UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL"

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Ingeniero en Sistemas Computacionales e Informáticos

LÍNEA DE INVESTIGACIÓN: Seguridad de Unidades Informáticas

AUTOR: David Noe Cruz Ojeda
TUTOR: Ing. David Omar Guevara Aulestia, Mg

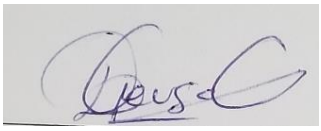
Ambato - Ecuador
2018

CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA
PLASTICAUCHO INDUSTRIAL", del señor DAVID NOE CRUZ OJEDA, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato

Ambato, junio de 2018



Ing. David Omar Guevara Aulestia, Mg

EL TUTOR

AUTORÍA DEL TRABAJO

El presente trabajo de investigación titulado: "PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, junio de 2018

David Noe Cruz Ojeda

CC: 180431011-6

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato Para que haga uso de este trabajo de titulación como un documento disponible para lectura, consulta y procesos de investigación.

Cedo los derechos de autor de mi Trabajo de titulación con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la universidad.

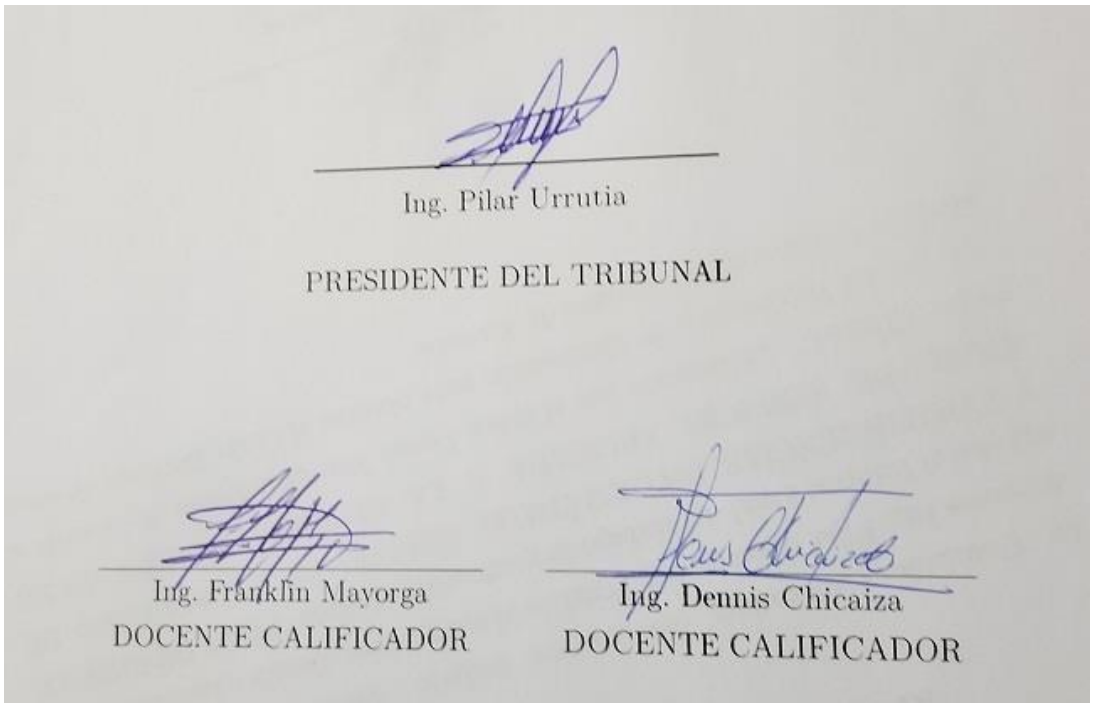
Ambato, junio de 2018

David Noe Cruz Ojeda

CC: 180431011-6

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Pilar Urrutia, Ing. Franklin Mayorga e Ing. Dennis Chicaiza, revisó y aprobó el Informe Final del trabajo de graduación titulado “PLAN DE RIESGOS
Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO
INDUSTRIAL”, presentado por el señor David Noe Cruz Ojeda de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.



DEDICATORIA

A mi madre Lid Ojeda, por ser mi motivación y mi inspiración, por su lucha incansable, su sacrificio y su entrega infinita para de poder brindar un futuro mejor para sus hijos, por apoyarme y darme siempre ese empujón para lograr mis metas.

David Noe Cruz Ojeda

AGRADECIMIENTO

A mi familia por su paciencia, su dedicación y su amor, que han ayudado a que me forje como una persona de bien.

A mis profesores que me guiaron durante la carrera, en especial al Ing. Franklin Mayorga, Ing. Clay Aldas que me brindaron su amistad y su apoyo, especialmente a mi tutor y amigo Ing. David Guevara por su ayuda en este proceso.

A la empresa Plasticaucho Industrial por abrirme sus puertas para que pueda realizar mi trabajo de titulación, especialmente al Ing. William Velasteguí por su apertura y buena disposición con el trabajo; también al Grupo TI 2015 por su motivación para finalizar mi trabajo.

A mis amigos Alexander y Fernando por ser un apoyo incondicional.

David Noe Cruz Ojeda

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la actualidad, el mundo está conformado por un flujo creciente de información y en el contexto empresarial no puede ser de otra manera, conforme las empresas van creciendo acumulan información indispensable para la gestión diaria de las mismas, convirtiéndose en uno de sus principales activos, consecuentemente con este crecimiento, las empresas buscan preservar su continuidad en el tiempo, por lo que ven como una necesidad el salvaguardar la integridad de su información ante los posibles riesgos, que de la misma manera se encuentran presentes, los cuales si no son detectados y controlados a tiempo pueden causar grandes pérdidas en el negocio, para mitigar estos riesgos es necesario contar con una adecuada Gestión de Riesgos para lo cuál existen varios métodos adaptables según el ambiente en la que se desarrolla la empresa.

En el presente trabajo se han descrito los conceptos relacionados a la metodología, estándares y gestión de los riesgos de la seguridad de información que proporcionan guías necesarias que ayudarán a reducir el número de vulnerabilidades a los que los activos se encuentran expuestos. Para una organización es de vital importancia mantener respaldos de la información que posee y la correcta implementación de un plan de contingencias que pueda garantizar la continuidad del negocio.

Por este motivo se ha previsto la necesidad de desarrollar un análisis de riesgos a los que se exponen los activos tecnológicos que componen los servicios que se encuentran en el acuerdo de nivel de servicios de manera cualitativa siguiendo la metodología MAGERIT. Procediendo a identificar los principales activos, otorgándoles un nivel de importancia a los mismos y determinando el impacto que pueden generar y los riesgos potenciales a los que están expuestos.

Finalmente, con este estudio se identifica el nivel de riesgo en que se encuentran los activos, se identifica el nivel de madurez de la seguridad actual y sobre todo se establece un proceso de gestión e implementación referente a la seguridad de la información y recursos que permitirán la reducción del impacto que pueda ocasionar la materialización de una amenaza.

ABSTRACT

Nowadays, the world is formed by great deal of information, therefore in a business context is not different. While the companies go up, they pile up essential information to manage them is the main asset of these companies. In addition, the companies look for preserving their continuity through time, so it is a necessity to protect the integrity of the information from the possible risks that are current. If those risks are not detected and monitored on time, they can cause big losses in a business. It is necessary to have an adequate "Gestión de Riesgos" in order to soothe the possible risks, therefore there are some adaptable methods according to the environment where the company develops.

In this work we have described the concepts related to methodology, standards and information security management that provide necessary guides that will help to reduce the number of vulnerabilities to which the assets are exposed. For an organization, it is vital to maintain the information backups. it has and the correct implementation of a contingency plan that can guarantee the business continuity.

For this reason, the need has been foreseen to develop a risk analysis to which the technological assets that make up the services included in the service level agreement that are presented in a qualitative manner following the MAGERIT methodology. Proceeding to identify the main assets, giving them a level of importance to them and determining the impact they can generate and the potential risks which they are exposed to.

Finally, this study identifies the level of risk which the assets are located in, the level of maturity of the current security is identified and, a management and implementation process is established too regarding the security of the information and resources that will allow the reduction of the impact that can cause the materialization of threat.

INTRODUCCIÓN

La información es el bien más valioso con el que cuentan las empresas, el ritmo de vida de la actualidad y el aumento en la competitividad a obligado a las organizaciones a depender cada vez más de la información, su disponibilidad, el proceso de la misma y sobretodo de las tecnologías de la información. Existen varios eventos o incidentes imprevistos que pueden comprometer dicha información de alguna manera, y poner en riesgo la continuidad del negocio que van desde lo trascendente a lo catastrófico.

Cuando se habla de mantener la seguridad sobre la tecnología generalmente se piensa en términos de seguridad lógica, física y protección de los sistemas, siendo estos únicamente referentes a medidas técnicas. Sin embargo se vuelve limitado, por lo que es necesario apoyarse con procedimientos y gestión de procesos adecuados que garanticen la continuidad del negocio. Hay que tomar en cuenta que no se puede tener un sistema completamente seguro, ya que conforme avanza la tecnología surgen nuevas amenazas, pero existen medidas de seguridad que permiten minimizar los daños y problemas que los intrusos pudiesen ocasionar. Por este hecho se han creado leyes, normas y estándares cuyo propósito es poder mitigar riesgos y prevenir ataques.

Para este efecto existen varias metodologías reconocidas a nivel mundial, una de ellas es Magerit, la cual se basa en una valoración de activos para la medición del riesgo, posee un enfoque cualitativo y cuantitativo que proporcionará una información más entendible para los directivos facilitando la toma de decisiones.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

"PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL"

1.2. Planteamiento del problema

Esta era tecnológica ha permitido que todo el mundo pueda estar conectado y no solamente eso, la transición a la web 3.0 también ha permitido tener las aplicaciones tradicionales disponibles a nivel web para los usuarios finales. Esto ha llevado a que se aumente el trabajo en equipo en tiempo real y la efectividad de las compañías reemplazando así muchas aplicaciones de escritorio tradicionales. Pero también ha traído consecuencias como el aumento de las amenazas y riesgos a la información que se maneja, aprovechándose de vulnerabilidades en especial la de grandes empresas lo cual en varios casos a implicado pérdidas importantes

En Ecuador se han dado varios casos de vulneración de seguridad, en el año 2015 el diario elcomercio.com publica "Vulneraban las seguridades del portal web del Servicio de Contratación Pública. La banda utilizaba un software para adulterar el sistema informático en beneficio de empresas, microempresas o personas, quienes pagaban altas sumas de dinero para resultar favorecidas en los concursos públicos y así obtener contratos.", otra parte del mismo artículo dice "Por casos como este, las alertas se encendieron en el país ya que se descubrió que hay vulnerabilidades en los sitios web oficiales y de empresas privadas. Esto se ratificó en enero de este año, cuando cibermafias atacaron 17 firmas privadas e instituciones públicas de Quito, Guayaquil y Cuenca... ¿Cómo ocurrió? Un programa fraudulento ingresó en los computadores y logró acceder y dañar archivos sensibles: documentos levantados en Word, Excel, Autocad. Una de las firmas perjudicadas perdió carpetas en las que se almacenaba datos de su departamento de contabilidad."[1]. Por lo citado anteriormente se puede observar que en el Ecuador varias empresas tanto públicas como privadas han sufrido ataques en

los últimos años, lo cual ha producido fraude en varios casos, en otros el robo de información y hasta la destrucción de la misma causando perjuicios y graves daños, creando así una alerta en el país acerca de los sistemas de informáticos y la información que se intercambia vía web.

Las empresas de Tungurahua no han sido ajenas a este tipo de ataques, un caso fue una empresa reconocida que en los últimos años ha sufrido ataques maliciosos perjudicando a dicha empresa; no solamente en lo que se refiere a información, varios perfiles de usuario fueron alterados y en algunos casos hasta eliminados causando así pequeñas interrupciones en la continuidad de la empresa. Plasticaucho Industrial al ser una empresa de varios años tiene sus procesos ya bien estructurados y cuenta con políticas tanto empresariales como por áreas, pero no cuenta con un plan de prevención de riesgos informáticos de software y de hardware que permitan disminuir los riesgos y amenazas a las que se encuentran expuestos.

Se debe evaluar las amenazas y riesgos físicos a los que se encuentran expuestos los equipos informáticos considerando la situación actual del país ya que en el 2016 se produjo un terremoto de gran magnitud, además la provincia de Tungurahua se encuentra rodeada de dos volcanes activos; que demuestra la falta de procedimientos de gestión de riesgo que permita tomar las medidas necesarias para minimizar el impacto a los procesos en caso de que una amenaza se materialice.

1.3. Delimitación

1.3.1. Delimitación de Contenido

El campo de la investigación está basado en la Tecnología Informática:
Área Académica: Administrativas Informáticas.
Líneas de Investigación: Normas y estándares.
Sublínea de Investigación: Seguridad de Unidades Informáticas.

