y servicios se mantenga al nivel acordado, gestionando los eventos en base a los riesgos que se introducen. |
| **Conclusión** |
| Para lograr la continuidad del negocio es necesario entender que la gestión de riesgos es un elemento clave, puesto que los riesgos están presentes en todas las áreas de la organización y afrontarlos de forma efectiva permite seguir entregando valor para las partes interesadas. |
| **Aporte al proyecto** |
| Este apartado ayuda a comprender como la gestión de riesgos debe apoyar la creación de valor en la organización, sobre todo cuando de nuevos productos y servicios se trata. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 13: Ficha bibliográfica N°9

Elaborado por: Jorge Bonilla

| Identificación del texto |
|---|
| Autor(es): ISACA<br>Título: COBIT 5 para riesgos<br>Editorial: ISACA<br>Palabras clave: Creación de valor, riesgos, objetivo, recursos, beneficios |
| **Síntesis de contenido** |
| **Objetivo de gobierno: Creación de valor.**<br>Las empresas existen para crear valor para sus accionistas, este es su objetivo principal, crear valor significa obtener beneficios con pocos recursos, mientras se optimiza el riesgo.<br>Según las partes interesadas la creación de valor puede tener un significado diferente y en ocasiones conflictivo.<br>**Creación de valor:**<br>• Realización de beneficios<br>• Optimización de riesgos<br>• Optimización de recursos |
| **Conclusión** |
| No importa el rubro del negocio, la creación de valor es la única razón de existir de una empresa, pero esto conlleva riesgos, los cuales surgen en función de las necesidades de las partes interesadas, por lo cual es importante gestionar el riesgo a la par de la creación de valor. |
| **Aporte al proyecto** |
| Esta definición sobre la creación de valor contribuye a entender por qué surgen los riesgos en una organización y porque se deben gestionarlos, dejando claro además que los riesgos son una parte inherente de todo proceso para crear valor por parte de una organización. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 14: Ficha bibliográfica N°10

Elaborado por: Jorge Bonilla

Identificación del texto

Autor(es): ISACA
Título: COBIT 5 para riesgos
Editorial: ISACA
Palabras clave: Riesgo, negocio, operaciones, TI, impacto al negocio.

**Síntesis de contenido**

**Riesgo:**
Se define el riesgo como la combinación de la probabilidad de un evento y sus consecuencias, las cuales se reflejan cuando los objetivos de la empresa no se logran. COBIT 5 define el riesgo de TI como un riesgo de negocio, específicamente asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en la empresa. El riesgo de TI consiste de eventos relacionados a TI con potencial de impactar el negocio, este puede darse con frecuencia e impactos inciertos, representando retos para la organización.

**Categorías de riesgo:**

- Riesgo en la habilitación de valor/beneficio de TI: Asociado con las oportunidades perdidas de utilización de la tecnología con el fin de mejorar la eficiencia o efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocio.
- Riesgo en la entrega de programas y proyectos de TI: Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas, generalmente bajo la forma de programas y proyectos que forman parte de portafolios de inversión.
- Riesgo en la entrega de operaciones y servicios de TI: Asociado con todos los aspectos del negocio como el desempeño normal de sistemas y servicios de TI, los que pueden destruir o reducir el valor para la empresa.

Estas categorías pertenecen a riesgos decrecientes (dejar de ganar y perder), su contraparte, creciente (ganar y preservar), es necesario mantener presente esta dualidad a la hora de tomar decisiones relacionadas al riesgo.

- Crear o preservar valor: La información y la tecnología bien gobernadas y gestionadas entregan beneficios al negocio y preservan el valor
- Dejar de ganar valor: La información y la tecnología mal gobernadas y gestionadas destruyen valor o fallan la entrega de beneficios.

**Conclusión**

El riesgo de TI según COBIT 5, está ligado completamente a la existencia de TI en la empresa, el hecho de que la tecnología forme parte de la organización implica riesgos, esto causado por oportunidades desaprovechadas, entre otras causas

**Aporte al proyecto**

| |
|---|
| Esta sección contribuye a entender los riesgos de TI en base a COBIT 5 y contrastar con otras metodologías. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 15: Ficha bibliográfica N°11

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): ISACA<br>Título: COBIT 5 para riesgos<br>Editorial: ISACA<br>Palabras clave: Función, gobierno, gestión |
| **Síntesis de contenido** |
| **Alcances de COBIT 5:**<br>• Perspectiva de la función de riesgos: La optimización de riesgos es un objetivo clave de valor, COBIT 5 considera al gobierno y a la gestión del riesgo como parte del gobierno y gestión global de TI en la organización.<br>• Perspectiva de la gestión de riesgos: Comprende el gobierno y la gestión, en si es como identificar, analizar y responder al riesgo, esto implementando procesos principales del riesgo (EDM03 Asegurar la optimización del riesgo y APO12 Gestionar el riesgo).<br>En relación a los riesgos, COBIT 5 se focaliza en aplicar los catalizadores de COBIT 5 hacia el riesgo, esto desde la perspectiva de la función de riesgos, en otras palabras, por medio de los catalizadores de COBIT 5. |
| **Conclusión** |
| La gestión de riesgos de TI tiene claros limites, esto permite saber cómo gestionar riesgos de manera optima |
| **Aporte al proyecto** |
| Esto contribuye a entender las limitaciones de COBIT 5 relacionado a gestión de riesgos, dejando claro que elementos tomar. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 16: Ficha bibliográfica N°12

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): ISACA<br>Título: COBIT 5 para riesgos<br>Editorial: ISACA<br>Palabras clave: Principios, objetivos, catalizadores, fases. |
| **Síntesis de contenido** |
| **Aplicar los principios de COBIT 5 a la gestión de riesgos:**<br>COBIT 5 se basa en 5 principios:<br>• Satisfacer las necesidades de los interesados: El gobierno y la gestión de riesgos tienen como objetivo garantizar que los objetivos de la empresa se logren, la optimización de riesgos es uno de los tres componentes de la creación de valor.<br>• Cubrir la empresa de extremo a extremo: COBIT 5 cubre los catalizadores de gobierno y gestión, además de describir las fases requeridas de gobierno y gestión de riesgo.<br>• Aplicar un marco integrado: COBIT 5 se alinea con los principales marcos y estándares de gestión de riesgos.<br>• Posibilitar un enfoque holístico: COBIT 5 identifica todos los elementos interrelacionados de los catalizadores necesarios para proporcionar el gobierno y la gestión de forma adecuada.<br>• Separar gobernanza de administración: COBIT 5 distingue entre el gobierno del riesgo y las actividades de la gestión de riesgos. |
| **Conclusión** |
| Para poder gestionar riesgos es necesario contar con principios a seguir, todo con el fin de que la creación de valor se logre y se mitiguen los riesgos a la vez. |
| **Aporte al proyecto** |
| Entender los principios de COBIT 5 relacionados a la gestión de riesgos es necesario para contrastar con los principios de otras metodologías, para luego establecer los principios en común en busca de una guía más precisa. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 17: Ficha bibliográfica N°13

Elaborado por: Jorge Bonilla

| Identificación del texto |
| --- |
| Autor(es): ISACA<br>Título: COBIT 5 para riesgos<br>Editorial: ISACA<br>Palabras clave: Principios, objetivos, catalizadores, fases. |
| **Síntesis de contenido** |
| **Escenarios de riesgo:**<br>Un escenario de riesgo es la descripción de un posible evento que de ocurrir tendrá un impacto incierto en el logro de los objetivos de la empresa, este puede ser positivo o negativo.<br>Los escenarios de riesgo se pueden derivar por medio de dos mecanismos diferentes:<br>• Enfoque descendente: Comienza desde los objetivos de la empresa.<br>• Enfoque ascendente: Se base en una lista de escenarios genéricos para definir escenarios de riesgo relevantes.<br>Estos enfoques son complementarios, por loque se deben utilizar de forma simultánea. Los escenarios de riesgo de riesgo deben ser relevantes y estar vinculados a los riesgos reales del negocio, el uso de un conjunto de ejemplos escenarios de riesgos genéricos es de ayuda para identificar el riesgo. |
| **Conclusión** |
| Conocer los posibles escenarios de riesgo que pueden aparecer es fundamental para tomar un curso de acción, incrementando la efectividad de la gestión de riesgos y minimizando el impacto de estos. |
| **Aporte al proyecto** |
| Contar una guía sobre los posibles escenarios de riesgo es un punto importante para el desarrollo de una metodología para gestión de riesgos, pues estos representan una pauta importante. |
| **Nombre del investigador** |
| Jorge Bonilla |

Anexo 18: Ficha bibliográfica N°14

Elaborado por: Jorge Bonilla

## Anexo 19: Plan de procedimientos preventivos

## Contenido

## Introducción:

El presente documento define el plan de procedimientos preventivos para problemas con los activos de TI de la empresa, los procedimientos descritos a continuación buscan brindar una guía para el cuidado de los activos de TI, evitando en la medida de lo posible incidentes que detengan parcial o totalmente las actividades de la empresa.

## Alcance:

El plan de procedimientos preventivos incluye los activos identificados, sus componentes y los problemas relacionados a los mismos, acciones a ejecutar para prevenirlos, además de identificar seguros y proveedores de inventario ofimático.

### 1. Problemas y procedimientos preventivos para PCs

| Componente | Problema | Procedimientos | Seguros | Proveedores |
|---|---|---|---|---|
| CPU | Sobrecalentamiento | • Control de temperatura<br>• Mantenimiento preventivo<br>• Alimentación estable<br>• Firmware y drivers actualizados<br>• Seguridad informática<br>• Protocolo de uso<br>• Seguridad física<br>• Inventariado y etiquetado<br>• Capacitación | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>• Seguros Unidos – Su PYME | • SagaPC<br>• Novicompu<br>• Smart PC Store<br>• La casa del computador |
| | Fallos de ventiladores | | | |
| | Fallo de la fuente de poder | | | |
| | Pantallazo azul | | | |
| | Bloqueo del sistema | | | |
| | Error de arranque | | | |
| | Bajo rendimiento | | | |
| | Ruido excesivo del ventilador | | | |
| | Fallas de la tarjeta madre | | | |
| | Puertos inoperables | | | |
| | Fallas de procesador | | | |

| | | | | |
|---|---|---|---|---|
| | Procesador incompatible<br>Fallos de disco duro<br>Fallos de memoria RAM<br>Fallos de tarjeta gráfica<br>Fallos de la fuente de poder<br>Fallos de la tarjeta de red<br>Fallas de la BIOS<br>Robo o perdida | • Respaldo de datos | | |
| Monitor | Pixeles muertos<br>Problemas de retroalimentación<br>Imagen distorsionada<br>Problemas de encendido<br>Pantalla sin imagen<br>Parpadeo de pantalla<br>Fallos de color o imagen<br>Resolución incorrecta<br>Robo o perdida | • Protocolo de uso<br>• Condiciones ambientales<br>• Actualizar firmware<br>• Golpes y caídas<br>• Mantenimiento preventivo<br>• Seguridad física<br>• Inventariado y etiquetado<br>• Capacitación | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>Seguros Unidos – Su PYME | • SagaPC<br>• Novicompu<br>• Smart PC Store<br>• La casa del computador |
| Teclado | Teclas atascadas<br>Daños por líquidos<br>Cable dañado<br>Fallos de teclas<br>Caracteres incorrectos<br>Tiempo de respuesta prolongado<br>Teclas pegadas o ruidosas<br>Robo o perdida | • Protocolo de uso<br>• Mantenimiento preventivo<br>• Golpes y caídas<br>• Reparación/reemplazo<br>• Seguridad física<br>• Inventariado y etiquetado<br>• Capacitación | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>• Seguros Unidos – Su PYME | • SagaPC<br>• Novicompu<br>• Smart PC Store<br>• La casa del computador |
| Mouse | Cursor con movimiento errático<br>Clics inconsistentes o con retardo | • Protocolo de uso | | • SagaPC |

| | | | | |
|---|---|---|---|---|
| | Desplazamiento irregular<br>Mouse sin respuesta<br>Robo o perdida | • Mantenimiento preventivo<br>• Golpes y caídas<br>• Reparación/reemplazo<br>• Seguridad física<br>• Inventariado y etiquetado<br>• Capacitación | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>• Seguros Unidos – Su PYME | • Novicompu<br>• Smart PC Store<br>• La casa del computador |

Procedimientos preventivos detallados para PCs

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| CPU | Control de temperatura | • Verificar que el equipo se ventile correctamente, comprobar la circulación de aire.<br>• Comprobar el estado de ventiladores y disipadores de calor, limpiarlos de ser necesario.<br>• Con ayuda de herramientas para monitoreo de temperatura verificar los valores térmicos del CPU. | • CPU.<br>• Ventiladores<br>• Disipador de calor<br>• Tarjeta madre compatible.<br>• Fuente de poder | • Sistema operativo actualizado.<br>• Drivers actualizados.<br>• Antivirus y antimalware.<br>• Herramientas de monitoreo y diagnostico (CPU-Z, HWMonitor, CrystalDiskInfo, Seatools, Prime95, AIDA64, |
| | Mantenimiento preventivo | • Definir un periodo regular para el mantenimiento.<br>• Limpiar los componentes internos con ayuda de aire comprimido y brochas, entre los componentes se incluye ventiladores y disipadores de calor. | | |

| | | | | |
|---|---|---|---|---|
| | | • Comprobar el estado de los cables y sus conexiones.<br>• Evaluar el funcionamiento en busca de irregularidades como ruidos extraños o temperatura elevada.<br>• Registrar las actividades realizadas, incluyendo resultados. | | administrador de tareas,).<br>• Software para diagnóstico (Memest86, funciones integradas del sistema operativo) |
| | Alimentación estable | • Comprobar el estado de las toma corrientes, evitar sobrecargar las mismas<br>• Utilizar reguladores de voltaje para prevenir los picos de tensión.<br>• Utilizar UPS para evitar daños por cortes de electricidad<br>• Mantener cables y conexiones eléctricas en buen estado<br>• Reemplazar fuentes de poder defectuosas de ser necesario. | | |
| | Firmware y drivers actualizados | • Definir un periodo regular para las actualizaciones.<br>• Comprobar el estado de firmware y controladores.<br>• Verificar que las versiones disponibles sean compatibles con el hardware en uso.<br>• Actualizar siguiendo las instrucciones del fabricante,<br>• Registrar las actualizaciones ejecutadas y sus novedades. | | |

| | | | | |
|---|---|---|---|---|
| | Seguridad informática | • instalar antivirus y mantenerlo actualizado.<br>• Definir un periodo regular para escaneos de virus y malware.<br>• Capacitar a los usuarios en materia de seguridad informática.<br>• Implementar mecanismos de seguridad como cortafuegos o entre otros para evitar accesos no autorizados.<br>• Ejecutar auditorias de seguridad periódicas en busca de vulnerabilidades y corregirlas | | |
| | Protocolo de uso | • Establecer reglas para los usuarios del inventario ofimático.<br>• Capacitar a los usuarios en materia de instalación y actualización de componentes.<br>• Promover el uso de pulseras antiestáticas a la hora de realizar mantenimientos.<br>• Definir un proceso para reportes de daños físicos o mal funcionamiento. | | |
| | Seguridad física | • Mantener el CPU en una ubicación segura, esta debe permitir el acceso solo a personal autorizado.<br>• La ubicación debe proteger al dispositivo ante situaciones y condiciones adversas.<br>• Utilizar candados para cada CPU<br>• Instalar cerraduras de calidad en el inmueble.<br>• Mantener un sistema de videovigilancia en el inmueble. | | |

| | | | | |
|---|---|---|---|---|
| | Inventariado y etiquetado | • Llevar un inventario actualizado de los CPUs y sus componentes, esto incluye registrar números de serie de los componentes.<br>• Etiquetar claramente los CPUs y sus componentes | | |
| | Capacitación | • Mantener capacitado al personal en materia de seguridad y protección de equipos, hacer énfasis en los riesgos asociados.<br>• Definir un canal de comunicación para reportes de robos o perdidas. | | |
| | Respaldo de datos | • Definir el plan de acción para el respaldo de la información almacenada.<br>• Mantener las copias de seguridad en una locación segura, de preferencia contratar servicios en de almacenamiento en la nube. | | |
| Monitor | Protocolo de uso | • Definir parámetros de encendido y apagado.<br>• Proporcionar instrucciones para configurar brillo y contraste basadas en las especificaciones del fabricante y las necesidades de los usuarios.<br>• Promover el apagado de monitores cuan no estén en uso. | • Monitor<br>• Cable HDMI<br>• Cable de poder<br>• Filtro de luz azul | • Drivers actualizados |
| | Condiciones ambientales | • Mantener los monitores lejos de fuentes de humedad como ventanas abiertas o contenedores de líquidos.<br>• Utilizar fundas protectoras para cubrir los monitores mientras no estén en uso.<br>• Llevar a cabo limpiezas externas periódicamente. | | |

| | | | | |
|---|---|---|---|---|
| | | • Mantener cables y conexiones eléctricas en buen estado | | |
| | Actualizar firmware | • Definir un periodo regular para las actualizaciones.<br>• Comprobar el estado de firmware.<br>• Verificar que las versiones disponibles sean compatibles con el hardware en uso.<br>• Actualizar siguiendo las instrucciones del fabricante. | | |
| | Golpes y caídas | • Definir el procedimiento para transporte seguro de monitores.<br>• Enfatizar sobre la importancia de evitar golpes y caídas. | | |
| | Mantenimiento preventivo | • Definir un periodo regular para el mantenimiento.<br>• Llevar a cabo limpieza externa con ayuda de paños suaves.<br>• Mantener cables y conexiones eléctricas en buen estado<br>• Registrar las actividades realizadas, incluyendo resultados. | | |
| | Seguridad física | • Instalar cerraduras de calidad en el inmueble.<br>• Mantener un sistema de videovigilancia en el inmueble.<br>• La ubicación debe proteger al dispositivo ante situaciones y condiciones adversas. | | |