1.3.2. Delimitación Espacial

La presente investigación se realizará en la empresa PLASTICAUCHO INDUSTRIAL.

1.3.3. Delimitación Temporal

El desarrollo de este proyecto se tomará 6 meses.

1.4. Justificación

Un plan de Riesgos y Contingencias para la empresa Plasticaucho Industrial es de gran relevancia pues permite precautelar la integridad y continuidad de los datos del negocio al momento de presentarse alguna circunstancia que ponga en riesgo la información que se maneja en la empresa y pueda afectar a la continuidad de la misma, por esta razón es de vital importancia que existan políticas y procedimientos que garanticen la seguridad de la información. La importancia de este plan de riesgos es salvaguardar la integridad de la información y de los activos que la almacenan y distribuyen en caso que algún siniestro ocurra y no se habla solamente de ataques a la información, también hay que precautelar los activos que corren riesgos físicos.

Por estos motivos en la empresa Plasticaucho Industrial se debe asegurar la continuidad del negocio cuidando el flujo de información y garantizando la disponibilidad, confidencialidad e integridad de la misma; por esta razón se hace necesaria la implementación de procedimientos de análisis de riesgos informáticos que permitan identificar las vulnerabilidades y amenazas para poder tomar las acciones tendientes a minimizar o eliminar el impacto de las mismas. Esta investigación es factible realizar debido a que se cuenta con la apertura de parte del Jefe de Tecnologías de la Información de Plasticaucho Industrial y el departamento que está a su cargo para desarrollar el estudio, la obtención de datos, el levantamiento de requerimientos, el análisis de vulnerabilidades y amenazas para poder desarrollar el plan de riesgos y contingencias para los servicios principales que brinda el departamento a la empresa.

Al desarrollar el plan de riesgos y contingencias de la información se beneficiara la empresa Plasticaucho Industrial en caso de que una amenaza se materialice sabrá que rumbo tomar para evitar que se interrumpan los procesos y la línea de negocio. Se ha tomado como referencia para una primera parte de este plan el Acuerdo de nivel de servicios firmado y aprobado por los gerentes de la empresa, pues al ser una organización grande llevaría mucho tiempo levantar los activos de todas las sucursales.

1.5. Objetivos

1.5.1. General

- Desarrollar un plan de Riesgos y Contingencias Informáticas basado en un acuerdo de nivel de servicio aplicada a la empresa Plasticaucho Industrial.

1.5.2. Específicos

- Definir los principales activos que forman parte los servicios del Acuerdo de nivel de servicio.
- Determinar la metodología para el levantamiento de riesgos y amenazas.
- Realizar un análisis de riesgos sobre los activos.
- Elaborar el plan de Riesgos y Contingencias Informáticas aplicando la metodología seleccionada.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

La inseguridad de la información se ha convertido en un punto que merece atención por las múltiples formas de ataque que día a día van desarrollando, para la salvaguarda de datos muchos son los trabajos que tratan de abordar la seguridad de la información, se cuenta con diferentes trabajos de investigación que se mencionan a continuación.

Cristina Elizabeth Padilla Pacha en su tesis denominada "Análisis y Gestión de Riesgos Informáticos para la protección de sistemas de información en el área de tecnologías informáticas del Gobierno Provincial de Tungurahua" recomienda la metodología de gestión de riesgo MAGERIT como la más adecuada para el control de la información y de los activos físicos de la organización[2].

En su investigación Gabriela Catherine Torres Andagana y Diego Fernando Llanca Salcan titulado "Estudio e implementación de una metodología de prevención de intrusos para redes LAN, Faculta de Informática y Electrónica de la Escuela Superior Politécnica del Chimborazo" concluyen que proporcionar lineamientos de seguridad con una amplia participación del personal y fundamenta las seguridades en el liderazgo y las buenas prácticas administrativas donde sobresale el liderazgo como característica relevante[3].

Md. Forhad Rabbi y Khan Olid Bin Mannan en su paper publicado en el 2016 bajo el tema "A Short Review for Selecting the Best Tools and Techniques to Perform Software Risk Management" determinan en su investigación que ninguna herramienta o técnica aislada es perfecta para medir riesgos en el desarrollo de software debido a sus diferentes características y procedimientos de trabajo[4].

En su tesis "Centro de gestión de riesgos para monitoreo de redes, en la Facultad de Ingeniería, Ciencias Físicas y Matemáticas de la Escuela Politécnica Nacional" Alexandra Espinosa Criollo, Freddy Roldan González y Dennis Collaguazo concluyen que la utilización de la metodología MAGERIT para el desarrollo de módulos para monitorear servidores de aplicaciones, de base de datos y dispositivos de interconexión que permiten detectar caída de servicios, ataques de intrusos para la toma de decisiones del administrador[5].

Rex Kelly Rainer, Charles Snyder y Houston Carr en su artículo "Risk Analysis for Information Technology" dice que la literatura de análisis de riesgo sugiere utilizar una metodología única, no una combinación de metodologías[6].

2.2. Fundamentación teórica

2.2.1. Lineamiento

Es una orientación de carácter general, corresponde a una directriz o disposición [7].

2.2.2. Activo Tecnológico

Equipo, maquinaria, herramienta o software necesario para realizar las actividades productivas específicas de una organización [8].

2.2.3. Amenaza

Es todo lo que puede causar un riesgo para la organización en sus diferentes áreas o dimensiones aunque cada organización es libre de determinar la calificación de las mismas y teniendo en cuenta su valoración se puede incurrir en un riesgo para la misma [9].
Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de modo accidental, se presente con una severidad su ciente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales. La caracterización de la amenaza debe incluir su ubicación, clasificación, magnitud o intensidad, y se evalúa en función de probabilidad de ocurrencia espacial y temporal [10].

2.2.4. Gestión de la continuidad de servicios de TI

Como la tecnología es un componente principal de la mayoría de los procesos de negocio, la alta disponibilidad del sistema de información es crítica con respecto a la supervivencia del conjunto de la actividad. Esto se consigue mediante la introducción de medidas de tratamiento del riesgo y opciones de recuperación de los servicios. El mantenimiento permanente de la capacidad de recuperación es esencial para mantener su eficiencia [11].

2.2.5. Gestión de la seguridad de la información

El objetivo consiste en alinear la seguridad de la información con la actividad de negocio y de asegurar que esa seguridad se gestiona eficazmente en todos los departamentos y sus actividades de gestión [11].

2.2.6. Gestión de riesgos

La Gestión de Riesgos consiste en un proceso cíclico que se inicia a partir de un conjunto de información recogida de diversas fuentes (requisitos, personas, procesos de desarrollo, presupuestos, expectativas. . .). Toda esta información proporciona una lista de riesgos a tener en cuenta. El proceso de Gestión de Riesgos los analiza, prioriza y plantea planes de respuesta, dando como resultado el conjunto de riesgos priorizados, los planes de respuesta a dichos riesgos y un conjunto de indicadores que se utilizarán para medir el éxito del proceso, y en su caso, mejorarlo [12].

2.2.7. Sistema de Gestión de seguridad de la información

El SGSI, tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados [9].

2.2.8. Riesgo

Riesgo específico, como el grado de pérdidas esperadas debido a la ocurrencia de un evento particular y como una función de la amenaza y la vulnerabilidad. Riesgo total, como el número de pérdidas humanas, heridos, daños a las propiedades y efectos sobre la actividad económica debido a la ocurrencia de un evento desastroso, es decir el producto del riesgo específico y los elementos bajo riesgo [13].

2.2.9. Riesgo de TI

Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas

adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto los riesgos se pueden clasificar en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura [9].

2.2.10. Vulnerabilidad

Son las posibilidades que se dan en el mismo ambiente, en el cual las características propician y se vuelven susceptibles a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reacción ante la presencia de un factor que pueda posibilitar una amenaza o un ataque. Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos informáticos, los datos o la información ante la posibilidad de la presencia de un ataque deliberado o no, por parte del personal interno o externo a la organización [9].

2.2.11. Análisis de la vulnerabilidad

Un análisis de vulnerabilidad, es un proceso mediante el cual se determina el nivel de exposición y la predisposición a la pérdida de un elemento o grupo de elementos ante una amenaza específica, contribuyendo al conocimiento del riesgo a través de interacciones de dichos elementos con el ambiente peligroso [13].

2.3. Propuesta de Solución

Mediante la elaboración de un plan de riesgo y contingencias para la información en la empresa Plasticaucho Industrial se podrá precautelar la información y los activos de principales para así en caso de algún siniestro se podrá saber cómo actuar y así asegurar el nivel de servicio.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la Investigación

3.1.1. Modalidad Bibliográfica o Documental

Esta modalidad será considerada ya que se apoyará en diferentes fuentes de información que pueden ser libros, artículos, tesis de varias universidades tanto nacionales como extranjeras que nos ayudarán para mejorar el enfoque.

3.1.2. Modalidad de Campo

Se empleará la investigación de campo, pues el investigador acudirá a la fuente para evaluar procesos también realizará un estudio técnico y herramientas que se emplean para cumplir los objetivos propuestos.

3.1.3. Modalidad Aplicada

Se utiliza la investigación aplicada ya que se procederá a seguir los pasos necesarios para poder aplicar correctamente la metodología que se escogerá para este proyecto.

3.2. Recolección de información

Para la recolección de información se acudirá a la empresa al levantamiento de los activos mediante inventario, también se acudirá a revisar la metodología que más se ajusta mediante investigación de levantamientos previos de riesgos en otras empresas. Se realizará el análisis siguiendo la metodología propuesta.

3.3. Procesamiento y análisis de datos

Para el procesamiento y análisis de la información se realizará lo siguiente:

- Listado de activos.
- Revisión de la información recogida.

- Agrupación de activos por servicios.
- Lectura de artículos relacionados con la investigación presentada.
- Análisis de la metodología.

3.4. Desarrollo del Proyecto

- Estudio del acuerdo de nivel de servicio de TI.
- Recolección de activos que influyen al acuerdo de nivel de servicio.
- Clasificación de activos por servicio.
- Determinación de metodología para el levantamiento de riesgos.
- Revisión de la metodología y anexos de la misma.
- Levantamiento y valoración de riesgos de los activos.
- Plan para elaboración de salvaguardas.
- Realización del documento a presentar.

CAPÍTULO 4

Desarrollo de la propuesta

4.1. Datos Informativos

4.1.1. Titulo

"PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL"

4.1.2. Institución ejecutora

Universidad Técnica de Ambato
Facultad de Ingeniería En Sistemas, Electrónica e Industrial
David Cruz (Investigador)

4.1.3. Beneficiarios

Plasticaucho Industrial

4.1.4. Ubicación

Ecuador

Catiglata: Panamericana Norte Km 2 1/2
Parque Industrial: Panamericana Norte Km 10 - Parque Industrial 4ta. Etapa Ambato

Colombia

Carrera 35 # 1355, Acopi - Yumbo
Cali

Perú

Los Eucaliptos s/n Urb. Huertos de Santa Genoveva
Lurin

4.1.5. Tiempo estimado para la ejecución

El tiempo estimado para la ejecución es de seis meses, desde el análisis de situación actual, hasta la búsqueda de salvaguardas adecuadas que nos permitan el cumplimiento de nuestro objetivo.

4.1.6. Equipo técnico responsable

Ing. David Guevara, Mg. (Tutor)
David Cruz Ojeda (Investigador)
Ing. William Velasteguí, Mg. (Jefe de TI en Plasticaucho Industrial)
Alexander Rojas. (Analista de Seguridades en Plasticaucho Industrial)

4.2. Antecedentes de la Propuesta

4.2.1. Situación actual de la empresa

Se establecen puntos claves relacionados con la seguridad informática:

4.2.1.1. Introducción

La empresa Plasticaucho Industrial es una sociedad anónima, constituida bajo las leyes ecuatorianas, dedicada a la elaboración y comercialización de calzado de cuero, lona y plástico, sus actividades se desarrollan con su sede principal en Ambato Ecuador y con filiales en Colombia y Perú.

Plasticaucho Industrial S.A. realiza la comercialización de su producto en Ecuador y se extiende bajo importaciones a Colombia y Perú de productos específicos que son producidos únicamente en el país. Es una empresa en la que prima la innovación de sus proceso y a su vez pone énfasis en la constante mejora tecnológica.

4.2.1.2. Misión

Lideramos el sector calzado en el Ecuador con procesos ágiles, eficiente e innovadoras.

4.2.1.3. Visión

Todo ecuatoriano usará un par de zapatos de una de las marcas comercializadas por la empresa.

4.2.1.4. Motivación

Debido a que la empresa cuenta con tres filiales y con el afán de preservar la información y preservar la continuidad del negocio, posee una infraestructura tecnológica centralizada en Ecuador, siendo la administración principal, desde donde se toman las decisiones que afectarán a la empresa en los 3 países que conforman el grupo empresarial, incrementando el riesgo que supone el contar con un número mayor de recursos tecnológicos. Razón por la cual Plasticaucho Ecuador cuenta con una estructura departamental sólida y con procesos especializados.

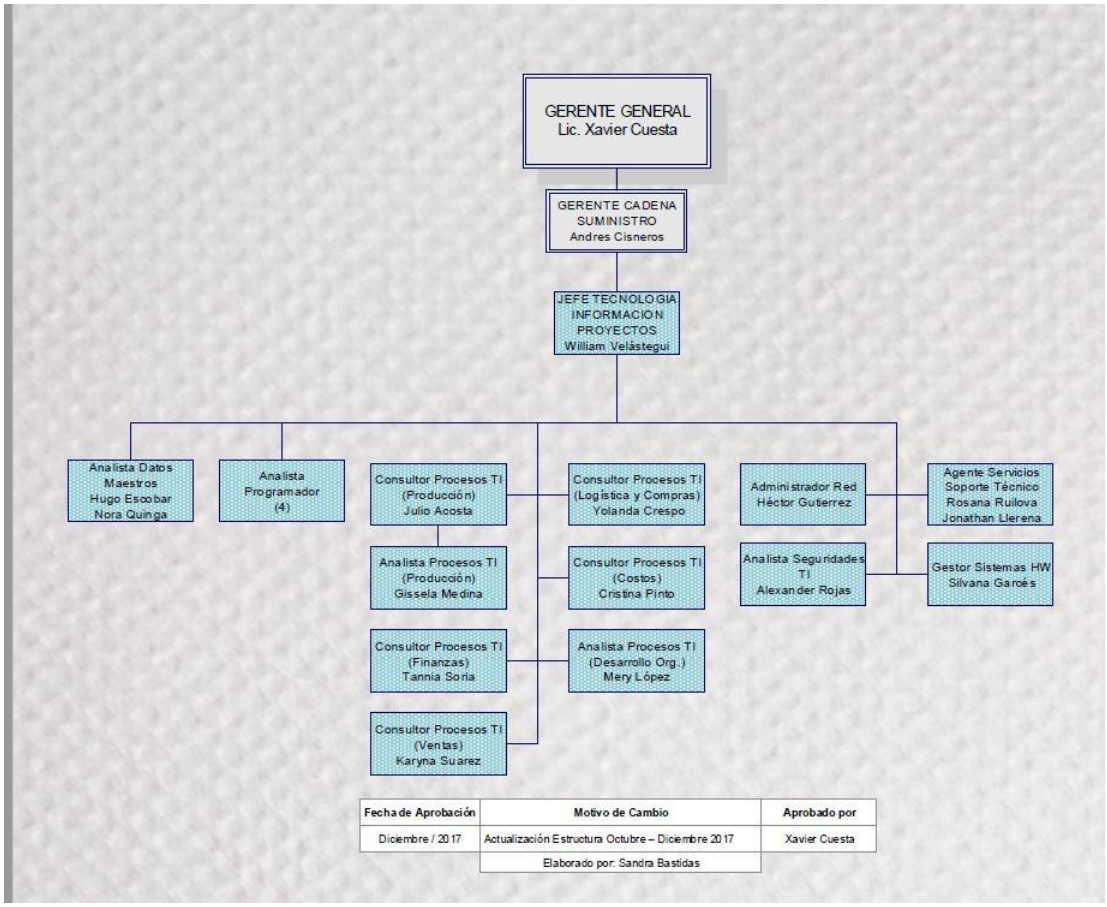


Figura 1: Organigrama del Departamento de TI

4.2.2. Análisis de la Entrevista

Para conocer la situación actual de la empresa Plasticaucho Industrial en temas de seguridad, se realizó una entrevista al responsable del área Alexander Rojas que se encuentra en el **Anexo C**, quién supo manifestar los siguientes datos relevantes para el desarrollo del proyecto:

Pregunta 1. ¿Qué problemas de seguridad informática ha tenido la empresa en los últimos años Plasticaucho Industrial S.A.?
ANÁLISIS: La empresa vio comprometida su información debido a varias falencias en la seguridad, entre las afectaciones estuvieron el borrado de información importante.
INTERPRETACIÓN: Esto nos indica, que pudiese haber un ataque informático pequeño o de gran magnitud debido a que las seguridades en la empresa no están reforzadas.

Pregunta 2. De lo mencionado ¿Cuál considera que fue el ataque más perjudicial para la compañía?
ANÁLISIS: Existe información que contribuyen a los procesos de control de calidad de la empresa, en uno de los ataques presentados, la información correspondiente a ese proceso fue borrada.
INTERPRETACIÓN: En la empresa existe información respaldada de diferentes maneras, sin embargo, no cuenta con una adecuada seguridad de manera que su vulneración es de fácil acceso. Por lo que es primordial buscar un mecanismo de protección de la información.

Pregunta 3. ¿De qué manera se gestiona actualmente la seguridad informática en la empresa?
ANÁLISIS: En la empresa se instauraron políticas y recomendaciones para que los usuarios puedan cuidar así la información que cada uno mantiene.
INTERPRETACIÓN: Es necesario verificar que otras acciones o procesos son necesarios para precautelar la información además de los ya instituidos y qué pasaría con la información de los usuarios que no son considerados clave y por ende no es respaldada correctamente su información.

Pregunta 4. En el caso de suscitarse un desastre natural, cuenta con un registro de los principales activos que le permita retomar las actividades normales.
ANÁLISIS: La empresa no cuenta con un registro de activos sino únicamente lo tienen como conocimiento general.
INTERPRETACIÓN: Para una eficiente gestión que no permita dejar a ningún activo sin resguardo de seguridad, es necesario contar con un levantamiento de activos de la empresa que permita evaluar cada uno de ellos y poder tomar

medidas en función a su accionar o rol en los procesos de la empresa. Con esta medida se asegura que no quede ninguno al azar.

Pregunta 5. Actualmente, ¿Posee un proceso de respaldo de información?

ANÁLISIS: Se ha realizado la compra de herramientas para el respaldo de información para las personas con documentos importantes para el negocio.

INTERPRETACIÓN: Esto nos indica que aunque se tiene un proceso de respaldo es actualmente solo para ciertas personas, mientras que para los demás colaboradores, ante algún suceso imprevisto pudiesen perder su información ya que no se contempla a toda la empresa dentro de este proceso .

Pregunta 6. En caso de que se sufra un ataque informático, se cuenta con un procedimiento para disminuir el impacto?

ANÁLISIS: Actualmente la empresa espera que suceda algún ataque informático para tomar medidas tanto de corrección como de prevención conforme se vayan presentando, sin tomar en cuenta que en ese proceso se puede ver afectada considerablemente la información.

INTERPRETACIÓN: La empresa ha sabido responder ante las circunstancias que se le han presentado sin embargo no es suficiente ya que en ese proceso se pueden ver afectados activos o puede existir pérdida de información de manera que es importante detectar y planificar de qué manera se va a reaccionar antes de que ocurra el problema, además de tomar medidas para salvaguardar la integridad de la información y aseguren la correcta continuidad del negocio.

En función de los aspectos analizados en la entrevista, para la empresa Plasticaucho Industrial contar con un plan de riesgos y contingencias es fundamental debido a que su implementación y correcta ejecución del mismo ayudará a mitigar riesgos a los que se expone la empresa, aunque el riesgo no siempre tiene que suponer una amenaza, también puede generar oportunidades ya que la empresa debe ser capaz de identificar y aprovechar así mejorará la gestión de la empresa precautelando la continuidad del negocio.

4.2.3. Antecedentes

John Jairo Perafán Ruiz, dice en su trabajo que "De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de riesgos; muy seguramente en un futuro cercano podría ser

víctima de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros."[14], bajo esta premisa se puede mencionar que es muy importante saber que sistemas posee la empresa y a que riesgos están expuestos.

Continuando con la idea, Karina del Rocío Gaona Vásquez dice en su trabajo que "MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) mide la Vulnerabilidad por la frecuencia histórica cuantitativa de la materialización de la Amenaza sobre el Activo, cuando es factible (fiabilidad de un componente hardware, número de fallos de software); o bien por la potencialidad cualitativa de dicha materialización, cuya primera aproximación lleva a emplear una escala vista en las Amenazas potenciales (consideradas ahora reales, o sea agresiones)." [15], con esto se evidencia que la metodología Magerit cumple con el análisis de los riesgos que se busca, para poder mitigarlos en la mayor forma.

4.3. Justificación

Con la constante innovación de la tecnología y la inclusión de nuevas aplicaciones o herramientas en las actividades diarias de las personas, las empresas se han visto inmersas en la necesidad de hacer uso de estas herramientas, de manera que se requiere que sus colaboradores accedan a su información empresarial, desde cualquier parte y a cualquier momento, generando así nuevas brechas y vulnerabilidades que han permitido la gran propagación de ciberataques a las organizaciones, siendo los cifrados de archivos con información importante del negocio los que han causado un mayor impacto, llegando en algunos casos a la extorsión por medio de la solicitud de grandes sumas de dinero a cambio de las llaves para poder liberar dicha información, sin otorgar una garantía de que en un futuro no se vuelva a generar el mismo inconveniente o exista un nuevo contagio, ya sea con el mismo programa u otros.

Ecuador, no ha sido la excepción, debido a que también ha sufrido ataques de este tipo y así lo comunica el Diario Expreso, que publicó en su portal un artículo bajo el nombre "Ecuador y casi 100 países sufren ciberataque extorsivo"[16], en el cual menciona que "Los ataques se registraron en Guayaquil, Quito y Cuenca y afectando información sensible de tres empresas privadas"[16], lo que evidencia que las empresas son un blanco para estas organizaciones que se dedican a operar bajo esta modalidad, razón por la cual se vuelve un requisito indispensable para las empresas el estar preparadas para cualquier amenaza que ponga en riesgo la

continuidad del negocio y su bien más importante que es la información.

En base a estos motivos y en función al crecimiento que ha tenido Plasticaucho Industrial S.A., se plantea la necesidad de protegerse de posibles amenazas que afecten la estabilidad de la organización y no permitan la continuidad del negocio, de manera que la propuesta que se plantea, posee el enfoque para ayudar considerablemente a la empresa en caso de que sufra alguna violación a su seguridad de la información, mediante la aplicación racional de medidas de seguridad en base al conocimiento previo de las diferentes amenazas a las que están expuestos; aplicando una metodología de análisis y riesgos de los sistemas de información, identificándolos y analizando el comportamiento que pudiesen y así poder establecer medidas apropiadas que permitan controlar o mitigar la incidencia con la que puedan presentarse dichos riesgos, volviendo necesaria la elaboración e implementación del Plan de Riesgos y Contingencias Informáticas.

4.4. Objetivos

4.4.1. Objetivo general

Elaborar un plan de Riesgos y Contingencias de los Sistemas de Información de la empresa Plasticaucho Industrial.

4.4.2. Objetivos específicos

- Levantar inventario de los activos principales de la empresa.
- Clasificar activos principales por servicios.
- Valorar el riesgo de cada activo.

4.5. Análisis de Factibilidad

4.5.1. Política

A nivel de política pública nacional, no existe una ley que estipule que las empresas deban poseer de un Plan de Riesgos y Contingencias Informáticas. Sin embargo en base al Plan Estratégico y Políticas de la empresa Plasticaucho Industrial S.A. se contempla como uno de sus objetivos, precautelar por la continuidad del negocio y su sustentabilidad en el tiempo, de manera que las autoridades permiten la elaboración de este trabajo.

4.5.2. Tecnología

La tecnología, es una de las bases de ejecución de este proyecto, ya que su uso y análisis permite alcanzar los objetivos planteados y el resguardo de la misma a nivel empresarial y como parte de la gestión de la organización.

4.5.3. Organizacional

La empresa Plasticaucho Industrial, contará con la seguridad necesaria y el procedimiento adecuado para responder ante las diferentes amenazas y riesgos físicos que puedan suscitarse, precautelando así la continuidad del negocio.

4.5.4. Equidad de Género

Se involucra a todos los géneros, ya que su utilidad no distingue ni hace diferencia entre hombres y mujeres, encontrándose al alcance de todos.

4.5.5. Ambiental

El desarrollo de este proyecto no afectará al medio ambiente, sino más bien minimizará su impacto en la organización, sin alterarlo.

4.5.6. Económico – Financiera

Plasticaucho Industrial S.A. cuenta con el presupuesto, tanto en recursos económicos como el capital humano para la puesta en marcha del Plan, contando el departamento de Tecnologías de la Información con un área especializada en Seguridades Informáticas, a más de la asignación de una cuenta para solventar la inversión en temas de tecnología.

4.5.7. Socio – Cultural

El trabajo realizado, tiene un impacto positivo en los colaboradores de la institución beneficiaria, generando una cultura de prevención y conciencia en la administración de las herramientas tecnológicas con las que se desempeñan sus funciones.