| | | | | |
|---|---|---|---|---|
| | Inventariado y etiquetado | • Llevar un inventario actualizado de los periféricos, esto incluye el modelo y número de serie.<br>• Etiquetar claramente los periféricos. | | |
| | Capacitación | • Mantener capacitado al personal en materia de seguridad y protección de equipos, hacer énfasis en los riesgos asociados.<br>• Definir un canal de comunicación para reportes de robos o perdidas. | | |
| Teclado | Protocolo de uso | • Definir parámetros para el uso de teclados.<br>• Proporcionar instrucciones sobre el manejo correcto de las teclas, evitando causar daños a las mismas debido a objetos pesados o al uso de objetos punzantes.<br>• Enfatizar sobre la importancia de no consumir bebidas cerca de teclados.<br>• Promover el uso de fundas protectoras mientras los teclados no estén en uso. | • Teclado<br>• Protector de teclado | • Antivirus y antimalware<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo y diagnostico (CPU-Z, HWMonitor) |
| | Mantenimiento preventivo | • Definir un periodo regular para el mantenimiento.<br>• Proporcionar instrucciones para llevar a cabo limpieza externa de forma segura.<br>• Mantener cables y conexiones eléctricas en buen estado<br>• Registrar las actividades realizadas, incluyendo resultados. | | |
| | Golpes y caídas | • Definir el procedimiento para transporte seguro de teclados. | | |

| | | | | |
|---|---|---|---|---|
| | Reparación/reemplazo | • Definir un proceso para reportes de daños físicos o mal funcionamiento.<br>• Definir un proceso de evaluación y diagnóstico de los problemas reportados.<br>• Llevar a cabo la reparación o reemplazo de ser necesario. | | |
| | Seguridad física | • Instalar cerraduras de calidad en el inmueble.<br>• Mantener un sistema de videovigilancia en el inmueble.<br>• La ubicación debe proteger al dispositivo ante situaciones y condiciones adversas. | | |
| | Inventariado y etiquetado | • Llevar un inventario actualizado de los periféricos, esto incluye el modelo y número de serie.<br>• Etiquetar claramente los periféricos. | | |
| | Capacitación | • Mantener capacitado al personal en materia de seguridad y protección de equipos, hacer énfasis en los riesgos asociados.<br>• Definir un canal de comunicación para reportes de robos o perdidas. | | |
| Mouse | Protocolo de uso | • Definir parámetros para el uso de mouses.<br>• Proporcionar instrucciones sobre el manejo correcto de los mouses, evitando causar daños por uso en superficies irregulares o sucias, manipulación indebida del cable.<br>• Enfatizar sobre la importancia de no consumir bebidas cerca de mouses. | • Mouse<br>• Mousepad | • Drivers actualizados<br>• Antivirus y antimalware |

| | | | | |
|---|---|---|---|---|
| | Mantenimiento preventivo | • Definir un periodo regular para el mantenimiento.<br>• Proporcionar instrucciones para llevar a cabo limpieza externa de forma segura.<br>• Mantener cables y conexiones eléctricas en buen estado<br>• Registrar las actividades realizadas, incluyendo resultados. | | |
| | Golpes y caídas | • Definir el procedimiento para transporte seguro de mouses.<br>• Promover el uso de fundas protectoras mientras los mouses son transportados. | | |
| | Reparación/reemplazo | • Definir un proceso para reportes de daños físicos o mal funcionamiento.<br>• Definir un proceso de evaluación y diagnóstico de los problemas reportados.<br>• Llevar a cabo la reparación o reemplazo de ser necesario. | | |
| | Seguridad física | • Instalar cerraduras de calidad en el inmueble.<br>• Mantener un sistema de videovigilancia en el inmueble.<br>• La ubicación debe proteger al dispositivo ante situaciones y condiciones adversas. | | |
| | Inventariado y etiquetado | • Llevar un inventario actualizado de los periféricos, esto incluye el modelo y número de serie.<br>• Etiquetar claramente los periféricos. | | |

| | | | | |
|---|---|---|---|---|
| | Capacitación | • Mantener capacitado al personal en materia de seguridad y protección de equipos, hacer énfasis en los riesgos asociados.<br>• Definir un canal de comunicación para reportes de robos o perdidas. | | |

2. Problemas y procedimientos preventivos para bases de datos

| Componente | Problema | Procedimientos | Seguros | Proveedores |
|---|---|---|---|---|
| Datos | Corrupción de datos | • Respaldo frecuente<br>• Acceso seguro<br>• Accesos no autorizados<br>• Encriptación de datos<br>• Mantenimiento | No disponible | • MicroPlus SQL 2019 |
| | Perdida de datos | | | |
| | Inconsistencia de datos | | | |
| | Accesos no autorizados | | | |
| | Problemas de rendimiento | | | |

Procedimientos preventivos detallados para bases de datos

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| Datos | Respaldo frecuente | • Definir la frecuencia para llevar a cabo copias de seguridad, esto en función del nivel de sensibilidad de los datos.<br>• Elegir el método de respaldo, entre las opciones se incluyen respaldo incremental o respaldo completo, además es necesario contar con la herramienta adecuada en función del método.<br>• Asignar una ubicación segura para almacenar las copias de seguridad, debe ser de rápido acceso para eventos de restauración. | • Servidor sistema de facturación<br>• PCs de ventas<br>• Discos duros<br>• Cables de poder<br>• UPS<br>• Modem<br>• Switches<br>• Cables de red | • Sistema de facturación<br>• Sistema de gestión de base de datos<br>• Sistema operativo (Windows Server 2012)<br>• Antivirus y antimalware |
| | Acceso seguro | • Uso de sistema de autenticación, cada usuario debe tener credenciales individuales.<br>• Establecer permisos y roles en función del cargo o responsabilidad de los usuarios. | | |
| | Accesos no autorizados | • Implementar mecanismos o herramientas de monitoreo en la base de datos para dar seguimiento a los accesos y cambios de datos.<br>• Establecer un sistema de alerta en caso de accesos no autorizados o actividad inusual en la base de datos. | | |

| | | | | |
|---|---|---|---|---|
| | | • Designar personal y recursos para mitigar amenazas relacionadas al acceso no autorizado. | | |
| | Encriptación de datos | • Llevar a cabo un análisis de los datos e identificar los datos sensibles que requieren de encriptación en función de las necesidades de la empresa, determinar el mejor algoritmo de encriptación.<br>• Determinar la técnica necesaria para la encriptación, estas incluyen encriptación de columnas o campos, encriptación de disco o cifrado de conexión, implementarlo junto al método de encriptación.<br>• Mantener las claves de encriptación seguras. | | |
| | Mantenimiento | • Definir un periodo regular para el mantenimiento.<br>• Llevar a cabo tareas para mejorar el rendimiento de la base de datos, estas incluyen organizar índices y optimizar consultas.<br>• Mantener la seguridad de la base de datos con las actualizaciones proporcionadas por el proveedor de la misma.<br>• Gestionar el almacenamiento de la base de datos, evitar que este llegue a su límite | | |

| | | | | |
|---|---|---|---|---|
| | | y afecte al funcionamiento de la base de datos. | | |

3. Problemas y procedimientos preventivos para modem/access point

| Componente | Problema | • Procedimientos | Seguros | Proveedores |
|---|---|---|---|---|
| Interfaces de red | Conexión a internet inestable<br>Baja velocidad<br>Problemas de configuración<br>Problemas de seguridad<br>Problemas de incompatibilidad | • Seguridad de la red<br>• Calidad de servicio<br>• Configuración | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>• Seguros Unidos – Su PYME | • SagaPC<br>• Novicompu<br>• Smart PC Store<br>• La casa del computador<br>• Netlife<br>• CNT |
| Procesador | Conexión a internet inestable<br>Baja velocidad<br>Problemas de configuración<br>Problemas de seguridad<br>Problemas de incompatibilidad | • Control de temperatura<br>• Actualización<br>• Carga de trabajo | | |
| Memoria | Memoria insuficiente<br>Corrupción de datos<br>Actualizar firmware | • Administración<br>• Mantenimiento<br>• Actualización<br>• Capacidad y dimensionamiento | | |
| Sistema operativo | Fallos de firmware<br>Configuración incorrecta<br>Problemas de compatibilidad<br>Problemas persistentes | • Actualización<br>• Seguridad | | |

| | | | | |
|---|---|---|---|---|
| Tabla de enrutamiento | Tabla de enrutamiento incorrecta<br>Problemas de IP<br>Actualizar firmware | • Actualización<br>• Segmentación de red<br>• Enrutamiento estático<br>• Filtrado de rutas<br>• Monitoreo y limpieza | | |
| Firewall | Configuración incorrecta<br>Bloqueo de puertos necesarios<br>Restricciones de acceso<br>Actualizar firmware | • Configuración<br>• Reglas<br>• Actualización<br>• Acceso remoto | | |

Procedimientos preventivos detallados para modem/access point

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| Interfaces de red | Seguridad de la red | • Reemplazar las contraseñas por defecto de modem.<br>• Actualizar el firmware con frecuencia para corregir vulnerabilidades.<br>• Mantener firewalls activos para controlar el tráfico de la red. | • Modem<br>• Cables de red<br>• Tarjetas de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Wireshark, Nagios, Zabbix) |
| | Calidad de servicio | • Distribuir el ancho de banda en función de las necesidades de tráfico.<br>• Definir límites de ancho de banda para cada dispositivo conectado. | | |

| | | | | |
|---|---|---|---|---|
| | | • Dar seguimiento al uso de la red y configurar el modem en base a las necesidades y evitando congestiones. | | |
| | Configuración | • Implementar protocolos de encriptación para la red inalámbrica, estos incluyen WPA2 y WPA3.<br>• Inhabilitar servicios innecesarios, esto para reducir las brechas de seguridad<br>• Mantener una copia de seguridad de la configuración del modem para eventos de fallos. | | |
| Procesador | Control de temperatura | • Ubicar el modem en el entorno adecuado, esta debe estar bien ventilada y fuera del alcance de la radiación solar.<br>• Comprobar regularmente la temperatura del modem con ayuda de herramientas de monitoreo de temperatura.<br>• En caso de ser necesario instalar ventiladores de apoyo. | • Modem<br>• Cables de red<br>• Tarjetas de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Actualización | • Actualizar el firmware con frecuencia para corregir vulnerabilidades.<br>• Mantener actualizado el sistema operativo del modem por motivos de seguridad. | | |

| | | | | |
|---|---|---|---|---|
| | Carga de trabajo | • Identificar los límites de la capacidad del modem, se debe considerar todos los dispositivos conectados.<br>• Aplicar medidas como el balanceo de carga para evitar sobrecargar el modem. | | |
| Memoria | Administración | • Con ayuda de herramientas de monitoreo comprobar regularmente el uso de la memoria.<br>• Eliminar procesos y servicios innecesarios para optimizar el uso de memoria.<br>• Definir límites para el consumo de memoria, evitando que determinadas aplicaciones o servicios acaparen toda la memoria disponible. | • Modem<br>• Cables de red<br>• Tarjetas de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Mantenimiento | • Limpiar la memoria regularmente y liberar procesos innecesarios.<br>• Borrar archivos temporales y cache para liberar espacio.<br>• Realizar revisiones frecuentes en busca de errores de memoria con ayuda de herramientas de diagnóstico y corrección de memoria. | | |
| | Actualización | • Actualizar el firmware con frecuencia para corregir vulnerabilidades. | | |

| | | | | |
|---|---|---|---|---|
| | | • Mantener actualizado el sistema operativo del modem por motivos de seguridad. | | |
| | Capacidad y dimensionamiento | • Identificar los límites de capacidad de la memoria del modem para la carga de trabajo, se debe considerar todos los dispositivos conectados.<br>• Aplicar medidas para optimizar la memoria, estas incluyen configuración de cache y buffer.<br>• Expandir la capacidad de la memoria de ser necesario. | | |
| Sistema operativo | Actualización | • Actualizar el firmware con frecuencia para corregir vulnerabilidades.<br>• Mantener actualizado el sistema operativo del modem por motivos de seguridad.<br>• Mantener una copia de seguridad de la configuración del modem. | • Modem<br>• Cables de red<br>• Tarjetas de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Seguridad | • Reemplazar las contraseñas por defecto de modem.<br>• Actualizar el firmware con frecuencia para corregir vulnerabilidades.<br>• Mantener firewalls activos para controlar el tráfico de la red. | | |
| Tabla de enrutamiento | Actualización | • Actualizar el firmware con frecuencia para corregir vulnerabilidades. | | |

| | | | | |
|---|---|---|---|---|
| | Segmentación de red | • Analizar la estructura de la red para determinar cómo segmentarla.<br>• Segmentar la red con ayuda de subredes o VLAN's, asignar a cada la IP adecuada junto a sus máscaras de subred.<br>• Verificar la configuración de los dispositivos dentro de cada segmento. | • Modem<br>• Cables de red<br>• Tarjetas de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Enrutamiento estático | • Definir las rutas por asignar a la tabla de enrutamiento estática.<br>• Agregar las rutas estáticas mediante la interfaz de administración web o la línea de comandos.<br>• Verificar que las rutas estén correctamente establecidas | | |
| | Filtrado de rutas | • Establecer criterios de filtrado de rutas en función de las necesidades, considerar direcciones de origen y destino, métrica de enrutamiento.<br>• Aplicar las reglas de filtrado como aceptar, denegar y redirigir rutas. | | |
| | Monitoreo y limpieza | • Monitorear la tabla de enrutamiento en busca de rutas duplicadas, incorrectas u obsoletas.<br>• Eliminar las rutas innecesarias mediante la interfaz de administración. | | |

| | | | | |
|---|---|---|---|---|
| | | • Definir un cronograma para el monitoreo y limpieza de la tabla de enrutamiento. | | |
| Firewall | Configuración | • Mediante la interfaz de administración comprobar la verificación predeterminada del firewall, las conexiones entrantes deben estar bloqueadas por defecto.<br>• Habilitar la detección de intrusiones, bloqueo de paquetes sospechosos, entre otras medidas de seguridad. | • Modem<br>• Cables de red<br>• Tarjetas de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Reglas | • Clasificar los servicios y aplicaciones por bloquear o permitir.<br>• Definir reglas para permitir o bloquear tráfico según sea necesario, de ser necesario especificar IP's, puertos, entre otros criterios.<br>• | | |
| | Actualización | • Actualizar el firmware con frecuencia para corregir vulnerabilidades. | | |
| | Acceso remoto | • En la configuración del modem localizar la sección de acceso remoto, modificar las credenciales por defecto.<br>• Establecer credenciales seguras.<br>• Limitar el acceso remoto solo para direcciones IP específicas, utilizar VPN para conexiones más seguras. | | |

4. Problemas y procedimientos preventivos para switches

| Componente | Problema | Procedimientos | Seguros | Proveedores |
|---|---|---|---|---|
| Puertos | Problemas de conectividad | • Configuración predeterminada<br>• Asignación de puertos<br>• Segmentación de red<br>• Control de acceso | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>• Seguros Unidos – Su PYME | • Compumega<br>• Adecomp<br>• Agecom – system<br>• Tecno lap<br>• Alpa tech & store |
| | Direcciones MAC duplicadas | | | |
| | Bajo rendimiento de puertos | | | |
| | VLAN mal configurada | | | |
| Tabla de direccionamiento MAC | Tabla incompleta | • Seguridad de puertos<br>• Control de acceso<br>• Seguridad de VLAN | | |
| | Tabla llena | | | |
| | Direcciones duplicadas | | | |
| Motor de conmutación | Bajo rendimiento | • Mantenimiento<br>• Rendimiento<br>• Seguridad<br>• Disponibilidad | | |
| | Sobrecarga de CPU | | | |
| | Fallos de seguridad | | | |
| Memoria de búfer | Sobrecarga de búfer | • Monitoreo<br>• Gestión de tráfico<br>• Actualización<br>• Configuración | | |
| | Problema de latencia | | | |
| | Desbordamiento de búfer | | | |

Procedimientos preventivos detallados para switches

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| Puertos | Configuración predeterminada | • Mediante la interfaz de administración comprobar la configuración predeterminada de los puertos, esta debe ser segura por defecto.<br>• Inhabilitar funciones y servicios innecesarios en los puertos que no se usan como enlaces troncales. | • Switch<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Asignación de puertos | • Enlistar los dispositivos finales y de red que se conectaran al switch.<br>• Distribuir los puertos en función de las necesidades de la red.<br>• Configurar el modo dúplex y la velocidad para ca puerto en función de los dispositivos conectados. | | |
| | Segmentación de red | • Determinar los segmentos de red y VLANs necesarias.<br>• Asignar puertos a la VLANs y segmentos de red. | | |
| | Control de acceso | • Crear una lista de direcciones MAC seguras y configurar los puertos para conceder el acceso a dichas direcciones.<br>• Implementar un sistema de autenticación para validar las credenciales de los dispositivos antes de permitir su acceso. | | |

| | | | | |
|---|---|---|---|---|
| | | • Habilitar mecanismos de seguridad para detectar y combatir ataques de denegación de servicio o inundación. | | |
| Tabla de direccionamiento MAC | Seguridad de puertos | • Configurar la tabla para que solo permita el acceso a direcciones MAC autorizadas.<br>• Implementar el aprendizaje automático de direcciones MAC.<br>• Definir una Concepto de envejecimiento de direcciones MAC, esto ayudara a eliminar direcciones inactivas automáticamente. | • Switch<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Control de acceso | • Configurar listas de control de acceso (ACLs) para restringir el tráfico en base a las direcciones MAC.<br>• Establecer reglas en las ACLs para permitir o negar el acceso a determinadas direcciones MAC, adicionalmente bloquear direcciones no autorizadas. | | |
| | Seguridad de VLAN | • Segmentar y aislar el grafico de la red asignado puertos a VLANs en función de los requisitos de seguridad y niveles de acceso necesarios.<br>• Configurar el switch para permitir tráfico entre los dispositivos de la misma VLAN. | | |
| Motor de conmutación | Mantenimiento | • Definir un periodo regular para el mantenimiento.<br>• Llevar a cabo pruebas de rendimiento y estabilidad en busca de problemas. | • Switch<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado |

| | | | | |
|---|---|---|---|---|
| | | • Mantener una copia de seguridad actualizada de la configuración de switch. | | • Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |
| | Rendimiento | • Monitorear regularmente el uso de recursos del switch y los errores de conmutación.<br>• Definir umbrales de rendimiento y alertas en caso de superar los límites.<br>• Llevar a cabo análisis de rendimiento en busca de cuellos de botella. | | |
| | Seguridad | • Mantener actualizadas las funciones de seguridad como las ACLs y autenticación de puerto.<br>• Añadir medidas de seguridad adicionales como el filtrado de MAC y protección contra ataques de inundación de tráfico. | | |
| | Disponibilidad | • Habilita la redundancia en el switch con ayuda de métodos como enlaces troncales, protocolos de redundancia, agregación de enlaces.<br>• Mantener fuentes de alimentación alterna para casos de emergencia. | | |
| Memoria de buffer | Monitoreo | • Dar seguimiento al uso y disponibilidad de la memoria.<br>• Definir umbrales para el uso de la memoria de buffer y establecer alertas en caso de superarse los límites.<br>• Analizar periódicamente la memoria de buffer en busca de cuellos de botella. | • Switch<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo actualizado<br>• Herramientas de monitoreo de red |

| | | | | |
|---|---|---|---|---|
| | Gestión de tráfico | • Con ayuda de técnicas de administración de tráfico evitar la congestión de la memoria buffer, entre las técnicas se incluye la clasificación y limitación de tráfico.<br>• Controlar el flujo de tráfico con ayuda de ACLs y Conceptos de calidad de servicio.<br>• Llevar a cabo pruebas de carga de tráfico para evaluar rendimiento y capacidad de buffer. | | (Nagios, Zabbix,Wireshark) |
| | Actualización | • Actualizar el firmware con frecuencia para corregir vulnerabilidades.<br>• Identificar las correcciones relacionadas a la memoria buffer en las notas de la versión de firmware. | | |
| | Configuración | • Configurar el switch reduciendo el uso de la memoria buffer, esto evitando redundancias o configuraciones innecesarias.<br>• Reducir las características y funciones en la configuración para evitar el consumo excesivo de la memoria de buffer.<br>• Ajustar los parámetros de la memoria buffer en función de las necesidades de la red y con ayuda de las especificaciones del fabricante. | | |

5. Problemas y procedimientos preventivos para cables de red

| Componente | Problema | Procedimientos | Seguros | Proveedores |
|---|---|---|---|---|
| Conductor de cobre | Fallas de conectividad | • Instalación<br>• Protección física<br>• Mantenimiento | No disponible | • Compumega<br>• Adecomp<br>• Agecom – system<br>• Tecno lap<br>• Alpa tech & store |
| | Problemas de interferencia | | | |
| | Problemas de atenuación | | | |
| Pares trenzados | Cable mal ponchado | • Instalación<br>• Protección física<br>• Mantenimiento | | |
| | Problemas de interferencia | | | |
| | Problemas de longitud de cable | | | |
| Revestimiento | Daños físicos | • Instalación<br>• Protección física<br>• Mantenimiento | | |
| Conectores | Cableado incorrecto | • Instalación<br>• Protección física<br>• Mantenimiento | | |
| | Conector flojo o suelto | | | |
| | Oxidación o corrosión | | | |
| Cubierta exterior | Daños físicos | • Instalación<br>• Protección física<br>• Mantenimiento | | |
| | Problemas de interferencia | | | |
| | Problemas de flexibilidad | | | |

Procedimientos preventivos detallados para cables de red

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| Conductor de cobre | Instalación | • Uso de cables de red de calidad como el Cat6 o superior.<br>• Verificar el estado los conectores RJ-45.<br>• Manipular correctamente el cable durante la instalación, evitar doblar el cable o torcerlos.<br>• Mantener la longitud del cable dentro de los límites establecidos para evitar problemas de rendimiento. | • Cables de red<br>• Conectores RJ-45<br>• Panel de parcheo | • Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark)<br>• Herramientas de gestión de cableado (NetBox, EasyDCIM, CableIQ? |
| | Protección física | • Mantener los cables de red en un ambiente libre de humedad, calor excesivo o sustancias corrosivas.<br>• Evitar los daños mecánicos, estos incluyen cortes, aplastamiento, tirones.<br>• Verificar que no existan fuentes de interferencia electromagnética cerca de los cables de red. | | |
| | Mantenimiento | • Comprobar el estado físico de los cables regularmente en busca de signos de deterioro, cortes o daños en los conductores de cobre. | | |

| | | | | |
|---|---|---|---|---|
| | | • Llevar un registro de las inspecciones y sus resultados, además de tomar medidas correctivas de ser necesario. | | |
| Pares trenzados | Instalación | • Uso de cables de red de calidad como el Cat6 o superior.<br>• Utilizar las herramientas adecuadas para el ponchado de cable.<br>• Verificar el estado los conectores RJ-45.<br>• Manipular correctamente el cable durante la instalación, evitar doblar el cable o torcerlos.<br>• Mantener la longitud del cable dentro de los límites establecidos para evitar problemas de rendimiento. | • Cables de red<br>• Conectores RJ-45<br>• Panel de parcheo<br>• Protectores de cables<br>• Botas RJ45 | • Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark)<br>• Herramientas de gestión de cableado (NetBox, EasyDCIM, CableIQ? |
| | Protección física | • Mantener los cables de red en un ambiente libre de humedad, calor excesivo o sustancias corrosivas.<br>• Evitar los daños mecánicos, estos incluyen cortes, aplastamiento, tirones.<br>• Verificar que no existan fuentes de interferencia electromagnética cerca de los cables de red. | | |
| | Mantenimiento | • Comprobar el estado físico de los cables regularmente en busca de | | |

| | | | | |
|---|---|---|---|---|
| | | signos de deterioro, cortes o daños en los pares trenzados.<br>• Comprobar el estado de los pares trenzados con ayuda de un comprobador de cables o tester de red.<br>• Llevar a cabo pruebas de rendimiento y velocidad de la conexión en busca de problemas. | | |
| Revestimiento | Instalación | • Uso de cables de red de calidad como el Cat6 o superior.<br>• Manipular correctamente el cable durante la instalación, evitar doblar el cable o torcerlos. | • Cables de red | • Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark)<br>• Herramientas de gestión de cableado (NetBox, EasyDCIM, CableIQ? |
| | Protección física | • Mantener los cables de red en un ambiente libre de humedad, calor excesivo o sustancias corrosivas.<br>• Evitar los daños mecánicos, estos incluyen cortes, aplastamiento, tirones. | | |
| | Mantenimiento | • Comprobar el estado físico de los cables regularmente en busca de signos de deterioro, cortes o daños en el revestimiento.<br>• Llevar un registro de las inspecciones y sus resultados, además de tomar medidas correctivas de ser necesario. | | |

| | | | | |
|---|---|---|---|---|
| Conectores | Instalación | • Uso de conectores de red de calidad.<br>• Seguir el procedimiento estándar para la instalación de conectores.<br>• Utilizar las herramientas adecuadas para el ponchado de cable.<br>• Evaluar el rendimiento después de la instalación para verificar el funcionamiento de los conectores. | • Conectores RJ-45 | • Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark)<br>• Herramientas de gestión de cableado (NetBox, EasyDCIM, CableIQ? |
| | Protección física | • Mantener los conectores en un ambiente libre de humedad, calor excesivo o sustancias corrosivas.<br>• Evitar los daños mecánicos, estos incluyen cortes, aplastamiento, tirones. | | |
| | Mantenimiento | • Comprobar el estado físico de los conectores regularmente en busca de signos de deterioro, cortes o daños en el revestimiento.<br>• Realizar limpieza de los conectores periódicamente.<br>• Llevar un registro de las inspecciones y sus resultados, además de tomar medidas correctivas de ser necesario. | | |
| Cubierta exterior | Instalación | • Uso de cables de red de calidad como el Cat6 o superior, estos cuentan con cubierta exterior resistente. | • Conectores RJ-45 | • Herramientas de monitoreo de red (Nagios, Zabbix,Wireshark) |

| | | | | |
|---|---|---|---|---|
| | | • Manipular correctamente el cable durante la instalación, evitar doblar el cable o torcerlos. | | • Herramientas de gestión de cableado (NetBox, EasyDCIM, CableIQ? |
| | Protección física | • Mantener los cables de red en un ambiente libre de humedad, calor excesivo o sustancias corrosivas.<br>• Evitar los daños mecánicos, estos incluyen cortes, aplastamiento, tirones. | | |
| | Mantenimiento | • Comprobar el estado físico de los cables regularmente en busca de signos de deterioro, cortes o daños en el revestimiento.<br>• Reemplazar cables con daños en la cubierta exterior, evitando así daños de los conductores internos.<br>• Llevar un registro de las inspecciones y sus resultados, además de tomar medidas correctivas de ser necesario. | | |

6. Problemas y procedimientos preventivos para cámaras IP

<table>
<tr><th>Componente</th><th>Problema</th><th>Procedimientos</th><th>Seguros</th><th>Proveedores</th></tr>
<tr><td>Sensor de imagen</td><td>Baja calidad de imagen</td><td>• Instalación<br>• Mantenimiento<br>• Actualización</td><td rowspan="5">Seguros Condor – Corporativo e industrias - Equipo electrónico<br>Zurichseguros – Seguro de equipo electrónico para empresas<br>Pointer – Seguro PYMES<br>Seguros Unidos – Su PYME</td><td rowspan="5">Fulltec – Hikvision<br>IPCOM – Hikvision, Dahua<br>TIGRIS sistemas de seguridad – Imou<br>Matsiel - Sistemas de Seguridad y Domótica – Hikvision, Dahua, Hik Look</td></tr>
<tr><td rowspan="3">Procesador de imagen</td><td>Fallas de procesamiento</td><td rowspan="3">• Configuración<br>• Gestión de ancho de banda<br>• Actualización</td></tr>
<tr><td>Problemas de compresión de video</td></tr>
<tr><td>Fallas de procesamiento de imagen</td></tr>
<tr><td rowspan="3">Lente</td><td>Fallas de enfoque</td><td rowspan="3">• Limpieza<br>• Protección física<br>• Ajuste y enfoque<br>• Mantenimiento</td></tr>
<tr><td>Problema de viñeteado</td></tr>
<tr><td>Problemas de condensación</td></tr>
</table>

Procedimientos preventivos detallados para cámaras IP

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| Sensor de imagen | Instalación | • Seguir las instrucciones del fabricante para la instalación de las cámaras.<br>• Mantener las cámaras en un ambiente libre de humedad, polvo, temperaturas extremas o radiación solar. | • Cámara IP<br>• Switch<br>• Modem<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo provisto por el fabricante |
| | Mantenimiento | • Llevar a cabo el mantenimiento de las cámaras con las especificaciones del fabricante.<br>• Comprobar la calidad de la imagen periódicamente y realizar los ajustes necesarios. | | |
| | Actualización | • Mantener actualizado el firmware con la última versión.<br>• Conservar una copia de seguridad del firmware existente antes de llevar a cabo actualizaciones. | | |
| Procesador de imagen | Configuración | • Llevar a cabo la configuración de las cámaras siguiendo las instrucciones del fabricante.<br>• Ajustar los parámetros necesarios para procesamiento de imagen evitando sobrecargar el procesador, entre los parámetros se incluye el | • Cámara IP<br>• Switch<br>• Modem<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo provisto por el fabricante |

| | | | | |
|---|---|---|---|---|
| | | balance de blancos, nitidez, exposición. | | |
| | Gestión de ancho de banda | • Dar seguimiento al ancho de banda consumido por las cámaras, realizar los ajustes necesarios para evitar congestionar la red<br>• Recurrir a técnicas de compresión de video como la H.264 o H.265, reduciendo la carga del procesador y el uso del ancho de banda. | | |
| | Actualización | • Mantener actualizado el firmware con la última versión.<br>• Conservar una copia de seguridad del firmware existente antes de llevar a cabo actualizaciones. | | |
| Lente | Limpieza | • Desconectar la cámara de la alimentación<br>• Con ayuda de un paño suave limpiar el lente con movimientos circulares. | • Cámara IP<br>• Switch<br>• Modem<br>• Cables de red<br>• PC | • Firmware actualizado<br>• Sistema operativo provisto por el fabricante |
| | Protección física | • Ubicar la cámara en una ubicación segura.<br>• Mantener el lente protegido de golpes, rayaduras y el ambiente. | | |
| | Ajuste y enfoque | • Mediante la interfaz de administración acceder a la configuración.<br>• Realizar los ajustes necesarios para obtener una imagen clara. | | |

| | | | | |
|---|---|---|---|---|
| | | • Comprobar la calidad de la imagen con ayuda de monitores. | | |
| | Mantenimiento | • Llevar a cabo el mantenimiento de las cámaras con las especificaciones del fabricante.<br>• Comprobar la calidad de la imagen periódicamente y realizar los ajustes necesarios. | | |

**Anexo 20: Elementos de detección**

# Contenido

**Introducción:**

El presente documento define los procedimientos de detección para problemas con los activos de TI de la empresa, los procedimientos descritos a continuación buscan brindar una guía y herramientas para la detección de problemas de TI.

**Alcance:**

El plan de procedimientos preventivos incluye los activos identificados, sus componentes y los problemas relacionados a los mismos, sus síntomas, procedimientos y herramientas de detección.

1. **Problemas, síntomas y detección - PCs**

| Componente | Problema | Síntomas | Detección |
|---|---|---|---|
| CPU | Sobrecalentamiento | • Sistema lento<br>• Reinicios esporádicos<br>• Pantallas de error o congeladas<br>• Ventilador ruidoso | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Si el dispositivo cuenta con opciones de monitoreo activarlas tanto en la BIOS como en la configuración del sistema operativo. |
| | Fallos de ventiladores | • Sobrecalentamiento de CPU<br>• Ruidos fuera de lo normal<br>• Cambios en la velocidad<br>• Reinicios esporádicos<br>• Pantallas de error o congeladas | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Inspección física. |

| | | | |
|---|---|---|---|
| | Bloqueo del sistema | • Pantallas de error o congeladas<br>• Sistema lento<br>• Reinicios esporádicos<br>• Pantallazo azul | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Revisar el registro de eventos del sistema en busca de errores o advertencias.<br>• Mantener los controladores actualizados a la versión más reciente. |
| | Bajo rendimiento | • Ejecución lenta de tareas sencillas.<br>• Tiempos de respuesta prolongados.<br>• Carga excesiva de CPU. | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Mantener los controladores actualizados a la versión más reciente. |
| | Fallas de la tarjeta madre | • Fallas de alimentación o dificultades de arranque.<br>• Problemas de funcionamiento de dispositivos conectados por USB.<br>• Fallas de audio y video.<br>• Fallas de sistema como reinicios esporádicos, errores de memoria o bloqueos. | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Analizar los mensajes de error durante el proceso de arranque.<br>• Inspección física de la tarjeta madre.<br>• Someter la tarjeta a pruebas de diagnóstico en busca de problemas específicos. |
| | Puertos inoperables | • El sistema operativo no reconoce dispositivos conectados por USB y otros puertos.<br>• Baja velocidad de transferencia de datos. | Espontaneo/ indetectable |

| | | | |
|---|---|---|---|
| | | • Fallas de conectividad de red<br>• Fallas en la señal de video. | |
| | Fallas de procesador | • Reinicios esporádicos<br>• Pantallas de error o congeladas<br>• Pantallazo azul<br>• Bajo rendimiento<br>• Temperatura excesiva del procesador | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Revisar con frecuencia los reportes de pruebas de estrés con software especializado (CPU-Z, Prime95, AIDA64).<br>• Mantener firmware y controladores actualizados.<br>• Inspección física del procesador. |
| | Fallos de disco duro | • Ruidos fuera de lo normal.<br>• Tiempo de respuesta prolongado del sistema<br>• Perdida de datos<br>• Fallas de lectura y escritura | • Mantener activas y actualizadas las herramientas de monitoreo y diagnostico (CrystalDiskInfo, Seatools). |
| | Fallos de memoria RAM | • Reinicios esporádicos<br>• Pantallazo azul<br>• Bloqueos de sistema frecuentes<br>• Errores de ejecución<br>• Corrupción o perdida de información. | • Ejecutar con frecuencia pruebas de diagnóstico a las memorias RAM con software especializado (Memest86) o funcionalidades integradas en el sistema operativo.<br>• Revisión física de la memorias o reemplazo de ser necesario. |
| | Fallos de tarjeta gráfica | • Distorsiones de imagen fijas o intermitentes.<br>• Ausencia total de imagen (pantalla negra) | • Comprobar el funcionamiento de la tarjeta con ayuda de otros dispositivos.<br>• Mantener los controladores actualizados a la versión más reciente.<br>• Revisión física de la tarjeta gráfica. |

| | | | |
|---|---|---|---|
| | | • Ralentización o bloqueo de aplicaciones que requieren recursos gráficos.<br>• Reinicios esporádicos | |
| | Fallos de la fuente de poder | • Problemas de arranque por falta de energía.<br>• Reinicios esporádicos.<br>• Ruidos fuera de lo normal.<br>• Olor a quemado o humo saliendo de la fuente de poder.<br>• Sistema bloqueado o inestable. | • Revisión física de la fuente de poder, comprobar que la salida de voltaje este dentro de los limites adecuados. |
| | Fallos de la tarjeta de red | • Fallas de conectividad de red<br>• Baja velocidad de transferencia de datos.<br>• Red inestable.<br>• Perdida y corrupción de paquetes.<br>• Retraso en la comunicación. | • Revisión física de la tarjeta de red y de los cables de red.<br>• Mantener los controladores actualizados a su última versión.<br>• Verificar el estado de la conexión con ayuda de otros dispositivos.<br>• Someter a los equipos y cables de red a pruebas de diagnóstico. |

| | | | |
|---|---|---|---|
| | Fallas de la BIOS | • Errores de arranque del sistema.<br>• Cambios inesperados en la configuración de la BIOS.<br>• Dispositivos no reconocidos por la BIOS.<br>• Mensajes de error durante el arranque del sistema.<br>• Dificultad o imposibilidad de actualizar a BIOS. | • Revisión física de la tarjeta madre.<br>• Mantener actualizada la BIOS. |
| Monitor | Imagen distorsionada | • Imagen borrosa o distorsionada<br>• Fallas de color, colores equivocados.<br>• Pixeles muertos.<br>• Parpadeo de pantalla o cambios esporádicos en el color y el contraste. | • Revisión física del monitor.<br>• Comprobar la configuración del monitor.<br>• Verificar el estado físico de cables y conexiones.<br>• Mantener los controladores actualizados. |