4.5.8. Legal

Para el desarrollo de este trabajo, se toman en cuenta las leyes vigentes y su cumplimiento, evitando así que el mismo afronte algún problema legal.

Después de tomar en cuenta cada uno los aspectos analizados y verificar que no se tendrá un efecto negativo en otros sectores que quizás no sean relacionados al tema, sino más bien contribuyan a su desarrollo, se puede determinar la factibilidad del mismo.

4.6. Fundamentación Teórica

4.6.1. Metodologías para el Análisis de Riesgos

Para la gestión de un Plan de Riesgos y Contingencias Informáticas existen diferentes metodologías que facilitan su ejecución, por lo que se realiza un análisis y comparación de las mismas, para de esta manera poder determinar la que sea óptima y aplicable a la realidad de Plasticaucho Industrial S.A.
A continuación se encuentra una breve descripción de las metodologías que van a ser comparadas:

4.6.1.1. OCTAVE

Esta metodología posee dos versiones, una para grandes empresas y otra para empresas de menos de 100 colaboradores. Se centra en la recolección y análisis de información para poder diseñar una estrategia de protección y planes que permitan mitigar el riesgo operacional de seguridad de la organización.

4.6.1.2. MAGERIT

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

4.6.1.3. ISO/IEC 27005

Este documento, habla de la gestión de los riesgos de la seguridad de la información de manera genérica, cuenta con un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.

4.6.1.4. COBIT

COBIT (Control Objectives for Information and related Technology), define unos objetivos de control asociados con la información y la tecnología relacionada. COBIT considera fundamental el tratamiento de los riesgos asociados a los activos

de información electrónica, alineada con su misión, que consiste en investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes, auditores y usuarios.

METODOLOGÍA	CARACTERÍSTICAS	ÁMBITO DE APLICACIÓN
OCTAVE	1.- No es una metodología únicamente técnica 2.- Presenta principios básicos y mejores prácticas internacionales 3.- Relaciona amenazas y vulnerabilidades	Aplicable para seguridad de sistemas de información de las PYMES
MAGERIT	1.- Orientada a los Sistemas de Información 2.- Tiene como objetivos: - Crear conciencia en el usuario de la existencia de riesgos y de la necesidad de prevenirlos - Analizar bajo un método sistemático tales riesgos - Ayudar a descubrir y planificar medidas oportunas para mantener bajo control los riesgos - Que la empresa pueda estar lista para procesos de evaluación, auditoría, certificación o acreditación, según el caso	Análisis y gestión de riesgos de los sistemas de información: Gobierno, Organismos, Compañías Grandes, PYME, Compañías Comerciales y no Comerciales
ISO/IEC 27005	1.- Estudio de vulnerabilidad 2.- Proceso de evaluación de amenazas y vulnerabilidades 3.- Identificar los activos y las facilidades 4.- Análisis de los activos del sistema 5.- Herramienta de gestión	Su enfoque es a procesos.
COBIT	1.- Planificación y Organización 2.- Entrega y Soporte 3.- Mantener y Evaluar	Empresas medianas y grandes

Figura 2: Características de Metodologías

Como se describe, cada una de las metodologías posee sus propias características y en base a estás pueden ser adaptadas a diferentes realidades empresariales, en función al giro del negocio y sus necesidades. A continuación se muestra un detalle comparativo, mediante el cual podremos determinar la metodología apropiada

para la elaboración del Plan de Riesgos y Contingencias Informáticas:
Después de analizar la relación entre diferentes metodologías, podemos determinar varias conclusiones, primero no se opta por utilizar el método ISO/IEC 27005, debido a que solo posee un enfoque cualitativo, lo que puede llevar a una interpretación dada por el analista responsable del proceso además que se enfoca únicamente en la gestión de riesgo y para su ejecución necesita de varias herramientas pagadas por lo que los costos para su implementación se podrían elevar. Por su parte, tenemos el método de Magerit, el mismo que posee un enfoque cualitativo y cuantitativo que permitirá una información más entendible para los directivos, realizando una valoración de activos para la medición del riesgo, lo que facilitará la toma de decisiones y lo más importante se ajusta a los objetivos del Plan Estratégico que posee la empresa Plasticaucho Industrial S.A. por lo que su factibilidad en la misma tendrá una mayor aceptación.

Para la gestión de la tecnología en la empresa Plasticacucho Industrial S.A. se determinaron inicialmente objetivos dentro de su Plan Estratégico [17], empoderando y fomentando la integración y trabajo en equipo, mencionando: "La empresa tendrá claramente definidos la totalidad de sus procesos de gestión los cuales abarcan toda la operación de la misma. Los dueños de los procesos son los encargados de fomentar por medio del trabajo en equipo la evolución continua de los procesos." [17]. De manera que su interés se centra no solo en la ejecución del proceso sino en el compromiso colectivo de adoptarle e implementarlo como parte de la gestión de la compañía. Y la metodología de Magerit V.03 aporta a este concepto, ya que tiene como objetivos los en listados a continuación, según el libro I – Método[18]:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

4.6.2. Metodología Magerit V.3

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que las entidades que la utilicen tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[18].
Su marco de trabajo para la gestión de riesgos se basa en **Figura 2.**

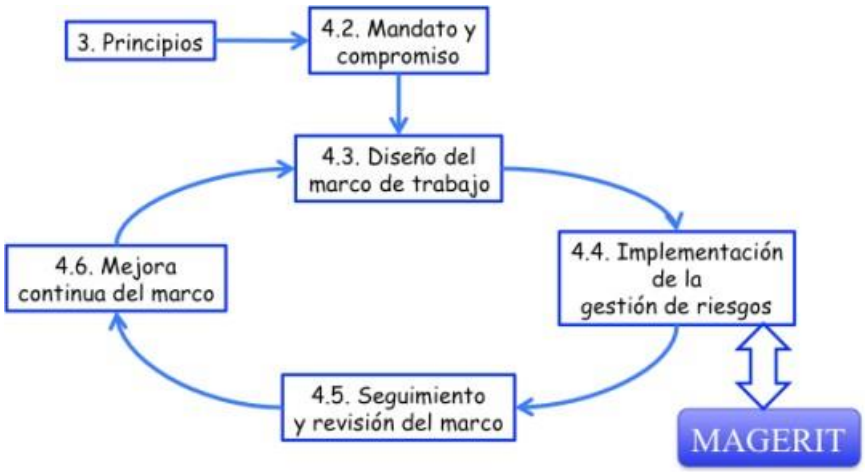


Figura 3: Marco de trabajo para la gestión de riesgos

Todas las empresas buscan objetivar el análisis de riesgos para saber cuán seguros o inseguros son los sistemas y no llamarse a engaño. El gran reto de todas las aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista [18].

El objetivo a proteger es la misión de la empresa, teniendo en cuenta las diferentes dimensiones de la seguridad:

- **Disponibilidad**: Disposición de los servicios a ser usados cuando sea necesario, hay que tomar en cuenta que la carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad.
- **Integridad:** La integridad afecta directamente al correcto desempeño de las funciones de la empresa, contra la integridad, la información puede aparecer manipulada, corrupta o incompleta.

- **Confidencialidad**: Trata de que la información llegue solamente a las personas autorizadas, contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo verse afectada la confianza de los demás en la empresa.
- **Autenticidad**: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos, contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. También se toma en cuenta la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.
- **Trazabilidad**: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes, además se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso.

4.7. Plan de Riesgos y Contingencias de Plasticaucho Industrial

4.7.1. Objetivos

- Analizar la infraestructura actual de la empresa.
- Conocer el riesgo que pueden ocasionar la materialización de amenazas.
- Aplicar salvaguardas para su mitigación.
- Proponer mejoras para su gestión.

4.7.2. Alcance

Desde el levantamiento del inventario de los activos informáticos de los servicios tecnológicos catalogados como críticos, su valoración y priorización hasta la identificación de amenazas y propuesta de acciones preventivas y correctivas que minimicen el riesgo y la probabilidad ocurrencia.

4.7.3. Análisis y Gestión Riesgos

El uso de Tecnologías de la Información y Comunicaciones han ayudado a la empresa a automatizar y llevar un mejor control de sus actividades permitiendo alcanzar sus objetivos, sin embargo el depender de forma creciente de los sistemas de información conlleva riesgos que deben manejarse prudentemente de modo que permitan garantizar la confianza depositada por la compañía.

El presente documento está enfocado en la gestión de los riesgos tecnológicos asociados a los servicios especializados catalogados como críticos según el documento de Acuerdo de Nivel de Servicio firmado con la Gerencia General. Los servicios que forman parte del alcance de este documento son:

1. Acceso a la Red Corporativa.
2. Acceso al aplicativo SAP.
3. Servicios de Internet.
4. Correo Electrónico.
5. Mitrol.
6. Servicio de Impresión.
7. Movilidad.
8. BW.
9. Sistema de Nómina.
10. Servicios de Respaldos.

4.7.4. Inventario de activos tecnológicos

Se tomó en cuenta para este listado el equipo, herramientas y software que intervienen en el acuerdo a los servicios principales de la empresa, para asegurar su disponibilidad, integridad, confidencialidad y autenticidad.

Item	Descripción	Dirección IP
1.1	Switch de Acceso	10.15.15.242
1.2	Switch de Core	10.11.1.200
1.3	Servidor Active Directory	10.11.0.40
1.4	Router Level 3	10.11.0.254
1.5	VPN Azure	10.10.60.0/28
1.6	Active Directory Azure	10.10.60.4
1.7	Switch de Core	10.12.0.201
1.8	Router Level 3	10.12.0.251
1.9	Servidor Active Directory WR	10.11.0.40
1.10	Servidor Active Directory RO	10.12.0.50
1.11	Active Directory Azure	10.10.60.4
1.12	Router Level 3	10.14.0.253
1.13	Servidor Active Directory WR	10.11.0.40
1.14	Servidor Active Directory RO	10.14.0.10
1.15	Active Directory Azure	10.10.60.4

Tabla 1: Activos principales para acceso a la Red Corporativa.

Item	Descripción	Dirección IP
2.1	Switch de Acceso	10.15.15.242
2.2	Switch de Core	10.11.1.200
2.3	Servidor Active Directory	10.11.0.40
2.4	Router Level 3	10.11.0.254
2.5	Firewall Level 3	10.111.121.66
2.6	Servidor Active Directory	10.14.0.10
2.7	Router Level 3	10.14.0.253
2.8	Firewall Level 3	10.111.121.66
2.9	Switch de acceso	10.12.0.201
2.10	Switch Core	10.12.0.254
2.11	Router Level 3	10.12.0.251
2.12	Servidor Active Directory	10.12.0.51
2.13	Firewall TMG	10.12.0.1
2.14	Dirección de Internet	8.8.8.8

Tabla 2: Activos principales para acceso al aplicativo SAP.

Item	Descripción	Dirección IP
3.1	Switch de acceso	10.15.15.242
3.2	Switch Core	10.11.1.200
3.3	Router Level 3	10.11.0.254
3.4	Servidor AD	10.11.0.40
3.5	Firewall	10.111.121.66
3.6	Active Directory Azure	10.10.60.4
3.7	ADFS	10.10.60.5
3.8	ADFS	10.10.60.6
3.9	ADFS Proxy	192.168.2.5
3.10	ADFS Proxy	192.168.2.4
3.11	Dirsync	10.10.60.7
3.12	Smtp	office365.com
3.13	Switch de acceso	10.12.0.201
3.14	Switch Core	10.12.0.254
3.15	Router Level 3	10.12.0.251
3.16	Servidor AD	10.12.0.51
3.17	Active Directory Azure	10.10.60.4
3.18	ADFS	10.10.60.5
3.19	ADFS	10.10.60.6
3.20	ADFS Proxy	192.168.2.5
3.21	ADFS Proxy	192.168.2.4
3.22	Dirsync	10.10.60.7
3.23	Smtp	office365.com

Tabla 3: Activos principales para acceso a los servicios de Internet.

Item	Descripción	Dirección IP
4.1	Switch Core PIA	10.11.1.200
4.2	Router Level 3 PIA	10.11.0.254
4.3	Switch Core Catiglata	10.10.1.200
4.4	Router Telconet Catiglata	10.10.1.240
4.5	Router Telconet PIA	10.11.0.240
4.6	Firewall Level 3 Bogota XV	10.9.1.2
4.7	Servidor SAP DB	10.125.15.6
4.8	Servidor SAP	10.125.15.4
4.9	Switch Core Yumbo	10.12.0.201
4.10	Router Yumbo	10.12.0.254
4.11	Router Level 3	10.12.0.251
4.12	Firewall Level 3 Bogota XV	10.9.1.2
4.13	Servidor SAP DB	10.125.15.6
4.14	Servidor SAP	10.125.15.7
4.15	Switch Principal	S/N
4.16	Router Level Lima	10.14.0.254
4.17	Firewall Level 3 Bogota XV	10.9.1.2
4.18	Servidor SAP DB	10.125.15.6
4.19	Servidor SAP	10.125.15.7

Tabla 4: Activos principales para acceso a Correo Electrónico.