## 2. Problemas, síntomas y detección - bases de datos

| **Componente** | **Problema** | • **Síntomas** | • **Detección** |
|---|---|---|---|
| Datos | Corrupción de datos | • Errores al leer o escribir datos.<br>• Perdida de integridad referencial<br>• Datos incompletos o incoherentes. | • Verificar la integridad referencial con ayuda de las herramientas del SGBD. |

| | | | |
|---|---|---|---|
| | | • Baja de rendimiento de la base de datos.<br>• Fallas del sistema y de la base de datos | • Comprobar la integridad de los datos con ayuda de consultas. O herramientas para validación de datos.<br>• Dar seguimiento al rendimiento de la base de datos. Esto incluye bloqueos, tiempos de respuesta y errores. |
| | Perdida de datos | • Dificultad para acceder a los datos.<br>• Discrepancias de datos o datos inconsistentes. | • Llevar a cabo una auditoria de los registros con frecuencia.<br>• Implementar un sistema de monitoreo para los datos, este debe registrar y alertar posibles errores o discrepancias. |
| | Inconsistencia de datos | • Información incorrecta o contradictoria.<br>• Datos duplicados<br>• Datos inconsistentes. | • Llevar a cabo una auditoria de los registros con frecuencia. |
| | Accesos no autorizados | • Datos modificados o eliminados.<br>• Actividad fuera de lo común<br>• Ajustes de seguridad modificados. | • Llevar a cabo una auditoria de los la base de datos con frecuencia.<br>• Dar seguimiento de los accesos a la base de datos y llevar un registro de los mismos. |

### 3. Problemas, síntomas y detección - modem/access point

| Componente | Problema | Síntomas | Detección |
|---|---|---|---|
| | | | |
| Interfaces de red | Conexión a internet inestable | • Baja velocidad de conexión.<br>• Interferencias en la conexión.<br>• Comunicación lenta o bloqueada. | • Ejecutar pruebas de velocidad de internet periódicamente.<br>• Revisar con frecuencia los reportes de las herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| | Problemas de configuración | • Conexión a internet inestable<br>• Baja velocidad de internet.<br>• Difícil acceso a la red Wi-Fi | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| | Problemas de seguridad | • Actividad sospechosa en la red.<br>• Cambios en el patrón de trafico de la red.<br>• Red lenta o inaccesible. | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| Procesador | Conexión a internet inestable | • Baja velocidad de conexión.<br>• Interferencias en la conexión.<br>• Comunicación lenta o bloqueada. | • Ejecutar pruebas de velocidad de internet periódicamente.<br>• Revisar con frecuencia los reportes de las herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| | Problemas de configuración | • Conexión a internet inestable<br>• Baja velocidad de internet.<br>• Difícil acceso a la red Wi-Fi | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |

| | | | |
|---|---|---|---|
| | Problemas de seguridad | • Actividad sospechosa en la red.<br>• Cambios en el patrón de trafico de la red.<br>• Red lenta o inaccesible. | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| Memoria | Memoria insuficiente | • Perdida frecuente de la conexión. | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| | Corrupción de datos | • Perdida frecuente de la conexión.<br>• Funcionamiento inusual como bloqueos, reinicios o respuestas lentas. | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| | Actualizar firmware | • Funcionamiento inusual como bloqueos, reinicios o respuestas lentas.<br>• Problemas de incompatibilidad | • Espontaneo/ indetectable |
| Sistema operativo | Configuración incorrecta | • Conexión a internet inestable<br>• Baja velocidad de internet.<br>• Difícil acceso a la red Wi-Fi | • Ejecutar con frecuencia herramientas de monitoreo de red (Wireshark, Nagios, Zabbix). |
| Tabla de enrutamiento | Actualizar firmware | • Funcionamiento inusual como bloqueos, reinicios o respuestas lentas.<br>• Problemas de incompatibilidad | Espontaneo/ indetectable |

| | | | |
|---|---|---|---|
| Firewall | Actualizar firmware | • Funcionamiento inusual como bloqueos, reinicios o respuestas lentas.<br>• Problemas de incompatibilidad | Espontaneo/ indetectable |

**4. Problemas, síntomas y detección - switches**

| Componente | Problema | Síntomas | Detección |
|---|---|---|---|
| Puertos | Problemas de conectividad | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |

**5. Problemas, síntomas y detección - cables de red**

| Componente | Problema | • Síntomas | • Detección |
|---|---|---|---|
| Conductor de cobre | Fallas de conectividad | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| | Problemas de interferencia | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |

| | | | |
|---|---|---|---|
| | Problemas de atenuación | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| Pares trenzados | Cable mal ponchado | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| | Problemas de interferencia | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| | Problemas de longitud de cable | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| Revestimiento | Daños físicos | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| Conectores | Cableado incorrecto | • Conexión nula | • Revisión física de los conectores |
| | Conector flojo o suelto | • Conexión nula | • Revisión física de los conectores |
| | Oxidación o corrosión | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Revisión física de los conectores |
| Cubierta exterior | Daños físicos | • Interferencias en la conexión. | • Comprobar la integridad física de los cables de red. |

| | | | |
|---|---|---|---|
| | | • Baja velocidad de transferencia. | • Ejecutar pruebas de velocidad de internet. |
| | Problemas de interferencia | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |
| | Problemas de flexibilidad | • Interferencias en la conexión.<br>• Baja velocidad de transferencia. | • Comprobar la integridad física de los cables de red.<br>• Ejecutar pruebas de velocidad de internet. |

## Anexo 21: Procedimientos de corrección

## Contenido

**Introducción:**

El presente documento define los procedimientos de corrección para problemas con los activos de TI de la empresa, los procedimientos descritos a continuación buscan brindar una guía para afrontar los diferentes problemas y corregirlos.

**Alcance:**

El plan de procedimientos preventivos incluye los activos identificados, sus componentes y los problemas relacionados a los mismos, sus soluciones, responsables y tiempo de respuesta

1. **Problemas, solución - PCs**

| **Componente** | **Problema** | **Solución** | **Responsables** | **Tiempo de respuesta** |
|---|---|---|---|---|
| CPU | Sobrecalentamiento | • Proceso de mantenimiento general para CPU | • Encargado de sistemas<br>• Ing. Roberto Pico | Entre 24 y 36 horas en días hábiles |
| | Fallos de ventiladores | • Proceso de mantenimiento general para CPU | | |
| | Fallo de la fuente de poder | • Proceso de mantenimiento general para CPU | | |
| | Pantallazo azul | • Reiniciar el sistema<br>• Actualizar o reinstalar drivers de hardware | | |

| | | | | |
|---|---|---|---|---|
| | | • Analizar el sistema en busca de virus o malware<br>• Restaurar el sistema a un punto de tiempo anterior al problema | | |
| | Bloqueo del sistema | • Reiniciar el sistema<br>• Verificar compatibilidad de software y controladores instalados, actualizarlo de ser necesario.<br>• Analizar el sistema en busca de virus o malware<br>• Verificar el estado del disco duro, repararlo de ser necesario | | |
| | Error de arranque | • Proceso de mantenimiento general para CPU | | |
| | Bajo rendimiento | • Proceso de mantenimiento general para CPU | | |
| | Ruido excesivo del ventilador | • Proceso de mantenimiento general para CPU<br>• Acceder a la BIOS y revisar la configuración. | | |
| | Fallas de la tarjeta madre | • Proceso de mantenimiento general para CPU<br>• Reemplazar la tarjeta de ser necesario | | |
| | Puertos inoperables | • Proceso de mantenimiento general para CPU | | |
| | Fallas de procesador | • Proceso de mantenimiento general para CPU | | |

| | | | | |
|---|---|---|---|---|
| | | • Reemplazar el procesador de ser necesario | | |
| | Procesador incompatible | • Revisar la versión de la BIOS y actualizarla de ser necesario con ayuda de las instrucciones del fabricante<br>• Revisar la compatibilidad del procesador con la tarjeta madre. | | |
| | Fallos de disco duro | • Proceso de mantenimiento general para CPU<br>• Analizar el disco en busca de errores y repararlos | | |
| | Fallos de memoria RAM | • Proceso de mantenimiento general para CPU<br>• Revisar la compatibilidad de la memoria RAM con la tarjeta madre | | |
| | Fallos de tarjeta gráfica | • Proceso de mantenimiento general para CPU<br>• Revisar la compatibilidad de la tarjeta gráfica con la tarjeta madre<br>• Reemplazar la tarjeta gráfica de ser necesario | | |
| | Fallos de la fuente de poder | • Proceso de mantenimiento general para CPU<br>• Reemplazar la fuente de poder de ser necesario | | |
| | Fallos de la placa de red | • Proceso de mantenimiento general para CPU | | |

| | | | | |
|---|---|---|---|---|
| | | • Revisar la configuración de red | | |
| | Fallas de la BIOS | • Acceder a la BIOS y revisar la configuración<br>• Revisar la versión de la BIOS y actualizarla de ser necesario con ayuda de las instrucciones del fabricante | | |
| | Robo o perdida de CPU | • Notificar a gerencia del evento<br>• Cambiar contraseñas de cuentas activas.<br>• Inhabilitar acceso remoto a la red en caso de estar activo.<br>• Contactar a la aseguradora o proveedor según corresponda. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 24 y 48 horas en días hábiles |
| | Incendios | • Evaluar el daño causado a los CPUs e identificar los componentes más afectados.<br>• Emitir reporte de los daños a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda.<br>• Búsqueda de locación provisional para continuar con las operaciones. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |
| | Desastres naturales | • Evaluar el daño causado a los CPUs e identificar los componentes más afectados.<br>• Emitir reporte de los daños a gerencia. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |

| | | | | |
|---|---|---|---|---|
| | | • Contactar a la aseguradora o proveedor según corresponda.<br>• Búsqueda de locación provisional para continuar con las operaciones.<br>• Búsqueda de locación provisional para continuar con las operaciones. | | |
| | Saqueos | • Evaluar las pérdidas de CPUs.<br>• Emitir reporte de pérdidas a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |
| Monitor | Pixeles muertos | • Uso de software para reparar pixeles<br>• Reemplazar el monitor si los pixeles muertos se agrupan en grandes cantidades | • Encargado de sistemas<br>• Ing. Roberto Pico | Entre 24 y 36 horas en días hábiles |
| | Problemas de retroalimentación | • Verificar configuraciones del monitor<br>• Reemplazar la retroiluminación de ser necesario | | |
| | Imagen distorsionada | • Ajustar la resolución<br>• Verificar estado de drivers<br>• Realizar ajuste manual | | |
| | Problemas de encendido | • Revisar cable y fuente de alimentación<br>• Verificar las conexiones<br>• Verificar la compatibilidad del monitor con el CPU | | |

| | | | | |
|---|---|---|---|---|
| | Pantalla sin imagen | • Proceso de mantenimiento general para monitor | | |
| | Parpadeo de pantalla | • Proceso de mantenimiento general para monitor<br>• Verificar el estado de los drivers y actualizarlos de ser necesario | | |
| | Fallos de color o imagen | • Proceso de mantenimiento general para monitor<br>• Comprobar la configuración de brillo, contraste y temperatura en el menú del monitor.<br>• Verificar el estado de los drivers y actualizarlos de ser necesario | | |
| | Resolución incorrecta | • Comprobar la configuración de resolución en el menú del monitor.<br>• Verificar el estado de los drivers y actualizarlos de ser necesario | | |
| | Robo o perdida de monitor | • Notificar a gerencia del evento<br>• Contactar a la aseguradora o proveedor según corresponda | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 24 y 48 horas en días hábiles |
| | Incendios | • Evaluar el daño causado a los monitores.<br>• Emitir reporte de los daños a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |

| | | | | |
|---|---|---|---|---|
| | | • Búsqueda de locación provisional para continuar con las operaciones. | | |
| | Desastres naturales | • Evaluar el daño causado a los CPUs e identificar los componentes más afectados.<br>• Emitir reporte de los daños a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda.<br>• Búsqueda de locación provisional para continuar con las operaciones.<br>• Búsqueda de locación provisional para continuar con las operaciones. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |
| | Saqueos | • Evaluar las pérdidas de CPUs.<br>• Emitir reporte de pérdidas a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |
| Teclado | Teclas atascadas | • Proceso de mantenimiento general para teclado<br>• Reemplazar teclas dañadas | • Encargado de sistemas<br>• Ing. Roberto Pico | Entre 24 y 36 horas en días hábiles |
| | Daños por líquidos | • Desconectar el teclado de inmediato<br>• Proceso de mantenimiento general para teclado | | |
| | Cable dañado | • Proceso de mantenimiento general para teclado<br>• Verificar la conexión del cable<br>• Verificar el estado del cable | | |

| | | | | |
|---|---|---|---|---|
| | | • Reemplazar el cable de ser necesario. | | |
| | Fallos de teclas | • Proceso de mantenimiento general para teclado<br>• Reemplazar el teclado si el problema persiste | | |
| | Caracteres incorrectos | • Proceso de mantenimiento general para teclado<br>• Verificar configuración de idioma y teclado<br>• Verificar el estado de los drivers y actualizarlos de ser necesario<br>• Reemplazar el teclado si el problema persiste | | |
| | Tiempo de respuesta prolongado | • Proceso de mantenimiento general para teclado<br>• Revisar el consumo de recursos del sistema.<br>• Verificar el estado de los drivers y actualizarlos de ser necesario<br>• Reemplazar el teclado si el problema persiste | | |
| | Teclas pegadas o ruidosas | • Proceso de mantenimiento general para teclado<br>• Reemplazar el teclado si el problema persiste | | |
| | Robo o perdida de teclado | • Notificar a gerencia del evento | | |

| | | | | |
|---|---|---|---|---|
| | Perdida o daños por eventos catastróficos | • Contactar a la aseguradora o proveedor según corresponda | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 24 y 48 horas en días hábiles |
| Mouse | Cursor con movimiento errático | • Proceso de mantenimiento general para mouse<br>• Verificar el estado de los drivers y actualizarlos de ser necesario | • Encargado de sistemas<br>• Ing. Roberto Pico | Entre 24 y 36 horas en días hábiles |
| | Clics inconsistentes o con retardo | • Proceso de mantenimiento general para mouse<br>• Verificar el estado de los drivers y actualizarlos de ser necesario<br>• Reemplazar el mouse si el problema persiste | | |
| | Desplazamiento irregular | • Proceso de mantenimiento general para mouse<br>• Verificar el estado de los drivers y actualizarlos de ser necesario<br>• Reemplazar el mouse si el problema persiste | | |
| | Mouse sin respuesta | • Proceso de mantenimiento general para mouse<br>• Reemplazar el mouse si el problema persiste | | |
| | Robo o perdida de mouse | • Notificar a gerencia del evento | | |

| | | | | |
|---|---|---|---|---|
| | Perdida o daños por eventos catastróficos | • Contactar a la aseguradora o proveedor según corresponda | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 24 y 48 horas en días hábiles |

**2. Problemas, solución - bases de datos**

| **Componente** | **Problema** | **Solución** | **Responsables** | **Tiempo de respuesta** |
|---|---|---|---|---|
| Datos | Corrupción de datos | • Restaurar los datos con una copia de seguridad reciente<br>• Uso de herramientas para recuperar y reparar bases de datos. | Ing. Cristóbal Paredes | Entre 24 y 36 horas en días hábiles |
| | Perdida de datos | • Restaurar los datos con una copia de seguridad reciente<br>• Aplicar técnicas de recuperación de datos<br>• Implementar métodos para copias de seguridad y recuperación de datos | | |
| | Inconsistencia de datos | • Verificar los datos periódicamente y corregir inconsistencias<br>• Establecer parámetros para el ingreso de datos | | |

| | | | | |
|---|---|---|---|---|
| | Accesos no autorizados | • Verificar las medidas de seguridad y su efectividad<br>• Actualizar tanto la base de datos como el software de apoyo<br>• Ejecutar periódicamente pruebas de penetración y auditorias de seguridad | | |
| | Problemas de rendimiento | • Optimizar consultas y los índices de la base de datos<br>• Implementar mejoras de hardware de ser necesario, esto incluye memoria RAM y almacenamiento<br>• Verificar que la configuración del gestor de base de datos sea optima | | |

### 3. Problemas, solución - modem/access point

| Componente | Problema | Solución | Responsables | Tiempo de respuesta |
|---|---|---|---|---|
| Interfaces de red | Conexión a internet inestable | • Verificar el estado de los cables de red<br>• Buscar dispositivos que puedan causar interferencias<br>• Reiniciar el dispositivo para reestablecer la conexión | • **Encargado de sistemas**<br>• **Netlife** | Máximo 24 horas en días hábiles |

| | | | | |
|---|---|---|---|---|
| | | • Solicitar soporte al proveedor de internet | | |
| | Baja velocidad | • Realizar pruebas de velocidad de internet<br>• Verificar si existen dispositivos que utilicen gran ancho de banda<br>• Reiniciar el dispositivo para reestablecer la conexión | | |
| | Problemas de configuración | • Revisar la configuración IP del modem, esto incluye la máscara de subred, puerta de enlace y DNS<br>• Verificar que los dispositivos conectados al modem obtienen direcciones IP por medio del protocolo DHCP<br>• Configurar manualmente la IP de los dispositivos conectados de ser necesario | | |
| | Problemas de seguridad | • Verificar la contraseña de administración y cambiarla de ser necesario<br>• Habilitar cifrado Wi-Fi para proteger la red inalámbrica<br>• Actualizar el firmware regularmente | | |

| | | | | |
|---|---|---|---|---|
| | Problemas de incompatibilidad | • Revisar que los dispositivos conectados sean compatibles<br>• Revisar actualizaciones de firmware o controladores para los dispositivos | | |
| Procesador | Conexión a internet inestable | • Verificar el estado de los cables de red<br>• Buscar dispositivos que puedan causar interferencias<br>• Reiniciar el dispositivo para reestablecer la conexión<br>• Solicitar soporte al proveedor de internet | | |
| | Baja velocidad | • Realizar pruebas de velocidad de internet<br>• Verificar si existen dispositivos que utilicen gran ancho de banda<br>• Reiniciar el dispositivo para reestablecer la conexión | | |
| | Problemas de configuración | • Revisar la configuración IP del modem, esto incluye la máscara de subred, puerta de enlace y DNS<br>• Verificar que los dispositivos conectados al modem | | |

| | | | | |
|---|---|---|---|---|
| | | obtienen direcciones IP por medio del protocolo DHCP<br>• Configurar manualmente la IP de los dispositivos conectados de ser necesario | | |
| | Problemas de seguridad | • Verificar la contraseña de administración y cambiarla de ser necesario<br>• Habilitar cifrado Wi-Fi para proteger la red inalámbrica<br>• Actualizar el firmware regularmente | | |
| | Problemas de incompatibilidad | • Revisar que los dispositivos conectados sean compatibles<br>• Revisar actualizaciones de firmware o controladores para los dispositivos | | |
| Memoria | Memoria insuficiente | • Revisar si es posible limpiar o borrar la memoria en la configuración del modem | | |
| | Corrupción de datos | • Reestablecer la memoria a su configuración predeterminada | | |
| | Actualizar firmware | • Revisar si hay actualizaciones disponibles en el sitio web del fabricante y actualizarlo según sus instrucciones | | |

| | | | | |
|---|---|---|---|---|
| Sistema operativo | Fallos de firmware | • Revisar si hay actualizaciones disponibles en el sitio web del fabricante y actualizarlo según sus instrucciones | | |
| | Configuración incorrecta | • Revisar las configuraciones de red, de seguridad entre otras opciones | | |
| | Problemas de compatibilidad | • Revisar que los dispositivos conectados sean compatibles con el firmware del modem | | |
| | Problemas persistentes | • Realizar restauración de fábrica, esto reestablecerá todas las configuraciones | | |
| Tabla de enrutamiento | Tabla de enrutamiento incorrecta | • Verificar las direcciones IP, máscaras de subred y puertas de enlace predeterminadas, corregir cualquier configuración incorrecta | | |
| | Problemas de IP | • Revisar que las direcciones IP de los dispositivos sean únicas, caso contrario cambiarlas. | | |
| | Actualizar firmware | • Revisar si hay actualizaciones disponibles en el sitio web del fabricante y actualizarlo según sus instrucciones | | |

| | | | | |
|---|---|---|---|---|
| Firewall | Configuración incorrecta | • Revisar las reglas de filtrado y políticas de seguridad, ajustar la configuración de forma que permita o bloquee servicios, puertos o IP’s | | |
| | Bloqueo de puertos necesarios | • Revisar configuración de firewall<br>• Agregar reglas de excepción para permitir tráfico por puertos determinados | | |
| | Restricciones de acceso | • Revisar configuración de firewall y sus restricciones de acceso<br>• Revisar que los dispositivos y aplicaciones estén permitidos en la configuración del firewall. | | |
| | Actualizar firmware | • Revisar si hay actualizaciones disponibles en el sitio web del fabricante y actualizarlo según sus instrucciones | | |

## 4. Problemas, solución - switches

| Componente | Problema | Solución | Responsables | Tiempo de respuesta |
|---|---|---|---|---|
| Puertos | Problemas de conectividad | • Verificar el estado de los cables de red y sus conectores<br>• Revisar el funcionamiento del cable de red | Ing. Roberto Pico | Entre 24 y 48 horas en días hábiles |
| | Direcciones MAC duplicadas | • Identificar dispositivos con MAC duplicada<br>• Cambiar la MAC manualmente o configurar el switch para que lo haga de forma automática | | |
| | Bajo rendimiento de puertos | • Revisar la configuración de los puertos, la velocidad y el modo dúplex<br>• Revisar el estado del cable de red<br>• Actualizar el firmware para garantizar mejoras de rendimiento | | |
| | VLAN mal configurada | • Revisar la asignación de puertos y configuración de enlaces troncales | | |

| | | | | |
|---|---|---|---|---|
| Tabla de direccionamiento MAC | Tabla incompleta | • Configurar el switch de forma que aprenda automáticamente las direcciones MAC<br>• Configurar el switch para que envié tráfico a todos los puertos, permitiendo la actualización de la tabla | | |
| | Tabla llena | • Incrementar el tamaño de la tabla si el switch cuenta con esa capacidad<br>• Configurar la función de envejecimiento de direcciones MAC, esto ayuda a liberar espacio | | |
| | Direcciones duplicadas | • Revisar los dispositivos conectados en busca de direcciones MAC duplicadas y asignar nuevas direcciones de ser necesario<br>• Configurar el switch para que envié tráfico a todos los puertos, permitiendo la actualización de la tabla | | |
| Motor de conmutación | Bajo rendimiento | • Revisar la capacidad de conmutación de switch o reemplazarlo por uno de mayor capacidad | | |

| | | | | |
|---|---|---|---|---|
| | | • Revisar la configuración de puertos<br>• Actualizar el firmware para garantizar mejoras de rendimiento | | |
| | Sobrecarga de CPU | • Revisar procesos y funciones del switch en busca de aquellos con alto consumo de recursos<br>• Redistribuir el tráfico con ayuda de enlaces troncales | | |
| | Fallos de seguridad | • Revisar las listas de control de acceso (ACL) y configurarlas para filtrar el trafico<br>• Actualizar el firmware para garantizar mejoras de seguridad | | |
| Memoria de búfer | Sobrecarga de búfer | • Incrementar el tamaño de búfer si el switch cuenta con esa capacidad<br>• Asignar prioridades a determinado tipo de tráfico para evitar congestión del búfer<br>• Limitar el ancho de banda | | |

| | | | | |
|---|---|---|---|---|
| | Problema de latencia | • Verificar la capacidad de la memoria búfer para manejar trafico<br>• Revisar procesos y funciones del switch en busca de aquellos con alto consumo de recursos<br>• Asignar prioridades a determinado tipo de tráfico para evitar congestión del búfer<br>• | | |
| | Desbordamiento de búfer | • Incrementar el tamaño de búfer si el switch cuenta con esa capacidad<br>• Aplicar mecanismos de control de congestión como descarte aleatorio o selectivo | | |

## 5. Problemas, solución - cables de red

| Componente | Problema | Solución | Responsables | Tiempo de respuesta |
|---|---|---|---|---|
| Conductor de cobre | Fallas de conectividad | • Verificar el estado del cable y sus conectores<br>• Comprobar que el emparejamiento de pares este acorde a la norma de cableado TIA/EIA 568ª o 568B | • Encargado de sistemas<br>• Ing. Roberto Pico | Entre 24 y 48 horas en días hábiles |
| | Problemas de interferencia | • Verificar que el cable de red no esté al alcance de fuentes de interferencia electromagnética cables o equipos eléctricos<br>• Utilizar cables blindados para reducir el impacto de la interferencia electromagnética<br>• Reemplazar conectores de ser necesario | | |
| | Problemas de atenuación | • Verificar la longitud del cable y sus limitaciones<br>• Utilizar repetidores de señal<br>• Reemplazar cables defectuosos de ser necesario | | |

| | | | | |
|---|---|---|---|---|
| Pares trenzados | Cable mal ponchado | • Comprobar que el emparejamiento de pares este acorde a la norma de cableado TIA/EIA 568ª o 568B<br>• Verificar que los hilos de cobre hagan contacto con el conector | | |
| | Problemas de interferencia | • Verificar que el cable de red no esté al alcance de fuentes de interferencia electromagnética cables o equipos eléctricos<br>• Utilizar cables blindados para reducir el impacto de la interferencia electromagnética<br>• Reemplazar conectores de ser necesario | | |
| | Problemas de longitud de cable | • Verificar la longitud del cable y sus limitaciones<br>• Utilizar repetidores de señal | | |
| Revestimiento | Daños físicos | • En caso de daños mejores reparar con cinta aislante o termo retráctil<br>• En caso de daños mayores reemplazar el cable | | |

| | | | | |
|---|---|---|---|---|
| Conectores | Cableado incorrecto | • Comprobar que el emparejamiento de pares este acorde a la norma de cableado TIA/EIA 568ª o 568B<br>• Verificar que los hilos de cobre hagan contacto con el conector | | |
| | Conector flojo o suelto | • Verificar la conexión a puertos<br>• Ajustar o reemplazar conectores | | |
| | Oxidación o corrosión | • Comprobar el estado de los conectores con regularidad<br>• Limpiar los conectores en caso de ser necesario<br>• Reemplazar el conector de ser necesario | | |
| Cubierta exterior | Daños físicos | • En caso de daños mejores reparar con cinta aislante o termo retráctil<br>• En caso de daños mayores reemplazar el cable | | |
| | Problemas de interferencia | • Verificar que el cable de red no esté al alcance de fuentes de interferencia electromagnética cables o equipos eléctricos | | |

| | | | | |
|---|---|---|---|---|
| | | • Utilizar cables blindados para reducir el impacto de la interferencia electromagnética | | |
| | Problemas de flexibilidad | • Utilizar cables resistentes y flexibles | | |

## 6. Problemas, solución - cámaras IP

| Componente | Problema | Solución | Responsables | Tiempo de respuesta |
|---|---|---|---|---|
| Sensor de imagen | Baja calidad de imagen | • Revisar la configuración de la cámara y ajustar la resolución<br>• Comprobar que el enfoque de cámara sea correcto<br>• Comprobar la calidad de la conexión de red y su velocidad de transmisión<br>• Reemplazar el sensor si el problema persiste | • Encargado de sistemas<br>• Fulltec | Entre 4 y 5 días hábiles |
| Procesador de imagen | Fallas de procesamiento | • Verificar la capacidad de procesamiento y si esta cumple con las necesidades de grabación | | |

| | | | | |
|---|---|---|---|---|
| | | • Comprobar que el ancho de banda asignado es suficiente para el flujo de video | | |
| | Problemas de compresión de video | • Revisar la configuración de la cámara y que el formato de compresión sea el adecuado en función de sus necesidades | | |
| | Fallas de procesamiento de imagen | • Revisar la configuración de la cámara y que el procesamiento sea el adecuado en función de sus necesidades | | |
| Lente | Fallas de enfoque | • Revisar el estado de la lente<br>• Ajustar el enfoque de la camera ya sea de forma manual o automática | | |
| | Problema de viñeteado | • Revisar el estado de la lente<br>• Verificar que este bien instalada y que no existan obstrucciones físicas | | |
| | Problemas de condensación | • Verificar las condiciones ambientales de la ubicación de la cámara | | |

**7. Proceso de mantenimiento general para CPU:**

**Responsable:** Auxiliar externo.

- Limpieza externa: Con ayuda de paños suaves, brochas o compresores de aire limpiar polvo y suciedad presente en la superficie externa del dispositivo, ranuras de ventilación y puertos.
- Limpieza interna: Abrir el dispositivo según las especificaciones del fabricante, con ayuda de brocha o compresor de aire limpiar los componentes internos del dispositivo, estos incluyen ventiladores, disipadores de calor, tarjeta madre, etc.
- Verificar conexiones: Revisar cables internos y externos en busca de daños o desperfectos, comprobar que estén conectados correctamente, reemplazar cables dañados si hace falta.
- Verificar componentes: Examinar físicamente componentes como conectores, memorias RAM, discos duros, placa madre, en busca de daños o desgaste de los mismos, reemplazar componentes dañados de ser necesario
- Actualizar controladores: Actualizar o reinstalar los controladores de hardware a su versión más reciente para evitar problemas de incompatibilidad y mejorar el rendimiento y seguridad de los dispositivos.
- Comprobar ventilación: Revisar que el dispositivo este ventilado correctamente, revisar que los ventiladores funcionen correctamente y limpiarlos para evitar obstrucciones, reemplazarlos de ser necesario, revisar disipadores de calor y
- Comprobar temperatura: Verificar que la temperatura este dentro los limites aceptables, para esto utilizar software especializado o verificar el sistema de ventilación.
- Respaldar datos: Respaldar los datos de forma periódica en dispositivos externos o servicios en la nube, esto para mantenerlos seguros.

**8. Proceso de mantenimiento general para monitor:**

**Responsable:** Encargado de sistemas.

- Limpieza: Con el monitor apagado y un paño suave limpiar la pantalla, el marco y la superficie en general, rejillas de ventilación.
- Verificación: Comprobar la calidad de la imagen, debe ser clara y sin distorsiones, comprobar la configuración del monitor y ajustarla según la necesidad. Revisar el estado de los cables y sus conectores.

**9. Proceso de mantenimiento general para teclado:**

**Responsable:** Encargado de sistemas.

- Limpieza: Con ayuda de un compresor y un cepillo suave limpiar entre las teclas, de ser necesario limpiar tecla por tecla con un paño húmedo.
- Verificación: Comprobar el estado y funcionamiento de las teclas, en caso de fallos volver a limpiar o reemplazar las teclas de ser necesario. Revisar el estado del cable y su conector.

**10. Proceso de mantenimiento general para mouse:**

- Limpieza: Con ayuda de un paño suave limpiar la superficie del mouse, con especial enfoque en la zona del sensor óptico.
- Verificación: Comprobar el estado y funcionamiento del mouse, el movimiento del mismo debe ser suave y los botones deben responder de inmediato, caso contrario considerar reemplazarlo. Revisar el estado del cable y su conector.

**Anexo 22: Políticas gestión de riesgos de TI**

**Políticas preventivas:**

**Mantenimiento:**
**Responsable:** Encargado de sistemas

- Establecer el cronograma para mantenimiento preventivo de computadores, este abarca CPU y periféricos, se recomienda ejecutarlo cada 6 meses.
- Utilizar herramientas y equipo adecuado para llevar a cabo la actividad, especial atención el uso de pulseras anti estáticas.
- El mantenimiento se limita a limpieza interna y externa, comprobar el estado de los componentes internos y sus conexiones, actualización de software y firmware.
- Emitir registro de las actividades realizadas y sus novedades, entregar en secretaria.

**Seguridad informática:**
**Responsable:** Encargado de sistemas

- Establecer el cronograma para inspecciones de seguridad informática, se recomienda ejecutarlo cada 6 meses.
- Utilizar software con licencia o de código abierto, evitar en lo posible recurrir software crackeado.
- Mantener actualizados antivirus y antimalware.
- Registrar las actividades relacionadas a instalación o actualización de software y sus novedades.
- Mantener actualizado los sistemas operativos en uso y llevar un registro de cada actualización.
- Definir perfiles de software para los usuarios en función de sus responsabilidades y necesidades.
- Emitir reporte de cada inspección, sus resultados y novedades, entregar en secretaria.

**Seguridad física:**
**Responsable:** Encargado de sistemas

- Mantener los equipos ofimáticos fuera del alcance de terceros y al alcance de los integrantes de la empresa.
- Los equipos ofimáticos deben mantenerse lejos de fuentes de humedad o estática, además de estar protegidos contra golpes y sobretensiones.
- La seguridad física de los dispositivos es responsabilidad del encargado de sistemas con apoyo de los usuarios de cada dispositivo.

- La seguridad física abarca el uso adecuado de los equipos ofimáticos y medidas contra robos.
- Realizar inspecciones al final de cada jornada de trabajo verificando que cada equipo este en su lugar, incluidos sus periféricos y accesorios.
- Emitir reportes semanales del estado actual de los dispositivos, entregar en secretaria.