Item	Descripción	Dirección IP
5.1	Switch Core Catiglata	10.10.1.200
5.2	Servidor Mitrol Aplicación	10.10.0.12
5.3	Servidor Mitrol Comunicaciones	10.10.0.13
5.4	Central de Comunicaciones SIEMENS	10.10.8.6
5.5	Switch Core Cali	10.12.0.201
5.6	Servidor Mitrol Aplicación	192.168.150.8
5.7	Servidor Mitrol Base de Datos	192.168.150.3
5.8	Router de comunicaciones	192.168.150.2

Tabla 5: Activos principales para acceso a Mitrol.

Item	Descripción	Dirección IP
6.1	Switch Core PIA	10.11.1.200
6.2	Router Level 3 PIA	10.11.0.254
6.3	Switch Core Catiglata	10.10.1.200
6.4	Router Telconet Catiglata	10.10.1.240
6.5	Router Telconet PIA	10.11.0.240
6.6	Firewall Level 3 Bogota XV	10.9.1.2
6.7	Servidor BW	10.125.15.7
6.8	Servidor SAP DB	10.125.15.6
6.9	Switch Core Yumbo	10.12.0.201
6.10	Router Yumbo	10.12.0.254
6.11	Router Level 3	10.12.0.251
6.12	Firewall Level 3 Bogota XV	10.9.1.2
6.13	Servidor BW	10.125.15.7
6.14	Servidor SAP DB	10.125.15.6
6.15	Switch principal	n/a
6.16	Router Level Lima	10.14.0.253
6.17	Firewall Level 3 Bogota XV	10.9.1.2
6.18	Servidor BW	10.125.15.7
6.19	Servidor SAP DB	10.125.15.6

Tabla 6: Activos principales para acceso a Servicio de Impresión.

Item	Descripción	Dirección IP
7.1	Switch Core PIA	10.11.1.200
7.2	Router Level 3 PIA	10.11.0.254
7.3	Switch Core Catiglata	10.10.1.200
7.4	Router Telconet Catiglata	10.10.1.240
7.5	Router Telconet PIA	10.11.0.240
7.6	Servidor Impresiones PIA	10.11.0.17
7.7	Servidor Impresiones Catiglata	10.10.0.17
7.8	Firewall Level 3 Bogota XV	10.9.1.2
7.9	Servidor SAP	10.125.15.5
7.10	Servidor SAP DB	10.125.15.6
7.11	Switch Core Yumbo	10.12.0.201
7.12	Router Yumbo	10.12.0.254
7.13	Router Level 3	10.12.0.251
7.14	Servidor de Impresión	10.12.0.15
7.15	Firewall Level 3 Bogota XV	10.9.1.2
7.16	Servidor BW	10.125.15.7
7.17	Servidor SAP DB	10.125.15.6

Tabla 7: Activos principales para acceso a Movilidad.

Item	Descripción	Dirección IP
8.1	Switch Core PIA	10.11.1.200
8.2	Router Level 3 PIA	10.11.0.254
8.3	Switch Core Catiglata	10.10.1.200
8.4	Router Telconet Catiglata	10.10.1.240
8.5	Router Telconet PIA	10.11.0.240
8.6	Servidor de Movilidad	10.125.15.12
8.7	Servidor SAP	10.125.15.6
8.8	Firewall Level 3 Bogota XV	10.9.1.2
8.9	Host mob.plasticaucho.com	64.76.89.173
8.10	Switch Core Yumbo	10.12.0.201
8.11	Router Yumbo	10.12.0.254
8.12	Router Level 3	10.12.0.251
8.13	Firewall Level 3 Bogota XV	10.9.1.2
8.14	Servidor de Movilidad	10.125.15.12
8.15	Servidor SAP	10.125.15.6
8.16	Host mob.plasticaucho.com	64.76.89.173

Tabla 8: Activos principales para acceso a BW.

Item	Descripción	Dirección IP
9.1	Switch Servidores	10.15.15.242
9.2	Switch Core PIA	10.11.1.200
9.3	Synology PIA	10.10.0.39
9.4	Router Telconet PIA	10.11.1.240
9.5	Telconet PIA	10.10.1.240
9.6	Synology Cat	201.234.213.50

Tabla 9: Activos principales para acceso a Sistema de Nómina.

Item	Descripción	Dirección IP
10.1	Switch de Acceso RRHH	10.15.15.245, 10.15.15.229, 10.15.15.244, 10.14.14.243
10.2	Switch de Acceso Servidores	10.15.15.242
10.3	Switch Core PIA	10.11.1.200
10.4	Servidor Base de Datos	10.11.0.7
10.5	Servidor De aplicación	10.11.0.4
10.6	Switch de Acceso Servidores	S/N
10.7	Servidor de aplicación	10.14.0.9
10.8	Switch de Acceso Servidores	10.12.0.201
10.9	Switch Core PIA	10.12.0.254
10.10	Servidor Base de Datos	10.12.0.12

Tabla 10: Activos principales para acceso a Servicios de Respaldos.

Del listado mostrado en las tablas existe una gran parte de activos que se repiten para cada servicio tecnológico, por lo que se presenta el listado a continuación.

Id	Dispositivo	Descripción
EC_SW_ACCESO	Switch de Acceso	Conjunto de switch de acceso en la red LAN del Parque Industrial Ambato
EC_SW_COREPIA	Switch de Core	Switch Core del Parque Industrial Ambato
CORP_ECUDC01	Servidor Active Directory	Servidor de dominio principal ubicado en el Parque Industrial PIA
EC_ROUTER_PIA	Router Level 3	Router del proveedor Level 3 que da conectividad a la red WAN y acceso a Internet
VPN_AZURE	VPN Azure	Servicio de red virtual privada con el servicio de Microsoft Azure
CORP_AZUREDC01	Active Directory Azure	Servidor de dominio principal ubicado en el la infraestructura de Azure
ECU_FW_LEVEL3	Firewall Level 3	Equipo de seguridad perimetral administrado por el proveedor de servicios de internet
CORP_ADFS01	ADFS	Servidor de federación de servicios, que permite la autenticación desde internet a la suite office365.
CORP_ADFS02	ADFS	Servidor de federación de servicios alterno, que permite la autenticación desde internet a la suite office365.
CORP_ADFSP01	ADFS Proxy	Servidor proxy de federación de servicios alterno, que permite la conexión entre usuarios externos y el servidor interno de adfs
CORP_ADFSP02	ADFS Proxy	Servidor proxy de federación de servicios alterno, que permite la conexión entre usuarios externos y el servidor interno de adfs
CORP_DIRSYNC	Dirsync	Servidor que permite la sincronización del Active Directory Local de las oficinas con el AD de Azure
	Smtp office365	Granja de servidores de Office 365
EC_ROUTER_TPIA	Router Telconet PIA	Router del proveedor Telconet ubicado en Parque Industrial
PSPISA01	Servidor Impresiones PIA	Servidor ubicado en el parque Industrial y administrado por Martec
NASPIA01	Synology PIA	Sistema de respaldos de la nube corporativa, ubicado en el Parque Industrial
ECUORABD01	Servidor Base de Datos ORADB	Servidor de base de datos del sistema de nómina Ecuador, ubicado en el Parque Industrial
ECUFIN01	Servidor de web services ecufin01	Servidor de web services utilizado por el sistema de nómina Ecuador, ubicado en el Parque Industrial

Tabla 11: Activos sin duplicados de los servicios tecnológicos críticos PIA - Ecuador

Id	Dispositivo	Descripción
EC_SW_CORECAT	Switch Core Catiglata	Switch Core ubicando el Catiglata
EC_ROUTER_TCAT	Router Telconet Catiglata	Router del proveedor Telconet ubicado en Catiglata Level 3
ECUMITROL01	Servidor Mitrol Aplicación	Servidor de aplicación de Mitrol ubicado en Catiglata
MITE1X-PC	Servidor Mitrol Comunicaciones	Central telefónica de Mitrol ubicado en Catiglata
HIPATH	Central de Comunicaciones SIEMENS	Central telefónica Siemens ubicada en Catiglata
PIA01	Servidor Impresiones Catiglata	Servidor ubicado en el Catiglata y administrado por Martec
NASCAT01	Synology Cat	Sistema de respaldos de la nube corporativa, ubicado en Catiglata

Tabla 12: Activos sin duplicados de los servicios tecnológicos críticos Catiglata - Ecuador

Id	Dispositivo	Descripción
CO_FW_LEVEL3	Firewall Level 3 Bogota XV	Equipo de seguridad que provee los controles en el data center Bogotá XV
PISADBPRD01	Servidor SAP DB	Servidor de base de datos del sistema SAP Ubicado en el data center Bogota XV
PISAPRD01	Servidor SAP	Servidor de aplicación del sistema SAP Ubicado en el data center Bogota XV
PISABWPRD01	Servidor BW	Servidor BW ubicado en el data center Bogota XV
OPTIMIZAAPP	Servidor de aplicación optimiza	servidor que ejecuta la aplicación optimiza y a los cuales se conectan los usuarios, ubicado en el data center de Bogota XV
OPTIMIZADB	Servidor de Base de datos optimiza	Servidor que tiene la Base de datos de optimiza, ubicado en el data center de Bogota XV
CO_SW_COREYUM	Switch de Core Yumbo	Switch Core la localidad de Yumbo Colombia
CO_ROUTER_YUM	Router Level 3 Yumbo	Router del proveedor de telecomunicaciones que nos da la conectividad para la localidad de Yumbo Colombia
PISADOMIN01	Servidor Active Directory WR Data Center Level3	Servidor de dominio principal ubicado en el data center de Bogota XV
CORP-COLDC01	Servidor Active Directory RO Yumbo	Servidor de dominio de lectura ubicado en Yumbo Colombia
COLTMG01	Firewall TMG	Equipo que cumple las funcionalidades de firewall en la oficina de Yumbo Colombia
CO_SW_ACCESO	Switch de acceso Yumbo	Conjunto de switch de acceso en la red LAN de la localidad de Yumbo Colombia
COLMIT01	Servidor Mitrol Aplicación	Servidor de aplicación de Mitrol ubicado en Yumbo Colombia
COLMITBD01	Servidor Mitrol Base de Datos	Central telefónica de Mitrol ubicado en Yumbo Colombia
CO_ROUTER_YUM_TEL	Router de comunicaciones Colombia	Router que da la conectividad a la red PSTN para la salida telefónica de la centrales
COLIMP01	Servidor de Impresión Yumbo	Servidor que controla las impresiones en la localidad de Yumbo Colombia
NASYUMBO01	Synology Colombia	Servidor de respaldos de información en Yumbo Colombia

Tabla 13: Activos sin duplicados de los servicios tecnológicos críticos Colombia

Id	Dispositivo	Descripción
PE_ROUTER_YUM	Router Level 3 Lima	Equipo ruteador de Lima que permite la comunicación a la red corporativa empresarial de Plasticaucho e Internet
PERDC01	Servidor Active Directory RO Lima	Servidor de dominio principal ubicado en el Parque Industrial PIA
SERVERNET	Servidor de marcaciones	Servidor que cuenta con la herramienta de marcaciones de asistencia del personal

Tabla 14: Activos sin duplicados de los servicios tecnológicos críticos Perú

4.7.5. Dependencia de Activos.

Se ha realizado la dependencia de activos jerárquicamente de acuerdo a los principales activos que conforman el nivel de servicios.

VPN	SI1	
SwitchCore - PIA		SWITCH1
UPS		UPS1
Aire Acondicionado		AC1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1

Tabla 15: Dependencias de la VPN

Directorio Activo, DNS, DHCP	SI2	
Servidor AD Principal		VHOST1
Servidor de Virtualización		HOST2
UPS		UPS1
		AC1
Cableado LAN		CABLING1
Servidor AD Secundario		VHOST2
Servidor de Virtualización		HOST3
UPS		UPS2
Aire Acondicionado		AC2
Cableado LAN		CABLING2

Tabla 16: Dependencias del Directorio Activo

Telefonía	SI3	
Centralita Hipath 3800		PABX1
UPS		UPS1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1
Centralita ExpansionBox Hipath 3800		PABX2
UPS		UPS2
Cableado LAN		CABLING2
Cableado Eléctrico		WIRE2
Servidor de Telefonía IP		HOST6
UPS		UPS2
Aire Acondicionado		AC2
Cableado LAN		CABLING2
Servidor AD Secundario		VHOST2
Servidor de Virtualización		HOST3
UPS		UPS2
Aire Acondicionado		AC2
Cableado LAN		CABLING2

Tabla 17: Dependencias de Telefonía

Correo Electrónico	SE1	
SwitchCore - PIA		SWITCH1
UPS		UPS1
Aire Acondicionado		AC1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1

Tabla 18: Dependencias del Correo Electrónico

Internet	SE2	
SwitchCore - PIA		SWITCH1
UPS		UPS1
Aire Acondicionado		AC1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1

Tabla 19: Dependencias del Internet

SAP	SE3	
SwitchCore - PIA		SWITCH1
UPS		UPS1
Aire Acondicionado		AC1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1

Tabla 20: Dependencias del Aplicativo SAP

BW	SE4	
SwitchCore - PIA		SWITCH1
UPS		UPS1
Aire Acondicionado		AC1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1

Tabla 21: Dependencias del Aplicativo para BW

Solución Optimiza	SE5	
SwitchCore - PIA		SWITCH1
UPS		UPS1
Aire Acondicionado		AC1
Cableado LAN		CABLING1
Cableado Eléctrico		WIRE1

Tabla 22: Dependencias de la Solución Optimiza

Impresión	SE6	
Cableado LAN		CABLING1
Cableado LAN		CABLING2

Tabla 23: Dependencias del Servicio de Impresión

4.7.6. Dimensiones de valoración.

Para la valoración de activos, se tomarán las dimensiones propuestas por la metodología valorando 5 aspectos que se detallan a continuación:

[D] Disponibilidad.

Propiedad o característica de los activos, consiste en que los usuarios o procesos autorizados tienen acceso a los servicios tecnológicos cuando lo requieren[18].

[I] Integridad de los datos.

Propiedad o característica en que la información almacenada de los diferentes servicios tecnológicos no ha sido alterada de manera no autorizada[18].

[C] Confidencialidad de la información.

Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a usuarios o procesos no autorizados[18].

[A] Autenticidad.

Propiedad o característica consistente en que un usuario es quien dice ser o bien que garantiza la fuente de la que proceden los datos[18].

[T] Trazabilidad.

Propiedad o característica consistente en que las actuaciones de un usuario o proceso puede ser imputadas exclusivamente a dicha entidad[18].
Estas dimensiones las utilizaremos en caso de que una amenaza se materialice para poder valorar las consecuencias y la extensión del perjuicio que ocasionaría si los activos se vieran comprometidos.
La valoración de activos se realizará con un enfoque técnico dado por los encargados del área de infraestructura en el departamento de TI y acorde a la escala de la siguiente tabla:

Valor		Criterio
10	Extremo	Altamente crítico
9	Muy alto	Muy crítico
6 – 8	Alto	Crítico
3 – 5	Medio	importante
1 – 2	Bajo	De Criticidad baja
0	Depreciable	Irrelevante

Tabla 24: Criterios de Valoración

A continuación se muestra el análisis de activos con su valoración de acuerdo a las dimensiones propuestas por la metodología:

Activos		Criterios				
Id	**Descripción**	**D**	**I**	**C**	**A**	**T**
EC_SW_ACCESO	Switch de Acceso	8	7	5	6	6
EC_SW_COREPIA	Switch de Core	10	9	7	9	8
CORP_ECUDC01	Servidor Active Directory	10	10	5	8	7
EC_ROUTER_PIA	Router Level 3	10	9	9	8	8
VPN_AZURE	VPN Azure	9	10	5	8	7
CORP_AZUREDC01	Active Directory Azure	9	10	5	8	7
ECU_FW_LEVEL3	Firewall Level 3	9	5	6	8	8
CORP_ADFS01	ADFS	9	10	5	8	7
CORP_ADFS02	ADFS	9	10	5	8	7
CORP_ADFSP01	ADFS Proxy	9	10	5	8	7
CORP_ADFSP02	ADFS Proxy	9	10	5	8	7
CORP_DIRSYNC	Dirsync	9	10	5	8	7
	Smtp Office365					
EC_ROUTER_TPIA	Router Telconet PIA	9	9	9	6	6
PSPISA01	Servidor Impresiones PIA	9	6	8	9	9
NASPIA01	Synology PIA	8	9	9	9	8
ECUORABD01	Servidor Base de Datos ORADB	10	10	10	10	9
ECUFIN01	Servidor de web Services ecufin01	9	9	6	6	7

Tabla 25: Inventario y valoración de los activos principales PIA - Ecuador

Activos		Criterios				
Id	**Descripción**	**D**	**I**	**C**	**A**	**T**
EC_SW_CORECAT	Switch Core Catiglata	10	9	7	9	8
EC_ROUTER_TCAT	Router Telconet Catiglata	9	9	9	6	6
ECUMITROL01	Servidor Mitrol Aplicación	9	10	10	8	9
MITE1X-PC	Servidor Mitrol Comunicaciones	10	10	8	8	9
HIPATH	Central de Comunicaciones SIEMENS	8	8	6	6	7
PIA01	Servidor Impresiones Catiglata	9	6	8	9	9
NASCAT01	Synology Cat	8	9	9	9	8

Tabla 26: Inventario y valoración de los activos principales Catiglata - Ecuador

Activos		Criterios				
Id	**Descripción**	**D**	**I**	**C**	**A**	**T**
CO_FW_LEVEL3	Firewall Level 3 Bogota XV	10	9	9	7	5
PISABWPRD01	Servidor BW	9	10	10	10	9
PISAPRD01	Servidor SAP	10	10	10	10	10
OPTIMIZAAPP	Servidor de aplicación optimiza	8	10	10	10	8
OPTIMIZADB	Servidor de Base de datos optimiza	8	10	10	10	8
CO_SW_COREYUM	Switch de Core Yumbo	10	9	7	9	8
CO_ROUTER_YUM	Router Level 3 Yumbo	10	9	9	7	5
PISADOMIN01	Servidor Active Directory WR Data Center Level3	10	10	5	8	7
CORP-COLDC01	Servidor Active Directory RO Yumbo	10	10	5	8	7
COLTMG01	Firewall TMG	9	5	6	8	8
CO_SW_ACCESO	Switch de acceso Yumbo	8	7	5	6	6
COLMIT01	Servidor Mitrol Aplicación	9	10	10	8	9
COLMITBD01	Servidor Mitrol Base de Datos	10	10	8	8	9
CO_ROUTER_YUM_TEL	Router de comunicaciones Colombia	9	9	9	7	5
COLIMP01	Servidor de Impresión Yumbo	9	6	8	9	9
NASYUMBO01	Synology Colombia	8	9	9	9	8

Tabla 27: Inventario y valoración de los activos principales Colombia

Activos		Criterios				
Id	**Descripción**	**D**	**I**	**C**	**A**	**T**
PE_ROUTER_YUM	Router Level 3 Lima	10	9	9	7	5
PERDC01	Servidor Active Directory RO Lima	10	10	5	8	7
SERVERNET	Servidor de marcaciones	8	9	8	7	5

Tabla 28: Inventario y valoración de los activos principales Perú

4.7.7. Análisis de Amenazas

Para el análisis de amenazas se ha identificado los servicios críticos, se ha levantado la información de los activos tecnológicos relacionados y se propone evaluar y valorar las posibles amenazas.

Se va a trabajar con un listado de amenazas propuesta por la metodología Magerit la misma plantea que una amenaza afecta a determinados activos y en específicas dimensiones. A continuación se listan las amenazas mencionadas:

4.7.7.1. Fuego

Fuego	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [D] disponibilidad

Figura 4: Desastres Naturales - Fuego

4.7.7.2. Erupción Volcánica

Erupción Volcánica	
Tipos de activos: [COM] redes de comunicaciones [AUX] equipamiento auxiliar [HW] equipos informáticos (hardware)	**Dimensiones:** [D] disponibilidad [A] autenticidad [T] trazabilidad

Figura 5: Desastres Naturales - Erupción Volcánica

4.7.7.3. Terremoto

Terremoto	
Tipos de activos: [COM] redes de comunicaciones [AUX] equipamiento auxiliar [HW] equipos informáticos (hardware)	**Dimensiones:** [D] disponibilidad [T] trazabilidad

Figura 6: Desastres Naturales - Terremoto

4.7.7.4. Avería de origen físico o lógico

Avería de origen fisico o lógico	
Tipos de activos: [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	**Dimensiones:** [D] disponibilidad

Figura 7: De origen Industrial - Avería de origen físico o lógico

4.7.7.5. Corte del suministro eléctrico

Corte del suministro eléctrico	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	**Dimensiones:** [D] disponibilidad

Figura 8: De origen Industrial - Corte del suministro eléctrico

4.7.7.6. Condiciones inadecuadas de temperatura

Condiciones inadecuadas de temperatura	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	**Dimensiones:** [D] disponibilidad

Figura 9: De origen Industrial - Condiciones inadecuadas de temperatura

4.7.7.7. Errores de usuarios

Errores de los usuarios	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [Media] soportes de información	**Dimensiones:** [D] disponibilidad [I] integridad [C] confidencialidad

Figura 10: Errores y fallos no intencionados- Errores de usuarios

4.7.7.8. Errores del administrador

Errores del administrador	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [Media] soportes de información [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	**Dimensiones:** [D] disponibilidad [I] integridad [C] confidencialidad

Figura 11: Errores y fallos no intencionados - Errores de administrador

4.7.7.9. Difusión de Software dañino

Difusión de software dañino	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** [D] disponibilidad [I] integridad [C] confidencialidad

Figura 12: Errores y fallos no intencionados - Difusión de software dañino

4.7.7.10. Fallo de servicios de comunicaciones

Fallo de servicios de comunicaciones	
Tipos de activos: [COM] redes de comunicaciones	**Dimensiones:** [D] disponibilidad

Figura 13: Errores y fallos no intencionados - Fallo de servicios de comunicaciones

4.7.7.11. Alteración Accidental de la información

Alteración accidental de la información	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [Media] soportes de información [COM] redes de comunicaciones	**Dimensiones:** [I] integridad

Figura 14: Errores y fallos no intencionados - Alteración Accidental de la información

4.7.7.12. Destrucción de la información

Destrucción de información	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [Media] soportes de información [COM] redes de comunicaciones	**Dimensiones:** [D] disponibilidad

Figura 15: Errores y fallos no intencionados - Destrucción de la información

4.7.7.13. Fugas de información

Fugas de información	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [Media] soportes de información [COM] redes de comunicaciones [P] personal (revelación)	**Dimensiones:** [C] confidencialidad

Figura 16: Errores y fallos no intencionados - Fugas de información

4.7.7.14. Pérdida de Equipos

Pérdida de equipos	
Tipos de activos: [HW] equipos informáticos (hardware) [AUX] equipamiento auxiliar [Media] soportes de información	**Dimensiones:** [D] disponibilidad [C] confidencialidad

Figura 17: Errores y fallos no intencionados - Pérdida de Equipos

4.7.7.15. Suplantación de identidad del usuario

Suplantación de la identidad del usuario	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones	**Dimensiones:** [C] confidencialidad [A] autenticidad [I] integridad

Figura 18: Errores y fallos no intencionados - Terremoto

4.7.7.16. Abuso de Privilegios de Acceso

Abuso de privilegios de acceso	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	**Dimensiones:** [I] integridad [D] disponibilidad [C] confidencialidad

Figura 19: Errores y fallos no intencionados - Abuso de Privilegios de Acceso

4.7.7.17. Acceso no autorizado

Acceso no autorizado	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [I] integridad [C] confidencialidad

Figura 20: Errores y fallos no intencionados - Acceso no autorizado

4.7.7.18. Manipulación de Equipos

Manipulación de los equipos	
Tipos de activos: [HW] equipos informáticos (hardware) [AUX] equipamiento auxiliar [Media] soportes de información	**Dimensiones:** [C] confidencialidad [D] disponibilidad

Figura 21: Errores y fallos no intencionados - Manipulación de Equipos

4.7.7.19. Robo

Robo	
Tipos de activos: [HW] equipos informáticos (hardware) [AUX] equipamiento auxiliar [Media] soportes de información	**Dimensiones:** [C] confidencialidad [D] disponibilidad

Figura 22: Errores y fallos no intencionados - Robo

4.7.7.20. Extorsión

Extorsión	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información	**Dimensiones:** [I] integridad [C] confidencialidad [D] disponibilidad

Figura 23: Errores y fallos no intencionados - Extorsión

4.7.7.21. Ingeniería social

Ingeniería social (picaresca)	
Tipos de activos: [P] personal interno	**Dimensiones:** [I] integridad [D] disponibilidad [C] confidencialidad

Figura 24: Errores y fallos no intencionados - Ingeniería social

4.7.8. Análisis de Amenazas

Para calificar la frecuencia con que las amenazas aparecen se utilizó la **Tabla 29,** que posteriormente nos ayudará también con el cálculo de riesgos e impactos potenciales.

Frecuencia	Valor
FE	100
FA	10
FM	1
FB	0,1
FMB	0,01

Tabla 29: Valores de frecuencia de amenazas.