**Inventariado:**
**Responsable:** Encargado de sistemas

- Llevar a cabo el inventario de los equipos ofimáticos, este abarca computadores, impresoras, etc.
- Registrar la información de cada equipo, incluir modelo, fecha de adquisición, estado actual, uso y especificaciones técnicas.
- Actualizar periódicamente el inventario, sobre todo al adquirir, reparar o modificar los equipos. Trabajo asignado al encargado de sistemas.
- Emitir un reporte cada vez que se actualice el inventario de equipos ofimáticos, entregar en secretaria.

**Seguros:**
**Responsable:** secretaria, encargado de sistemas

- Gestionar los seguros contratados, dar seguimiento a los términos y condiciones de los mismos.
- Evaluar la relación costo beneficio de los seguros contratados, de ser necesario cambiar de aseguradora.
- Actualizar el plan de cobertura en función a los resultados de análisis de riesgos periódicos.
- Emitir un reporte de acciones realizadas y las decisiones tomadas, entregar en secretaria.

**Dispositivos de red:**
**Responsable:** Auxiliar externo

- Uso de dispositivos/accesorios certificados y con garantía.
- Para las conexiones por cable utilizar cable categoría 6 certificado.
- Utilizar las herramientas estándar para montaje de redes.
- Llevar a cabo las instalaciones según las especificaciones de los fabricantes.
- Emitir el reporte de las actividades realizadas, entregar en secretaria.

**Seguridad de la red:**
**Responsables:** Auxiliar externo, encargado de sistemas

- Mantener los dispositivos de red en ubicaciones seguras, evitar exponerlos a fuentes de humedad o estática.
- Uso de contraseñas robustas en todos los dispositivos dentro de la red.
- Mantener firewalls activos en los dispositivos conectados a la red
- Monitorear la red durante las jornadas de trabajo.
- Emitir reportes del estado de la red, sus dispositivos y sus novedades, entregar en secretaria.

**Datos.**
**Responsables:** Auxiliar externo, encargado de sistemas

- Cumplir con las leyes y regulaciones estatales sobre protección de datos.
- El ingreso de datos debe llevarse a cabo bajo las normas y nomenclaturas de la empresa.
- El acceso a la información debe ir acorde al rol de cada usuario del sistema.
- Llevar a cabo copias de seguridad incrementales al final de cada jornada de trabajo y copia de seguridad completa al final de cada semana.
- Almacenar la copia de seguridad en una ubicación segura y de preferencia fuera de la empresa.
- Emitir reportes cada vez que se realice copias de seguridad o se restaure una, entregar en secretaria.

**Accesibilidad.**
**Responsable:** Encargado de sistemas.

- El acceso a los activos de TI debe basarse en los roles de los usuarios.
- Uso de credenciales personales y contraseñas robustas.
- Registrar el acceso de los usuarios a los activos de TI, entregar en secretaria al final de cada jornada de trabajo.

**Recursos de apoyo.**
**Responsables:** Encargado de sistemas, secretaria.

- Mantenerse al día con los pagos de servicios básicos relacionados a los activos de TI.
- Mantener el suministro eléctrico estable, recurrir a sistemas de respaldo si es necesario.
- Uso eficiente de electricidad, apagar los dispositivos que no se estén usando.
- Asignar el ancho de banda necesario en función de la carga de trabajo de cada dispositivo.

**Incendios**
**Responsables:** Encargado de sistemas, secretaria.

- Inspeccionar las instalaciones eléctricas de forma frecuente y mantenerlas en buen estado.
- Contar con una copia de seguridad reciente de los datos de la empresa
- Contar con pólizas de seguros para todos los activos de TI o al menos los más importantes.
- Mantener extintores cargados en puntos estratégicos.
- Uso de detectores de humo.
- Almacenar combustibles y materiales inflamables en una locación segura y lejos de la infraestructura de TI

**Desastres naturales**
**Responsables:** Encargado de sistemas, secretaria.

- Contar con una copia de seguridad reciente de los datos de la empresa
- Contar con pólizas de seguros para todos los activos de TI o al menos los más importantes.

**Saqueos:**
**Responsables:** Encargado de sistemas, secretaria.

- Contar con una copia de seguridad reciente de los datos de la empresa
- Contar con pólizas de seguros para todos los activos de TI o al menos los más importantes.
- Mantener activas las medidas de seguridad las 24 horas del día.

**Políticas Correctivas:**

**Correcciones:**

**Responsables:** Encargado de sistemas, auxiliares externos.

- En caso de eventos adversos llevar a cabo las actividades detalladas por cada activo de TI.
- Los responsables asignados a cada actividad deben presentar un reporte de las actividades realizadas y sus novedades.
- El plan de contingencia se debe actualizar en base a los reportes y novedades.

**Incendios y desastres naturales**

**Responsables:** Encargado de sistemas, secretaria.

- Evaluar los daños causados a la infraestructura de TI e inventario ofimático.
- Listar los dispositivos afectados, separar los dispositivos que se pueden reparar de los que no.

- Contactar con proveedores o aseguradoras según sea necesario.
- Buscar una locación provisional para continuar con las operaciones de la empresa.
- Contactar con los auxiliares externos correspondientes y planificar el reacondicionamiento o montaje de la infraestructura de TI.

**Saqueos:**
**Responsables:** Encargado de sistemas, secretaria.

- Identificar las pérdidas de inventario ofimático y daños a la infraestructura de TI.
- Emitir un registro de las pérdidas y daños identificados.
- Contactar con proveedores o aseguradoras según sea necesario.
- Contactar con los auxiliares externos correspondientes y planificar el reacondicionamiento o montaje de la infraestructura de TI.

## Anexo 23: Metodología para la gestión de riesgos

## Contenido

**Introducción:**

La presente metodología define los pasos a seguir para la gestión de riesgos de las tecnologías de la información (TI) presentes en la empresa, facilitando la toma de decisiones ante sucesos que detengan parcial o totalmente las actividades de la empresa.

En necesario aclarar que el presente documento se basa en la integración de las metodologías COBIT 5 e ITIL v4, representando una guía genérica que se puede utilizar en otras empresas.

**Objetivo:**

Establecer una guía para la gestión de riesgos de TI, misma que mediante las mejores prácticas faciliten la mitigación de los diferentes riesgos y problemas relacionados a la infraestructura de TI e inventario ofimático de la empresa.

**Alcance:**

La presente metodología se enfoca en el proceso para la identificación, evaluación, análisis y gestión de riesgos de TI derivados del uso de inventario ofimático en procesos críticos dentro de una empresa o institución, estableciendo lineamientos claros para poner en práctica el proceso.

**Definiciones y términos:**

**Inventario ofimático:**

Hardware o software especializado destinado al uso empresarial o de oficina.

**Activo de TI:**

Todo aquel elemento de inventario ofimático importante para el funcionamiento de la empresa.

**Gobierno de TI:**

Conjunto de prácticas, procesos y políticas para la correcta administración de activos de TI e inventario ofimático.

**Partes interesadas:**

Cualquier integrante de la empresa o cliente de la misma.

**Diagrama de procesos:**

Organizador gráfico que describe una serie de actividades, herramientas y responsables relacionados entre sí.

**Principios para la gestión de riesgos:**

Establecer el contexto.

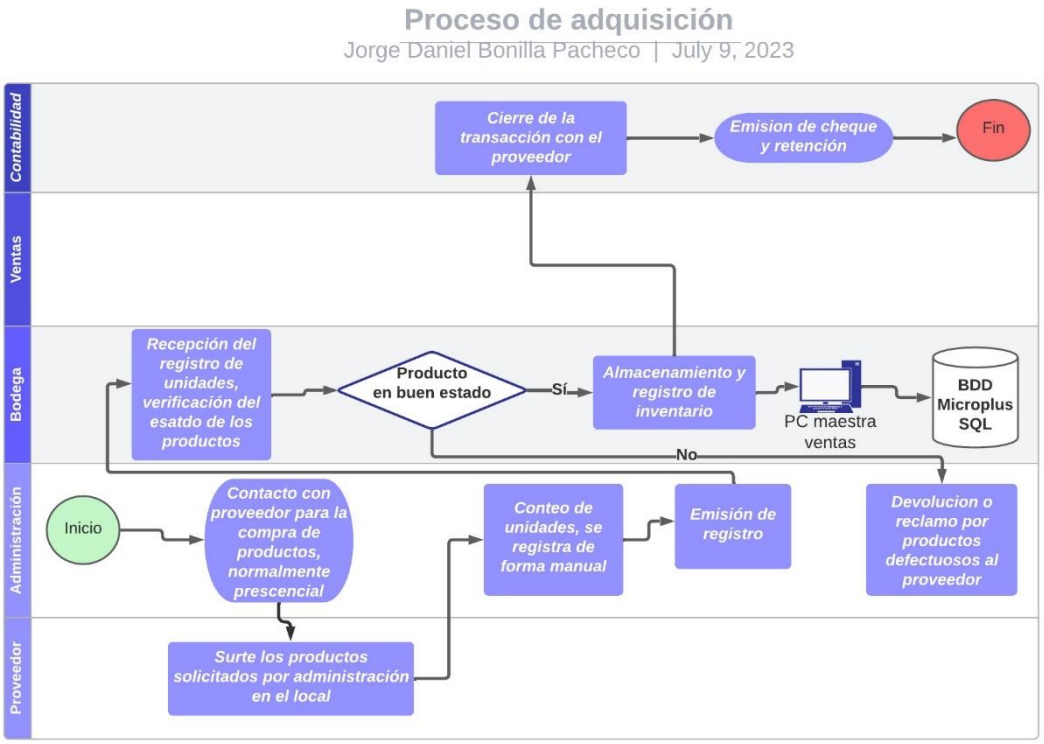
En esta etapa se identifican y comprometen las partes interesadas de la empresa, los requerimientos, estado actual de la empresa y una noción del futuro gobierno de TI.

Entre las actividades necesarias en esta etapa se encuentran:

- Análisis e identificación de factores internos y externos del entorno, así como tendencias de negocio con potencial para influir en la gestión de riesgos de TI.
- Definir la relevancia de TI y su rol en relación al negocio.
- Considerar regulaciones externas, obligaciones legales y contractuales, determinar cómo aplicarlas en la gestión de riesgos de TI.
- Alinear uso y procesamiento ético de la información y su impacto en las partes interesadas internas y externas con los objetivos, visión y dirección de la empresa.
- Establecer los principios guía para la toma de decisiones sobre riesgos de TI.
- Analizar la cultura empresarial para toma de decisiones de TI.
- Establecer niveles para delegación de autoridad, incluyendo reglas de umbrales, para las decisiones de TI.

El resultado sugerido para estas actividades es el diagrama de proceso, pues en este se incluyen responsables o departamentos involucrados, inventario ofimático utilizado, activos de TI y las actividades correspondientes.

**Ejemplo:**




**Identificación de activos de TI en este proceso:**

- Pc maestro ventas
- Servidor sistema de facturación
- BD sistema de facturación.
- Modem
- Switch
- Cables de red

En este ejemplo se describe el proceso de adquisición de productos de la empresa, se distingue claramente los departamentos involucrados, las actividades necesarias, toma de decisiones y los activos de TI o inventario ofimático necesario.

**Identificación de riesgos.**

En esta etapa se identifican y recopilan datos de riesgos potenciales relacionados al uso de inventario ofimático, se incluye además la probabilidad e impacto de los mismos.

Entre las actividades necesarias en esta etapa se encuentran:

- Establecer un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, este puede incluir la frecuencia esperada e impacto potencial.
- Registrar datos relevantes del entorno de operación interno y externo de la empresa que puedan influir en la gestión del riesgo de TI.
- Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI.
- Determinar las causas de los eventos de riesgo y su impacto en la frecuencia del evento y la magnitud de perdida.

El resultado sugerido para estas actividades es un listado de riesgos, este listado se basa en los activos de la empresa previamente identificados en los diagramas de procesos. Cada riesgo incluye una breve descripción de sus causas y consecuencias.

**Ejemplo:**

**R1.** Errores humanos leves: Cualquier error menor en el ingreso de datos, errores tipográficos, errores de consulta o errores de archivado que causan dificultades leves en las operaciones de la empresa

**R2.** Errores humanos moderadores: Cualquier error relacionado a perdida o borrado de archivos importantes, inserción de datos erróneos o configuraciones de servidores causan dificultades menores.

**R3.** Errores humanos graves: Cualquier error significativo para las operaciones de TI, como el borrado de una o más BD, errores en la gestión de usuarios, falta de medidas de seguridad en la red implican dificultades mayores que pueden detener las operaciones de la empresa por periodos prolongados junto al impacto económico moderado.

**R4.** Errores humanos críticos: Cualquier error severo que comprometa la integridad parcial o total del sistema, estos causan dificultades graves que detienen las operaciones por periodos prolongados e implican un impacto económico grave para la empresa.

**R5.** Robo o perdida de periféricos: Implica costos y dificultades para las operaciones de la empresa.

En este ejemplo se asigna un identificador único para el riesgo, seguido se describe brevemente en que consiste, sus causas y posibles consecuencias.

**Evaluación de riesgos.**
Una vez identificados los riesgos, es necesario identificar la tolerancia de riesgo de la organización y establecer criterios para aceptar o rechazar riesgos.

**Nota:** Aceptar riesgos se refiere a que la empresa está en capacidad de resolverlos con sus propios recursos y personal, mientras que rechazar el riesgo consiste en contratar servicios de terceros o personal externo para afrontar los riesgos.

Entre las actividades necesarias en esta etapa se encuentran:

- Determinar y documentar la capacidad de riesgo y el apetito de riesgo que la empresa está dispuesta a asumir para cumplir sus objetivos.
- Determinar los servicios TI y recursos de infraestructuras de necesarios para los procesos de negocio. Identificar vulnerabilidades.
- Evaluar factores de riesgo TI previo a la toma de decisiones estratégicas pendientes.
- Analizar costo-beneficio de las actividades ante riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar

El resultado sugerido para estas actividades es una matriz en donde se describa brevemente como afecta el riesgo identificado a los procesos críticos de la empresa. Además de una matriz adicional que muestre los activos de TI o inventario ofimático afectado por los riesgos identificados.

**Ejemplo:**

| Procesos / Riesgos | Adquisición | Ventas | Facturación | Transacciones | Reembolso | Seguridad |
|---|---|---|---|---|---|---|
| **R1** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |
| **R2** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |
| **R3** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas. Discrepancias en el registro contable. Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **R4** | Discrepancias en el inventario. | Fallos a la hora de realizar ventas | Fallos a la hora de emitir facturas | Discrepancias en el registro de transacciones | Discrepancias en el registro de ventas.<br>Discrepancias en el registro contable.<br>Ralentización de los reembolsos. | Brechas de en el sistema de seguridad. |
| **R5** | Ralentización del ingreso de nuevos productos.<br>Robo o perdida de información de inventario. | Ralentización en la generación de nuevas ventas.<br>Robo o perdida de información de ventas. | Ralentización en la generación de nuevas facturas.<br>Robo o perdida de información de facturación. | Ralentización en el proceso contable.<br>Robo o perdida de información contable. | Ralentización de los reembolsos.<br>Robo o perdida de información de notas de crédito. | Brechas en el sistema de seguridad.<br>Reducción del alcance de la videovigilancia. |

En este ejemplo se incluyen las consecuencias más generales en función de los riesgos y procesos, en este caso se aplica los identificadores definidos previamente.

| Elementos / Riesgos | Servidor sistema de facturación | BD sistema de facturación | PCs contadoras | PC secretaria | PC cobros | PCs ventas | Modem | Switches | Cables de red | Cámaras IP | PC videovigilancia |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **R1** | | | | | | | | | | | |
| **R2** | | | | | | | | | | | |
| **R3** | | | | | | | | | | | |
| **R4** | | | | | | | | | | | |
| **R5** | | | | | | | | | | | |

**Análisis de riesgos**

Tras la evaluación de los riesgos el siguiente paso comprender la naturaleza de los mismos y su impacto en la empresa.

Entre las actividades necesarias en esta etapa se encuentran:

- Considerar todos los factores de riesgo y su impacto en el negocio. Definir el alcance del análisis de riesgos basado en el análisis costo-beneficio.
- Plantear escenarios de riesgo de TI, que incluyan escenarios compuestos o amenazas coincidentes
- Determinar la frecuencia y magnitud de pérdida o ganancia bajo escenarios de riesgos de TI.

El resultado sugerido para estas actividades son tablas de probabilidad e impacto o tablas de priorización, las cuales se pueden generan aplicando la metodología Delphi, al cual consiste en establecer una escala tanto para la probabilidad como para el impacto de los riesgos identificados, se recomienda trabajar con un numero impar de personas que califiquen los riesgos dentro de la escala definida, misma que debe contar con pocos niveles.

Posteriormente se promedian las calificaciones obtenidas y se clasifican los riesgos según su criticidad, la cual se recomienda representar un mapa de calor.

Además, es necesario identificar los problemas de TI en base a los activos de TI de la empresa y ubicarlos en los riesgos identificados.

**Ejemplo:**

| Riesgo ID | Encargado de TI | | Contadora | | Investigador | | Consultor 1 | | Consultor 2 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto | Probabilidad | Nivel de impacto |
| **R1** | 2 | 1 | 1 | 1 | 3 | 1 | 4 | 1 | 4 | 3 |
| **R2** | 1 | 2 | 1 | 1 | 2 | 1 | 4 | 2 | 3 | 3 |
| **R3** | 3 | 2 | 2 | 2 | 2 | 3 | 3 | 4 | 4 | 4 |
| **R4** | 3 | 4 | 2 | 2 | 2 | 4 | 2 | 5 | 3 | 5 |
| **R5** | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 3 |

En este ejemplo se trabaja con 5 personas, 2 integrantes de la empresa con un rol más activo en los procesos de la empresa y consultores externos, estas calificaciones se promedian posteriormente.

| Riesgo ID | Nombre riesgo | Probabilidad | Nivel de impacto | Calificación | Nivel de riesgo |
|---|---|---|---|---|---|
| **R13** | Spyware | 4 | 3 | 4;3 | Alto |
| **R31** | Acceso no autorizado a la data center | 2 | 5 | 2;5 | Alto |
| **R3** | Errores humanos graves | 3 | 3 | 3;3 | Medio |
| **R4** | Errores humanos críticos | 2 | 4 | 2;4 | Medio |
| **R6** | Robo o perdida de CPUs y sus componentes | 2 | 3 | 2;3 | Medio |

Breve ejemplo de cómo se clasifican los riesgos tras el análisis.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Impacto** | **5** | **Critico** | | R31 | | | |
| | **4** | **Grave** | R22, R29 | R4, R25 | R12, R28 | | |
| | **3** | **Moderado** | R16, R23, R24, R27 | R6, R15, R17, R18, R26, R32 | R3, R8, R11, R30 | R13 | |
| | **2** | **Leve** | R5, R19, R21 | R2, R7, R10, R14, R20 | | | |
| | **1** | **Muy leve** | | R9 | R1 | | |
| | | | **1% - 20%** | **21% - 40%** | **41% - 60%** | **61% - 80%** | **81% - 100%** |
| | | | **1** | **2** | **3** | **4** | **5** |
| | | | **Probabilidad** | | | | |

Ejemplo de matriz probabilidad/impacto o de priorización de riesgos.

| Riesgo ID | Nombre riesgo | Problemas | Nivel de riesgo |
|---|---|---|---|
| R13 | Spyware | • **Bajo rendimiento**<br>• **Corrupción de datos**<br>• **Perdida de datos**<br>• **Inconsistencia de datos** | Alto |
| R31 | Acceso no autorizado a la data center | • **Corrupción de datos**<br>• **Perdida de datos**<br>• **Inconsistencia de datos**<br>• **Accesos no autorizados a la base de datos**<br>• **Problemas de rendimiento de la base de datos** | Alto |
| R3 | Errores humanos graves | • **VLAN mal configurada** | Medio |
| R4 | Errores humanos críticos | • **Problemas de seguridad (modem)**<br>• **Problemas de seguridad (switch)** | Medio |
| R6 | Robo o perdida de CPUs y sus componentes | • **Robo o perdida de CPUs** | Medio |

Ejemplo de problemas de TI identificados y clasificados.

**Planificación de la gestión de riesgos.**
En esta etapa se definen políticas, planes, procesos y herramientas para prevenir, detectar y reducir el impacto de los riesgos de TI.

Entre las actividades necesarias en esta etapa se encuentran:

- Definir un inventario de actividades de control que se alineen con el apetito y tolerancia de riesgo.
- Determinar si cada unidad organizativa supervisa el riesgo dentro de sus niveles de tolerancia individuales.
- Generar propuestas para reducir el riesgo, o proyectos que den paso a oportunidades estratégicas empresariales, considerando costo/beneficio y su impacto en el perfil de riesgo actual.
- Generar planes con pasos específicos a seguir cuando un evento de riesgo cause un incidente significativo a nivel operativo.
- Clasificar los incidentes en base a exposiciones reales y a la capacidad de riesgo. Comunicar los impactos en el negocio a los responsables de actualizar el perfil de riesgo.
- Aplicar plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.

El resultado sugerido para estas actividades es instructivo para prevención, detección y corrección, los cuales cuentan con tablas en las que se detallan los componentes de los activos identificados y sus problemas, así como sus actividades de prevención, detección y corrección.

Adicional es necesario definir políticas de apoyo para estas actividades, las cuales establecen lineamientos para facilitar la gestión de riesgos de TI

**Ejemplo:**

- Problemas y procedimientos preventivos para PCs

| Componente | Problema | Procedimientos | Seguros | Proveedores |
|---|---|---|---|---|
| CPU | Sobrecalentamiento | • Control de temperatura<br>• Mantenimiento preventivo<br>• Alimentación estable<br>• Firmware y drivers actualizados<br>• Seguridad informática<br>• Protocolo de uso<br>• Seguridad física<br>• Inventariado y etiquetado<br>• Capacitación<br>• Respaldo de datos | • Seguros Condor – Corporativo e industrias - Equipo electrónico<br>• Zurichseguros – Seguro de equipo electrónico para empresas<br>• Pointer – Seguro PYMES<br>• Seguros Unidos – Su PYME | • SagaPC<br>• Novicompu<br>• Smart PC Store<br>• La casa del computador |
| | Fallos de ventiladores | | | |
| | Fallo de la fuente de poder | | | |
| | Pantallazo azul | | | |
| | Bloqueo del sistema | | | |
| | Error de arranque | | | |
| | Bajo rendimiento | | | |
| | Ruido excesivo del ventilador | | | |
| | Fallas de la tarjeta madre | | | |
| | Puertos inoperables | | | |
| | Fallas de procesador | | | |
| | Procesador incompatible | | | |
| | Fallos de disco duro | | | |
| | Fallos de memoria RAM | | | |
| | Fallos de tarjeta gráfica | | | |
| | Fallos de la fuente de poder | | | |
| | Fallos de la tarjeta de red | | | |
| | Fallas de la BIOS | | | |
| | Robo o perdida | | | |

En ese ejemplo se incluye el componente, los problemas relacionados al mismo, los procedimientos a ejecutar, seguros y proveedores.

- **Procedimientos preventivos detallados para PCs**

| Componente | Procedimiento | Pasos | Hardware | Software |
|---|---|---|---|---|
| CPU | Control de temperatura | • Verificar que el equipo se ventile correctamente, comprobar la circulación de aire.<br>• Comprobar el estado de ventiladores y disipadores de calor, limpiarlos de ser necesario.<br>• Con ayuda de herramientas para monitoreo de temperatura verificar los valores térmicos del CPU. | • CPU.<br>• Ventiladores<br>• Disipador de calor<br>• Tarjeta madre compatible.<br>• Fuente de poder | • Sistema operativo actualizado.<br>• Drivers actualizados.<br>• Antivirus y antimalware.<br>• Herramientas de monitoreo y diagnostico (CPU-Z, HWMonitor, CrystalDiskInfo, Seatools, Prime95, AIDA64, administrador de tareas,).<br>• Software para diagnóstico (Memest86, funciones integradas del sistema operativo) |
| | Mantenimiento preventivo | • Definir un periodo regular para el mantenimiento.<br>• Limpiar los componentes internos con ayuda de aire comprimido y brochas, entre los componentes se incluye ventiladores y disipadores de calor.<br>• Comprobar el estado de los cables y sus conexiones.<br>• Evaluar el funcionamiento en busca de irregularidades como ruidos extraños o temperatura elevada.<br>• Registrar las actividades realizadas, incluyendo resultados. | | |
| | Alimentación estable | • Comprobar el estado de las toma corrientes, evitar sobrecargar las mismas<br>• Utilizar reguladores de voltaje para prevenir los picos de tensión. | | |

| | | | | |
|---|---|---|---|---|
| | | • Utilizar UPS para evitar daños por cortes de electricidad<br>• Mantener cables y conexiones eléctricas en buen estado<br>• Reemplazar fuentes de poder defectuosas de ser necesario. | | |
| | Firmware y drivers actualizados | • Definir un periodo regular para las actualizaciones.<br>• Comprobar el estado de firmware y controladores.<br>• Verificar que las versiones disponibles sean compatibles con el hardware en uso.<br>• Actualizar siguiendo las instrucciones del fabricante,<br>• Registrar las actualizaciones ejecutadas y sus novedades. | | |
| | Seguridad informática | • instalar antivirus y mantenerlo actualizado.<br>• Definir un periodo regular para escaneos de virus y malware.<br>• Capacitar a los usuarios en materia de seguridad informática.<br>• Implementar mecanismos de seguridad como cortafuegos o entre otros para evitar accesos no autorizados.<br>• Ejecutar auditorias de seguridad periódicas en busca de vulnerabilidades y corregirlas | | |
| | Protocolo de uso | • Establecer reglas para los usuarios del inventario ofimático. | | |

| | | | | |
|---|---|---|---|---|
| | | • Capacitar a los usuarios en materia de instalación y actualización de componentes.<br>• Promover el uso de pulseras antiestáticas a la hora de realizar mantenimientos.<br>• Definir un proceso para reportes de daños físicos o mal funcionamiento. | | |
| | Seguridad física | • Mantener el CPU en una ubicación segura, esta debe permitir el acceso solo a personal autorizado.<br>• La ubicación debe proteger al dispositivo ante situaciones y condiciones adversas.<br>• Utilizar candados para cada CPU<br>• Instalar cerraduras de calidad en el inmueble.<br>• Mantener un sistema de videovigilancia en el inmueble. | | |
| | Inventariado y etiquetado | • Llevar un inventario actualizado de los CPUs y sus componentes, esto incluye registrar números de serie de los componentes.<br>• Etiquetar claramente los CPUs y sus componentes | | |
| | Capacitación | • Mantener capacitado al personal en materia de seguridad y protección de equipos, hacer énfasis en los riesgos asociados.<br>• Definir un canal de comunicación para reportes de robos o perdidas. | | |
| | Respaldo de datos | • Definir el plan de acción para el respaldo de la información almacenada. | | |

| | | | | |
|---|---|---|---|---|
| | | • Mantener las copias de seguridad en una locación segura, de preferencia contratar servicios en de almacenamiento en la nube. | | |

La presente tabla es el complemento de os procedimientos propuestos, aquí se definen los pasos a seguir además de especificar hardware y software necesario.

- **Problemas, síntomas y detección - PCs**

| **Componente** | **Problema** | **Síntomas** | **Detección** |
|---|---|---|---|
| CPU | Sobrecalentamiento | • Sistema lento<br>• Reinicios esporádicos<br>• Pantallas de error o congeladas<br>• Ventilador ruidoso | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Si el dispositivo cuenta con opciones de monitoreo activarlas tanto en la BIOS como en la configuración del sistema operativo. |
| | Fallos de ventiladores | • Sobrecalentamiento de CPU<br>• Ruidos fuera de lo normal<br>• Cambios en la velocidad<br>• Reinicios esporádicos<br>• Pantallas de error o congeladas | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Inspección física. |

| | | | |
|---|---|---|---|
| | Bloqueo del sistema | • Pantallas de error o congeladas<br>• Sistema lento<br>• Reinicios esporádicos<br>• Pantallazo azul | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Revisar el registro de eventos del sistema en busca de errores o advertencias.<br>• Mantener los controladores actualizados a la versión más reciente. |
| | Bajo rendimiento | • Ejecución lenta de tareas sencillas.<br>• Tiempos de respuesta prolongados.<br>• Carga excesiva de CPU. | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Mantener los controladores actualizados a la versión más reciente. |
| | Fallas de la tarjeta madre | • Fallas de alimentación o dificultades de arranque.<br>• Problemas de funcionamiento de dispositivos conectados por USB.<br>• Fallas de audio y video.<br>• Fallas de sistema como reinicios esporádicos, errores de memoria o bloqueos. | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Analizar los mensajes de error durante el proceso de arranque.<br>• Inspección física de la tarjeta madre.<br>• Someter la tarjeta a pruebas de diagnóstico en busca de problemas específicos. |
| | Puertos inoperables | • El sistema operativo no reconoce dispositivos conectados por USB y otros puertos. | Espontaneo/ indetectable |

| | | | |
|---|---|---|---|
| | | • Baja velocidad de transferencia de datos.<br>• Fallas de conectividad de red<br>• Fallas en la señal de video. | |
| | Fallas de procesador | • Reinicios esporádicos<br>• Pantallas de error o congeladas<br>• Pantallazo azul<br>• Bajo rendimiento<br>• Temperatura excesiva del procesador | • Mantener activas y actualizadas las herramientas de monitoreo (CPU-Z, HWMonitor, administrador de tareas).<br>• Revisar con frecuencia los reportes de pruebas de estrés con software especializado (CPU-Z, Prime95, AIDA64).<br>• Mantener firmware y controladores actualizados.<br>• Inspección física del procesador. |
| | Fallos de disco duro | • Ruidos fuera de lo normal.<br>• Tiempo de respuesta prolongado del sistema<br>• Perdida de datos<br>• Fallas de lectura y escritura | • Mantener activas y actualizadas las herramientas de monitoreo y diagnostico (CrystalDiskInfo, Seatools). |
| | Fallos de memoria RAM | • Reinicios esporádicos<br>• Pantallazo azul<br>• Bloqueos de sistema frecuentes<br>• Errores de ejecución<br>• Corrupción o perdida de información. | • Ejecutar con frecuencia pruebas de diagnóstico a las memorias RAM con software especializado (Memest86) o funcionalidades integradas en el sistema operativo.<br>• Revisión física de la memorias o reemplazo de ser necesario. |
| | Fallos de tarjeta gráfica | • Distorsiones de imagen fijas o intermitentes. | • Comprobar el funcionamiento de la tarjeta con ayuda de otros dispositivos. |

| | | | |
|---|---|---|---|
| | | • Ausencia total de imagen (pantalla negra)<br>• Ralentización o bloqueo de aplicaciones que requieren recursos gráficos.<br>• Reinicios esporádicos | • Mantener los controladores actualizados a la versión más reciente.<br>• Revisión física de la tarjeta gráfica. |
| | Fallos de la fuente de poder | • Problemas de arranque por falta de energía.<br>• Reinicios esporádicos.<br>• Ruidos fuera de lo normal.<br>• Olor a quemado o humo saliendo de la fuente de poder.<br>• Sistema bloqueado o inestable. | • Revisión física de la fuente de poder, comprobar que la salida de voltaje este dentro de los limites adecuados. |
| | Fallos de la tarjeta de red | • Fallas de conectividad de red<br>• Baja velocidad de transferencia de datos.<br>• Red inestable.<br>• Perdida y corrupción de paquetes.<br>• Retraso en la comunicación. | • Revisión física de la tarjeta de red y de los cables de red.<br>• Mantener los controladores actualizados a su última versión.<br>• Verificar el estado de la conexión con ayuda de otros dispositivos.<br>• Someter a los equipos y cables de red a pruebas de diagnóstico. |

| | | | |
|---|---|---|---|
| | Fallas de la BIOS | • Errores de arranque del sistema.<br>• Cambios inesperados en la configuración de la BIOS.<br>• Dispositivos no reconocidos por la BIOS.<br>• Mensajes de error durante el arranque del sistema.<br>• Dificultad o imposibilidad de actualizar a BIOS. | • Revisión física de la tarjeta madre.<br>• Mantener actualizada la BIOS. |

Segunda parte de la planificación, aquí se detallan los síntomas de los problemas detectados por cada componente y los elementos necesarios para su detección.

- **Problemas, solución - PCs**

| Componente | Problema | Solución | Responsables | Tiempo de respuesta |
|---|---|---|---|---|
| CPU | Sobrecalentamiento | • Proceso de mantenimiento general para CPU | • Encargado de sistemas<br>• Ing. Roberto Pico | Entre 24 y 36 horas en días hábiles |
| | Fallos de ventiladores | • Proceso de mantenimiento general para CPU | | |
| | Fallo de la fuente de poder | • Proceso de mantenimiento general para CPU | | |
| | Pantallazo azul | • Reiniciar el sistema<br>• Actualizar o reinstalar drivers de hardware<br>• Analizar el sistema en busca de virus o malware<br>• Restaurar el sistema a un punto de tiempo anterior al problema | | |
| | Bloqueo del sistema | • Reiniciar el sistema<br>• Verificar compatibilidad de software y controladores instalados, actualizarlo de ser necesario.<br>• Analizar el sistema en busca de virus o malware<br>• Verificar el estado del disco duro, repararlo de ser necesario | | |
| | Error de arranque | • Proceso de mantenimiento general para CPU | | |
| | Bajo rendimiento | • Proceso de mantenimiento general para CPU | | |
| | Ruido excesivo del ventilador | • Proceso de mantenimiento general para CPU<br>• Acceder a la BIOS y revisar la configuración. | | |

| | | | | |
|---|---|---|---|---|
| | Fallas de la tarjeta madre | • Proceso de mantenimiento general para CPU<br>• Reemplazar la tarjeta de ser necesario | | |
| | Puertos inoperables | • Proceso de mantenimiento general para CPU | | |
| | Fallas de procesador | • Proceso de mantenimiento general para CPU<br>• Reemplazar el procesador de ser necesario | | |
| | Procesador incompatible | • Revisar la versión de la BIOS y actualizarla de ser necesario con ayuda de las instrucciones del fabricante<br>• Revisar la compatibilidad del procesador con la tarjeta madre. | | |
| | Fallos de disco duro | • Proceso de mantenimiento general para CPU<br>• Analizar el disco en busca de errores y repararlos | | |
| | Fallos de memoria RAM | • Proceso de mantenimiento general para CPU<br>• Revisar la compatibilidad de la memoria RAM con la tarjeta madre | | |
| | Fallos de tarjeta gráfica | • Proceso de mantenimiento general para CPU<br>• Revisar la compatibilidad de la tarjeta gráfica con la tarjeta madre<br>• Reemplazar la tarjeta gráfica de ser necesario | | |
| | Fallos de la fuente de poder | • Proceso de mantenimiento general para CPU<br>• Reemplazar la fuente de poder de ser necesario | | |
| | Fallos de la placa de red | • Proceso de mantenimiento general para CPU<br>• Revisar la configuración de red | | |
| | Fallas de la BIOS | • Acceder a la BIOS y revisar la configuración | | |

| | | | | |
|---|---|---|---|---|
| | | • Revisar la versión de la BIOS y actualizarla de ser necesario con ayuda de las instrucciones del fabricante | | |
| | Robo o perdida de CPU | • Notificar a gerencia del evento<br>• Cambiar contraseñas de cuentas activas.<br>• Inhabilitar acceso remoto a la red en caso de estar activo.<br>• Contactar a la aseguradora o proveedor según corresponda. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 24 y 48 horas en días hábiles |
| | Incendios | • Evaluar el daño causado a los CPUs e identificar los componentes más afectados.<br>• Emitir reporte de los daños a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda.<br>• Búsqueda de locación provisional para continuar con las operaciones. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |
| | Desastres naturales | • Evaluar el daño causado a los CPUs e identificar los componentes más afectados.<br>• Emitir reporte de los daños a gerencia.<br>• Contactar a la aseguradora o proveedor según corresponda.<br>• Búsqueda de locación provisional para continuar con las operaciones.<br>• Búsqueda de locación provisional para continuar con las operaciones. | • Encargado de sistemas<br>• Proveedor o representante aseguradora | Entre 3 y 4 días hábiles |
| | Saqueos | • Evaluar las pérdidas de CPUs.<br>• Emitir reporte de pérdidas a gerencia. | • Encargado de sistemas | Entre 3 y 4 días hábiles |

| | | | | |
|---|---|---|---|---|
| | | • Contactar a la aseguradora o proveedor según corresponda. | • Proveedor o representante aseguradora | |

Tercera parte de la planificación, se detallan las actividades correctivas para cada problema detectado, se define los encargados y el tiempo de respuesta de los mismos.