Tomando en cuenta estas escalas y las amenazas a las que están expuestos los activos se realizo el calculo de la frecuencia con la que sucede cada amenaza y el porcentaje de impacto para cada dimensión. Hay que tener en cuenta que se tomará los valores mas altos en frecuencia y porcentaje de riesgo en las dimensiones para la valoración.

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S1] Acceso a la Red Corporativa	FM	80%	80%	100%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FMB	10%	10%	10%		
[4.2.3.2] Errores del administrador	FM	70%	70%	60%		
[4.2.3.6] Alteración accidental de la información	FMB		50%			
[4.2.3.7] Destrucción de información	FB	80%				
[4.2.3.8] Fugas de información	FM			70%		
[4.2.4.3] Suplantación de la identidad del usuario	FB		50%	70%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FB	50%	80%	50%		
[4.2.4.5] Acceso no autorizado	FMB		80%	50%		
[4.2.4.8] Divulgación de información	FM			100%		

Tabla 30: Valoración de frecuencia de ataques y la disponibilidad de la VPN

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S2] SAP	FM	100%	80%	100%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FM	10%	70%	10%		
[4.2.3.2] Errores del administrador	FB	100%	70%	80%		
[4.2.3.6] Alteración accidental de la información	FMB		70%			
[4.2.3.7] Destrucción de información	FMB	80%				
[4.2.3.8] Fugas de información	FMB			80%		
[4.2.4.3] Suplantación de la identidad del usuario	FB		70%	70%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FMB	50%	80%	50%		
[4.2.4.5] Acceso no autorizado	FB		80%	50%		
[4.2.4.8] Divulgación de información	FM			100%		

Tabla 31: Valoración de frecuencia de ataques y la disponibilidad del Sistema SAP

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S3]Internet	FM	90%	70%	90%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FB	10%	10%	10%		
[4.2.3.2] Errores del administrador	FMB	90%	50%	50%		
[4.2.3.6] Alteración accidental de la información	FB		50%			
[4.2.3.7] Destrucción de información	FB	20%				
[4.2.3.8] Fugas de información	FMB			80%		
[4.2.4.3] Suplantación de la identidad del usuario	FB		70%	70%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FB	50%	70%	70%		
[4.2.4.5] Acceso no autorizado	FB		20%	20%		
[4.2.4.8] Divulgación de información	FM			90%		

Tabla 32: Valoración de frecuencia de ataques y la disponibilidad del Internet

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S4] Correo Electrónico	FM	90%	70%	90%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FB	10%	10%	50%		
[4.2.3.2] Errores del administrador	FB	90%	50%	70%		
[4.2.3.6] Alteración accidental de la información	FB		20%			
[4.2.3.7] Destrucción de información	FB	20%				
[4.2.3.8] Fugas de información	FM			90%		
[4.2.4.3] Suplantación de la identidad del usuario	FM		70%	70%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FB	50%	70%	70%		
[4.2.4.5] Acceso no autorizado	FB		50%	50%		
[4.2.4.8] Divulgación de información	FM			90%		

Tabla 33: Valoración de frecuencia de ataques y la disponibilidad del Correo Electrónico

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S5] Mitrol	FM	100%	70%	100%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FMB	10%	10%	10%		
[4.2.3.2] Errores del administrador	FB	100%	50%	50%		
[4.2.3.6] Alteración accidental de la información	FMB		30%			
[4.2.3.7] Destrucción de información	FMB	50%				
[4.2.3.8] Fugas de información	FB			90%		
[4.2.4.3] Suplantación de la identidad del usuario	FM		70%	70%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FMB	70%	50%	80%		
[4.2.4.5] Acceso no autorizado	FB		50%	90%		
[4.2.4.8] Divulgación de información	FM			100%		

Tabla 34: Valoración de frecuencia de ataques y la disponibilidad del Aplicativo Mitrol

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S6] Impresión	FA	100%	70%	80%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FA	70%	10%	10%		
[4.2.3.2] Errores del administrador	FB	100%	30%	30%		
[4.2.3.6] Alteración accidental de la información	FB		10%			
[4.2.3.7] Destrucción de información	FB	50%				
[4.2.3.8] Fugas de información	FB			60%		
[4.2.4.3] Suplantación de la identidad del usuario	FM		70%	70%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FB	20%	20%	80%		
[4.2.4.5] Acceso no autorizado	FB		20%	80%		
[4.2.4.8] Divulgación de información	FB			80%		

Tabla 35: Valoración de frecuencia de ataques y la disponibilidad del Servicio de Impresión

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S7] Movilidad/Optimiza	FA	100%	90%	80%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FA	10%	80%	10%		
[4.2.3.2] Errores del administrador	FB	100%	30%	30%		
[4.2.3.6] Alteración accidental de la información	FA		50%			
[4.2.3.7] Destrucción de información	FB	20%				
[4.2.3.8] Fugas de información	FB			60%		
[4.2.4.3] Suplantación de la identidad del usuario	FMB		90%	50%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FB	80%	20%	80%		
[4.2.4.5] Acceso no autorizado	FMB		20%	80%		
[4.2.4.8] Divulgación de información	FB			70%		

Tabla 36: Valoración de frecuencia de ataques y la disponibilidad del Aplicativo Movilidad/Optimiza

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S8] BI	FM	90%	80%	90%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FB	10%	60%	30%		
[4.2.3.2] Errores del administrador	FB	90%	10%	50%		
[4.2.3.6] Alteración accidental de la información	FM		80%			
[4.2.3.7] Destrucción de información	FMB	20%				
[4.2.3.8] Fugas de información	FMB			80%		
[4.2.4.3] Suplantación de la identidad del usuario	FMB		60%	80%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FB	40%	40%	90%		
[4.2.4.5] Acceso no autorizado	FB		40%	90%		
[4.2.4.8] Divulgación de información	FMB			90%		

Tabla 37: Valoración de frecuencia de ataques y la disponibilidad del Aplicativo BW

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S9] Sistema de Nómina	FM	100%	80%	80%	100%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FB	60%	80%	30%		
[4.2.3.2] Errores del administrador	FM	100%	80%	30%		
[4.2.3.6] Alteración accidental de la información	FB		80%			
[4.2.3.7] Destrucción de información	FMB	80%				
[4.2.3.8] Fugas de información	FB			60%		
[4.2.4.3] Suplantación de la identidad del usuario	FB		60%	80%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FMB	60%	70%	60%		
[4.2.4.5] Acceso no autorizado	FB		70%	60%		
[4.2.4.8] Divulgación de información	FB			60%		

Tabla 38: Valoración de frecuencia de ataques y la disponibilidad del Sistema de Nómina

ACTIVOS [S] Servicios	Frecuencia	D	I	C	A	T
[S10] Respaldos y Restauración	FM	100%	80%	90%	90%	
Amenazas						
[4.2.3.1] Errores de los usuarios	FM	80%	80%	30%		
[4.2.3.2] Errores del administrador	FM	100%	80%	30%		
[4.2.3.6] Alteración accidental de la información	FB		80%			
[4.2.3.7] Destrucción de información	FMB	50%				
[4.2.3.8] Fugas de información	FM			90%		
[4.2.4.3] Suplantación de la identidad del usuario	FB		60%	80%	90%	
[4.2.4.4] Abuso de privilegios de acceso	FB	60%	80%	70%		
[4.2.4.5] Acceso no autorizado	FB		70%	70%		
[4.2.4.8] Divulgación de información	FM			80%		

Tabla 39: Valoración de frecuencia de ataques y la disponibilidad del Servicio de Respaldo y Restauración

ACTIVOS [SW] Software	Frecuencia	D	I	C	A	T
[SW1] Squarenet	FA	100%	100%	75%	100%	
[SW2] Mitrol	FA	100%	100%	75%	100%	
[SW3] Hipath Manager	FA	100%	100%	75%	100%	
LISTA DE AMENAZAS						
[4.2.2.3] Avería de origen físico o lógico	FB	75%				
[4.2.3.1] Errores de los usuarios	FA	10%	10%	10%		
[4.2.3.2] Errores del administrador	FB	50%	30%	30%		
[4.2.3.5] Difusión de software dañino	FB	50%	30%	30%		
[4.2.3.6] Alteración accidental de la información	FMB		10%			
[4.2.3.7] Destrucción de información	FMB	50%				
[4.2.3.8] Fugas de información	FMB			20%		
[4.2.3.9] Vulnerabilidades de los programas (software)	FMB	30%	25%	25%		
[4.2.3.10] Errores de mantenimiento / actualización de programas (software)	FA	50%	30%			
[4.2.4.3] Suplantación de la identidad del usuario	FMB		100%	75%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FMB	50%	25%	25%		
[4.2.4.5] Acceso no autorizado	FMB		50%	75%		
[4.2.4.7] Manipulación de programas	FMB	100%	100%	50%		
[4.2.4.8] Divulgación de información	FMB			50%		

Tabla 40: Valoración de frecuencia de ataques y la disponibilidad del Software

ACTIVOS [HW] Equipamiento Servidor	Frecuencia	D	I	C	A	T
[HOST1] Servidor de BDD	FB	100%	50%	100%		
[HOST2] Servidor de Virtualización -PIA	FB	100%	50%	100%		
[HOST3] Servidor de Virtualización - CAT	FB	100%	50%	100%		
[HOST4] Servidor de Aplicación Mitrol	FB	100%	50%	100%		
[HOST5] Servidor de Comunicaciones Mitrol	FB	100%	50%	100%		
[HOST6] Servidor de Telefonía IP - CAT	FB	100%	50%	100%		
[HOST7] Servidor Administración Telefonía	FB	100%	50%	100%		
[HOST8] Servidor Telefonía IP - UIO	FB	100%	50%	100%		
[HOST9] Servidor de Impresión	FB	100%	50%	100%		
[VHOST1] Servidor AD Principal	FB	100%	50%	100%		
[VHOST2] Servidor AD Secundario	FB	100%	50%	100%		
[VHOST3] Servidor Aplicación SCCM	FB	100%	50%	100%		
[VHOST4] Servidor Base SCCM	FB	100%	50%	100%		
[VHOST5] Servidor Web Services	FB	100%	50%	100%		
[VHOST6] Servidor AD Bogotá	FB	100%	50%	100%		
[VHOST7] Nube Azure	FB	100%	50%	100%		
LISTA DE AMENAZAS						
[4.2.1.1] Fuego	FMB	100%				
[4.2.1.2] Erupción Volcánica	FMB	100%				
[4.2.1.3] Terremoto	FMB	100%				
[4.2.2.1] Fuego	FMB	100%				
[4.2.2.2] Daños por Agua	FMB	100%				
[4.2.2.3] Avería de origen físico o lógico	FMB	100%				
[4.2.2.4] Corte del suministro eléctrico	FB	50%				
[4.2.3.2] Errores del administrador	FB	50%	50%	50%		
[4.2.3.11] Pérdida de equipos	FMB	100%		100%		
[4.2.4.4] Abuso de privilegios de acceso	FMB	100%	50%	100%		
[4.2.4.5] Acceso no autorizado	FMB		50%	50%		
[4.2.4.9] Manipulación de los equipos	FMB	50%		50%		
[4.2.4.10] Robo	FMB	100%		100%		
[4.2.4.11] Ataque destructivo	FMB	100%				

Tabla 41: Valoración de frecuencia de ataques y la disponibilidad del Equipamiento Servidor

ACTIVOS [COM] Redes de comunicaciones	Frecuencia	D	I	C	A	T
[LAN1][LAN2][LAN3][LAN4][LAN5] Red Local	FB	100%	30%	50%	100%	
[WAN1][WAN2][WAN3][WAN4][WAN5] Enlaces entre sucursales	FB	100%	30%	50%	100%	
[WIFI1][WIFI2][WIFI3][WIFI4][WIFI5] Red Inalámbrica	FB	100%	30%	50%	100%	
[IEX1][IEX2][IEX3][IEX4][IEX5] Internet	FB	100%	30%	50%	100%	
[IPPHONE1][IPPHONE2][IPPHONE3] Telefonía IP	FB	100%	30%	50%	100%	
LISTA DE AMENAZAS						
[4.2.1.2] Erupción Volcánica	FMB	100%				
[4.2.1.3] Terremoto	FMB	100%				
[4.2.2.5] Fallo de servicios de comunicaciones	FB	50%				
[4.2.3.6] Alteración accidental de la información	FMB		20%			
[4.2.3.7] Destrucción de información	FMB	30%				
[4.2.3.8] Fugas de información	FB			20%		
[4.2.4.3] Suplantación de la identidad del usuario	FMB		25%	40%	100%	
[4.2.4.4] Abuso de privilegios de acceso	FMB	35%	10%	40%		
[4.2.4.5] Acceso no autorizado	FMB		30%	50%		
[4.2.4.6] Análisis de tráfico	FMB			20%		
[4.2.4.8] Divulgación de información	FMB			40%		