**Nota:** La empresa del caso de estudio no cuenta con departamento de TI, por lo cual recurren a servicios de terceros, por ende los tiempos de respuesta tienen a ser prolongados. En caso de contar con departamento de TI es necesario llevar un histórico de sucesos problemáticos, del cual se obtendrá tiempos de respuesta más cortos.

- Procedimientos correctivos

**Proceso de mantenimiento general para CPU:**
**Responsable:** Auxiliar externo.

- Limpieza externa: Con ayuda de paños suaves, brochas o compresores de aire limpiar polvo y suciedad presente en la superficie externa del dispositivo, ranuras de ventilación y puertos.
- Limpieza interna: Abrir el dispositivo según las especificaciones del fabricante, con ayuda de brocha o compresor de aire limpiar los componentes internos del dispositivo, estos incluyen ventiladores, disipadores de calor, tarjeta madre, etc.
- Verificar conexiones: Revisar cables internos y externos en busca de daños o desperfectos, comprobar que estén conectados correctamente, reemplazar cables dañados si hace falta.
- Verificar componentes: Examinar físicamente componentes como conectores, memorias RAM, discos duros, placa madre, en busca de daños o desgaste de los mismos, reemplazar componentes dañados de ser necesario
- Actualizar controladores: Actualizar o reinstalar los controladores de hardware a su versión más reciente para evitar problemas de incompatibilidad y mejorar el rendimiento y seguridad de los dispositivos.
- Comprobar ventilación: Revisar que el dispositivo este ventilado correctamente, revisar que los ventiladores funcionen correctamente y limpiarlos para evitar obstrucciones, reemplazarlos de ser necesario, revisar disipadores de calor y
- Comprobar temperatura: Verificar que la temperatura este dentro los limites aceptables, para esto utilizar software especializado o verificar el sistema de ventilación.
- Respaldar datos: Respaldar los datos de forma periódica en dispositivos externos o servicios en la nube, esto para mantenerlos seguros.

**Proceso de mantenimiento general para monitor:**
**Responsable:** Encargado de sistemas.

- Limpieza: Con el monitor apagado y un paño suave limpiar la pantalla, el marco y la superficie en general, rejillas de ventilación.
- Verificación: Comprobar la calidad de la imagen, debe ser clara y sin distorsiones, comprobar la configuración del monitor y ajustarla según la necesidad. Revisar el estado de los cables y sus conectores.

**Proceso de mantenimiento general para teclado:**
**Responsable:** Encargado de sistemas.

- Limpieza: Con ayuda de un compresor y un cepillo suave limpiar entre las teclas, de ser necesario limpiar tecla por tecla con un paño húmedo.
- Verificación: Comprobar el estado y funcionamiento de las teclas, en caso de fallos volver a limpiar o reemplazar las teclas de ser necesario. Revisar el estado del cable y su conector.
- **Proceso de mantenimiento general para mouse:**
- Limpieza: Con ayuda de un paño suave limpiar la superficie del mouse, con especial enfoque en la zona del sensor óptico.
- Verificación: Comprobar el estado y funcionamiento del mouse, el movimiento del mismo debe ser suave y los botones deben responder de inmediato, caso contrario considerar reemplazarlo. Revisar el estado del cable y su conector.

**Políticas.**

A continuación, se presenta un ejemplo de las políticas que se deben definir.

**Políticas preventivas:**

**Mantenimiento:**
**Responsable:** Encargado de sistemas

- Establecer el cronograma para mantenimiento preventivo de computadores, este abarca CPU y periféricos, se recomienda ejecutarlo cada 6 meses.
- Utilizar herramientas y equipo adecuado para llevar a cabo la actividad, especial atención el uso de pulseras anti estáticas.
- El mantenimiento se limita a limpieza interna y externa, comprobar el estado de los componentes internos y sus conexiones, actualización de software y firmware.

- Emitir registro de las actividades realizadas y sus novedades, entregar en secretaria.

**Políticas Correctivas:**

**Correcciones:**

**Responsables:** Encargado de sistemas, auxiliares externos.

- En caso de eventos adversos llevar a cabo las actividades detalladas por cada activo de TI.
- Los responsables asignados a cada actividad deben presentar un reporte de las actividades realizadas y sus novedades.
- El plan de contingencia se debe actualizar en base a los reportes y novedades.

**Comunicación y consulta.**

Una vez definida la planificación es necesario comunicarlo a las partes interesadas, coordinando las actividades y soluciones propuestas.

Entre las actividades necesarias en esta etapa se encuentran:

- Comunicar cambios y actividades de transición, los cuales incluyen proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
- Recopilar información relacionada a cambios e incidentes TI y comunicarla a las partes interesadas. La comunicación puede ser por medio de informes o reuniones periódicas.
- Coordinar y comunicar actividades operativas, roles y responsabilidades al personal correspondiente.
- Generar un plan de comunicación que defina contenido, frecuencia y destinatarios de la información relacionada a los servicios, incluyendo el estado del valor entregado y los riesgos identificados.

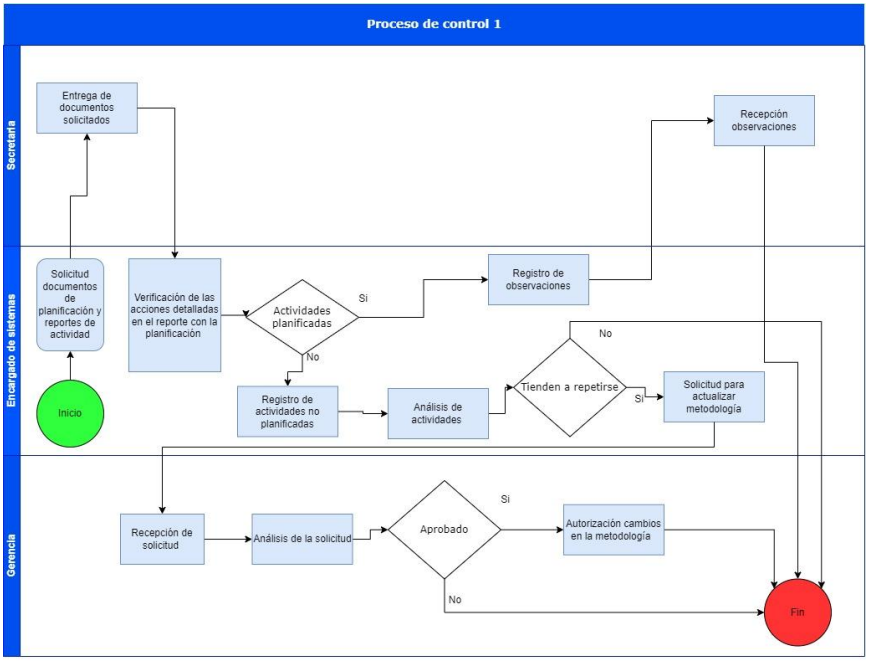
**Monitoreo y revisión.**
La etapa final consiste en definir procesos para supervisar, controlar y evaluar la ejecución de la planificación de la gestión de riesgos y procesos de TI.

Entre las actividades necesarias en esta etapa se encuentran:

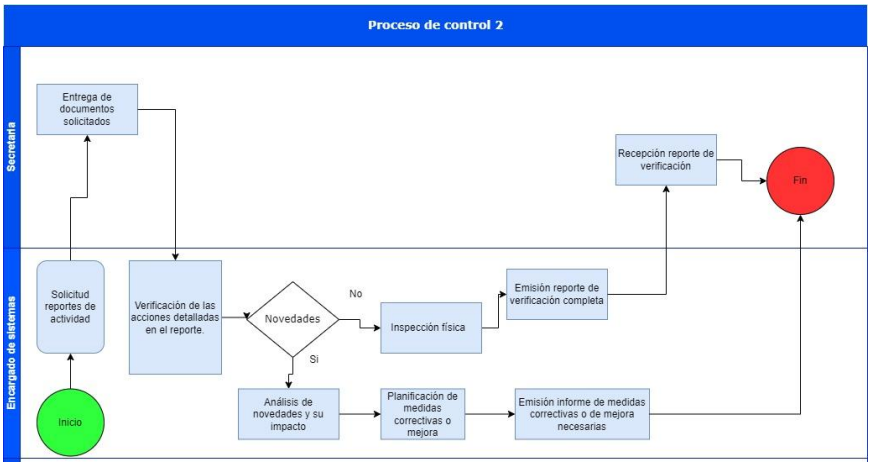
- Definir los objetivos y criterios de monitoreo y revisión, esto incluye el rendimiento de los procesos de TI, cumplimiento de controle, entre otros.
- Recopilar datos relevantes para evaluar el desempeño de los procesos de TI, esto puede incluir métricas, KPIs, entre otros
- Analizar los datos recopilados en busca de patrones, tendencia, posibles desviaciones y áreas de mejora.
- Evaluar la efectividad de los controles implementados en los procesos de TI, asegurando su funcionamiento adecuado para mitigar riesgos.
- Establecer un cronograma de revisiones periódicas.
- Tomar acciones correctivas y preventivas ante posibles desviaciones o deficiencias, esto puede implicar mejoras en los procesos.
- Comunicar los resultados del monitoreo y revisión a las partes interesadas.

El resultado sugerido para estas actividades son diagramas de procesos que detallen las actividades de control, la documentación requerida, los responsables y entregables de ser necesario.

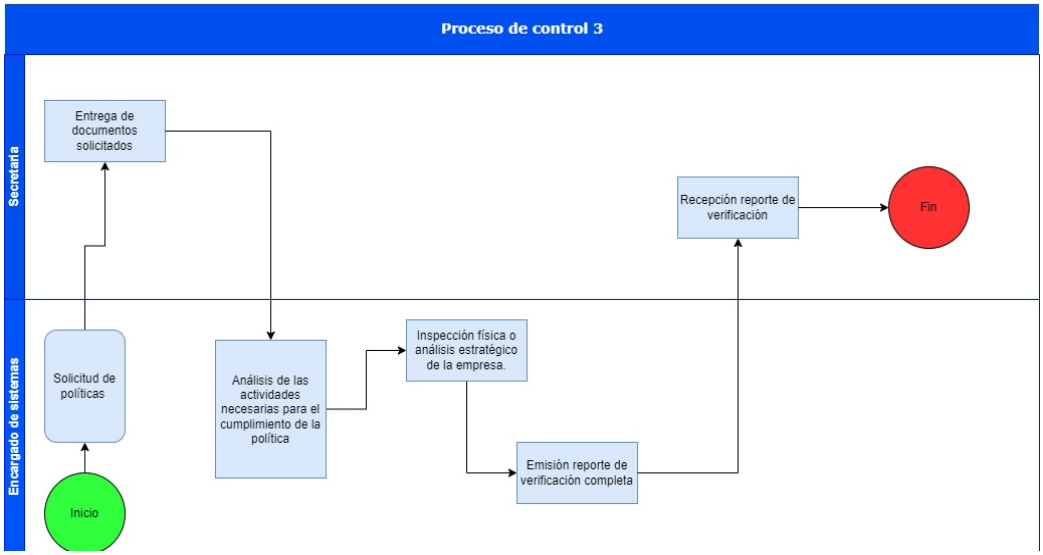
**Procesos de control:**



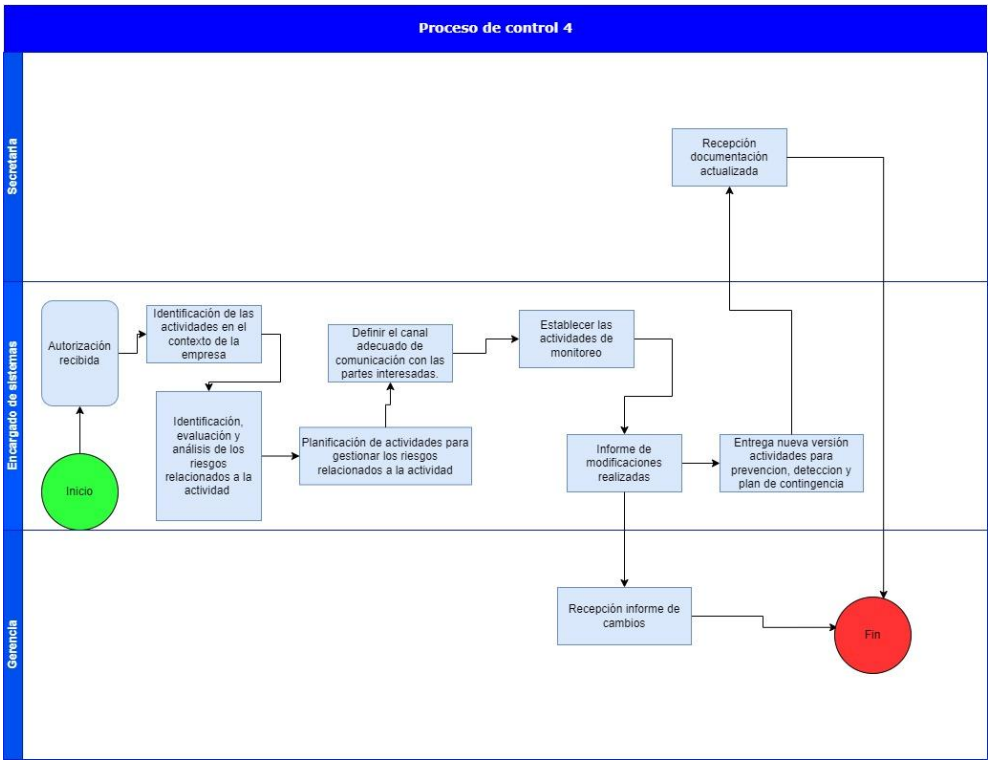

**Descripción:** Proceso de control para actividades que cuenten con planificación y su resultado sea reportes.



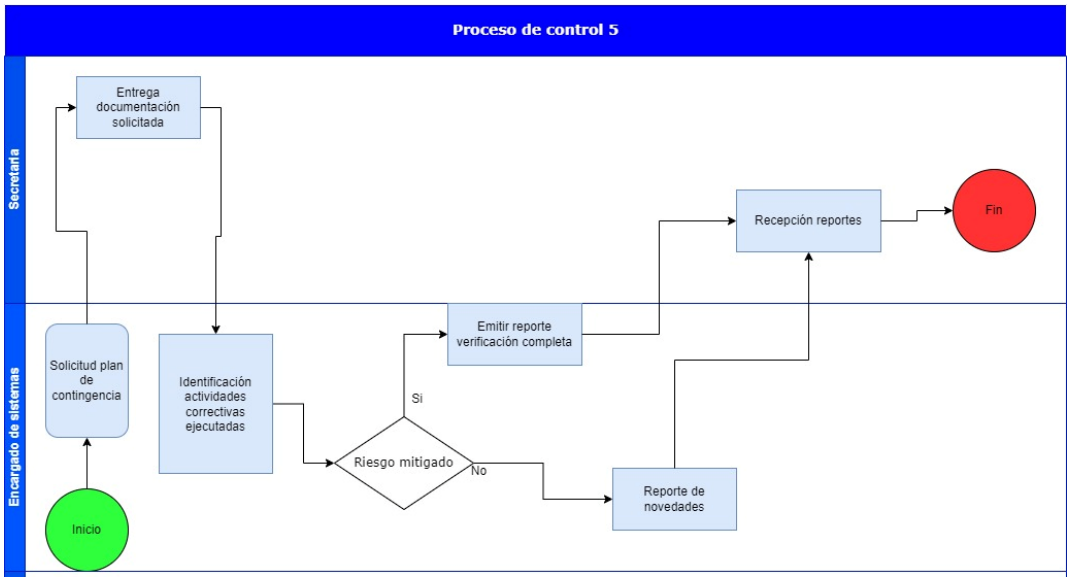

**Descripción:** Proceso de control para actividades sin planificación y su resultado sea reportes.




**Descripción:** Proceso de control para ejecución de políticas.




**Descripción:** Proceso de control para actualización de actividades preventivas, defectivas y plan de contingencia.




**Descripción:** Proceso de control para las actividades del plan de contingencia.