Tabla 42: Valoración de frecuencia de ataques y la disponibilidad de Redes de comunicaciones

ACTIVOS [Media] Soportes de información	Frecuencia	D	I	C	A	T
[NAS1][NAS2][NAS3][NAS4] Equipos de Respaldo	FB	100%	75%	100%		
LISTA DE AMENAZAS						
[4.2.1.1] Fuego	FMB	100%				
[4.2.2.1] Fuego	FMB	100%				
[4.2.2.2] Daños por Agua	FMB	100%				
[4.2.2.3] Avería de origen físico o lógico	FMB	100%				
[4.2.2.4] Corte del suministro eléctrico	FB	50%				
[4.2.3.1] Errores de los usuarios	FMB	10%	10%	10%		
[4.2.3.2] Errores del administrador	FMB	40%	20%	20%		
[4.2.3.6] Alteración accidental de la información	FMB		10%			
[4.2.3.7] Destrucción de información	FMB	10%				
[4.2.3.8] Fugas de información	FMB			50%		
[4.2.3.11] Pérdida de equipos	FMB	50%		100%		
[4.2.4.5] Acceso no autorizado	FMB		75%	100%		
[4.2.4.8] Divulgación de información	FMB			75%		
[4.2.4.9] Manipulación de los equipos	FMB	50%		50%		
[4.2.4.10] Robo	FMB	100%		100%		
[4.2.4.11] Ataque destructivo	FMB	100%				

Tabla 43: Valoración de frecuencia de ataques y la disponibilidad de Soportes de información

ACTIVOS [AUX] Equipamiento Auxiliar	Frecuencia	D	I	C	A	T
[UPS1] UPS	FB	100%	50%	100%		
[AC1] Aire Acondicionado	FB	100%	50%	100%		
[CABLING1] Cableado LAN	FB	100%	50%	100%		
[WIRE1] Cableado Eléctrico	FB	100%	50%	100%		
[FIBER1] Fibra óptica	FB	100%	50%	100%		
[FORNITURE1] Racks	FB	100%	50%	100%		
LISTA DE AMENAZAS						
[4.2.1.1] Fuego	FMB	100%				
[4.2.1.2] Erupción Volcánica	FMB	100%				
[4.2.1.3] Terremoto	FMB	100%				
[4.2.2.1] Fuego	FMB	100%				
[4.2.2.2] Daños por Agua	FMB	100%				
[4.2.2.3] Avería de origen físico o lógico	FB	100%				
[4.2.2.4] Corte del suministro eléctrico	FB	100%				
[4.2.3.11] Pérdida de equipos	FMB	50%		5%		
[4.2.4.5] Acceso no autorizado	FMB		50%	50%		
[4.2.4.9] Manipulación de los equipos	FB	100%		50%		
[4.2.4.10] Robo	FMB	100%		100%		
[4.2.4.11] Ataque destructivo	FMB	100%				

Tabla 44: Valoración de frecuencia de ataques y la disponibilidad del Equipamiento Auxiliar

ACTIVOS [P] Personal - Responsables	Frecuencia	D	I	C	A	T
[OP1] Operadores	FB	75%	50%	70%		
[ADM1] Jefe Sistemas	FB	75%	50%	70%		
[COM1] Administrador infraestructura y Redes	FB	75%	50%	70%		
[SEC1] Agente de Seguridades	FB	75%	50%	70%		
[ADM2] Consultores Internos	FB	75%	50%	70%		
[DES1] Analistas Programadores	FB	75%	50%	70%		
LISTA DE AMENAZAS						
[4.2.3.8] Fugas de información	FMB			70%		
[4.2.4.12] Indisponibilidad del personal	FB	75%				
[4.2.4.13] Extorsión	FMB	50%	50%	50%		
[4.2.4.12] Ingeniería social (picaresca)	FMB	20%	20%	20%		

Tabla 45: Valoración de frecuencia de ataques y la disponibilidad del Personal - Responsable

ACTIVOS [P] Personal - Usuarios	Frecuencia	D	I	C	A	T
[UI1] Usuarios Internos	FB	50%	20%	50%		
LISTA DE AMENAZAS						
[4.2.3.8] Fugas de información	FMB			50%		
[4.2.4.12] Indisponibilidad del personal	FB	50%				
[4.2.4.13] Extorsión	FMB	10%	10%	10%		
[4.2.4.12] Ingeniería social (picaresca)	FMB	20%	20%	20%		

Tabla 46: Valoración de frecuencia de ataques y la disponibilidad del Personal - Usuarios

4.7.9. Cálculo del Impacto Potencial

Siguiendo las bases dadas por Magerit[18], una vez valoradas las amenazas (al igual que los activos desde un enfoque técnico) en función del porcentaje de afectación del impacto para cada dimensión se tiene que realizar la siguiente operación:

Impacto Potencial = % Impacto * Valor del Activo

De esta manera tenemos el valor resultante que viene a ser el impacto potencial, mismo que nos servirá para encontrar el riesgo potencial, el cálculo de los mismos se encuentra en el **ANEXO D**.

4.7.10. Cálculo del Riesgo Potencial

Con el impacto potencial ahora es necesario identificar la probabilidad de ocurrencia que pueden llegar a tener las amenazas, los valores mas altos representarán los que tienen más riesgo.
Con la multiplicación de estos valores obtenemos el riesgo potencial:

Riesgo Potencial = Impacto Potencial * Probabilidad de Ocurrencia

A continuación se listan los activos con el valor de los riesgos potenciales priorizados tomando como umbral los que tienen un valor de riesgo mayor o igual a 30 en cualquiera de sus dimensiones y asumiendo los riesgos con valores menores que no constan en la siguiente tabla, para ver los cálculos completos estos están en el **ANEXO E.**

Id	Descripción	Amenaza	D	I	C	A
EC_SW_COREPIA	Switch de Core	Erupción Volcánica	30	6,75	0	0
CORP_ECUDC01	Servidor Active Directory	Difusión de Software dañino	36	28	14	22,4
EC_ROUTER_PIA	Router Level 3	Erupción Volcánica	30	13,5	0	0
PSPISA01	Servidor Impresiones PIA	Difusión de Software dañino	32,4	16,8	22,4	25,2
NASPIA01	Synology PIA	Difusión de Software dañino	28,8	36	25,2	25,2
ECUORABD01	Servidor Base de Datos ORADB	Erupción Volcánica	30	30	0	0
		Difusión de Software dañino	36	36	28	28
		Acceso no autorizado	15	27	27	30
ECUFIN01	Servidor de web services ecufin01	Difusión de Software dañino	32,4	25,2	7,2	7,2

Tabla 47: Riesgo Potencial de activos y amenazas PIA-Ecuador

Id	Descripción	Amenaza	D	I	C	A
ECUMITROL01	Servidor Mitrol Aplicación	Difusión de Software dañino	32,4	28	28	22,4
		Suplantación de identidad del usuario	10,8	36	36	28,8
MITE1X-PC	Servidor Mitrol Comunicaciones	Difusión de Software dañino	36	28	22,4	22,4
		Fallo de servicios de comunicaciones	40	4	0	0
PIA01	Servidor Impresiones Catiglata	Difusión de Software dañino	32,4	16,8	22,4	25,2
NASCAT01	Synology Cat	Difusión de Software dañino	28,8	36	25,2	25,2

Tabla 48: Riesgo Potencial de activos y amenazas Catiglata-Ecuador

Id	Descripción	Amenaza	D	I	C	A
CO_FW_LEVEL3	Firewall Level 3 Bogota XV	Errores del administrador	32	7,2	10,8	0
OPTIMIZAAPP	Servidor de aplicación optimiza	Errores del administrador	32	36	12	0
		Difusión de Software dañino	28,8	36	8	8
		Acceso no autorizado	12	24	30	30
OPTIMIZADB	Servidor de Base de datos optimiza	Errores del administrador	32	36	12	0
		Difusión de Software dañino	28,8	36	8	8
		Acceso no autorizado	12	24	30	30
PISADOMIN01	Servidor Active Directory WR Data Center Level3	Difusión de Software dañino	36	28	14	22,4
CORP-COLDC01	Servidor Active Directory RO Yumbo	Difusión de Software dañino	36	28	14	22,4
COLMIT01	Servidor Mitrol Aplicación	Errores del administrador	32,4	28	12	0
		Difusión de Software dañino	32,4	28	28	22,4
		Suplantación de identidad del usuario	10,8	36	36	28,8
COLMITBD01	Servidor Mitrol Base de Datos	Errores del administrador	36	28	9,6	0
		Difusión de Software dañino	36	28	22,4	22,4
		Fallo de servicios de comunicaciones	30	3	0	0
		Destrucción de la información	27	30	0	0
		Suplantación de identidad del usuario	12	36	28,8	28,8
CO_ROUTER_YUM_TEL	Router de comunicaciones Colombia	Avería de origen físico o lógico	32,4	18	0	0
		Fallo de servicios de comunicaciones	36	3,6	0	0
COLIMP01	Servidor de Impresión Yumbo	Difusión de Software dañino	32,4	16,8	22,4	25,2
NASYUMBO01	Synology Colombia	Difusión de Software dañino	28,8	36	25,2	25,2

Tabla 49: Riesgo Potencial de activos y amenazas Colombia

Id	Descripción	Amenaza	D	I	C	A
PE_ROUTER_LIM	Router Level 3 Lima	Corte del suministro eléctrico	30	13,5	0	0
PERDC01	Servidor Active Directory RO Lima	Avería de origen físico o lógico	36	20	0	0
		Corte del suministro eléctrico	40	4	0	0
		Difusión de Software dañino	36	28	14	22,4

Tabla 50: Riesgo Potencial de activos y amenazas Perú

4.7.11. Salvaguardas

Una vez analizados los diferentes riesgos y después de haberlos priorizados, se tienen que buscar las medidas a tomar para salvaguardar los mismos, las actividades para cumplir las salvaguardas se llevarán en un anexo que contemplará las fechas correspondientes, a continuación se listan los riesgos y las salvaguardas segmentando los activos por tipo y por quien esta encargado de realizarla:

Amenazas	R. Potencial	Activos	Salvaguardas	Responsable
Erupción Volcánica	30	EC_SW_COREPIA	Elaborar un plan de protección de los equipos que indique el procedimiento a seguir desde la notificación por parte del comité de emergencia hasta proteger los equipos de la ceniza o repercusiones de una posible erupción.	Héctor Gutierrez
			Elaborar un plan de respaldo de la configuración	Alexander Rojas

Tabla 51: Salvaguardas de activos en la categoría Switch

Amenazas	R. Potencial	Activos	Salvaguardas	Responsable
Erupción Volcánica	30	EC_ROUTER_PIA	Elaborar un plan de protección de los equipos que indique el procedimiento a seguir desde la notificación por parte del comité de emergencia hasta proteger los equipos de la ceniza o repercusiones de una posible erupción.	Héctor Gutierrez
Avería de origen físico o lógico	32,4	CO_ROUTER_ YUM_TEL	Analizar el tiempo de vida útil del dispositivo y elaborar un plan de renovación para el mismo.	Héctor Rincón
Fallo de servicios de comunicaciones	36	CO_ROUTER_ YUM_TEL	Elaborar un plan de respaldo de la configuración y accesos al dispositivo.	Héctor Rincón
Corte del suministro eléctrico	30	PE_ROUTER_LIM	Evaluar el tiempo de suministro de energía eléctrica de respaldo y definir el plan de acción en base a esa identificación.	Edu Gil - José Antonio Hernandez

Tabla 52: Salvaguardas de activos en la categoría Router

Amenazas	R. Potencial	Activos	Salvaguardas	Responsable
Errores del Administrador	32	CO_FW_LEVEL3	Revisar el nivel de servicio y los incidentes presentados con la empresa que nos brinda la gestión sobre el equipo	Alexander Rojas

Tabla 53: Salvaguardas de activos en la categoría Firewall

Amenazas	R. Potencial	Activos	Salvaguardas	Responsable
Erupción Volcánica	30	ECUORABD01	Elaborar un plan de protección de los equipos que indique el procedimiento a seguir desde la notiftcación por parte del comité de emergencia hasta proteger los equipos de la ceniza o repercusiones de una posible erupción.	Héctor Gutierrez
Errores del Administrador	32	OPTIMIZAAPP OPTIMIZADB	Administrar y documentar los permisos de accesos y privilegios por roles	Tomas Chapal - Alexander Rojas
	36	COLMIT01 COLMITBD01	Elaborar un procedimiento gestión de acceso a proveedores a la infraestructura tecnológica	Alexander Rojas
Difusión de Software dañino	36	PSPISA01 PIA01 OPTIMIZAAPP OPTIMIZADB ECUORABD01 ECUFIN01 COLMIT01 NASPIA01 NASCAT01	Implementar un proceso hardering de servidores que incluya una revisión y actualización periódica (al menos una vez semana) de los incidentes presentados	Alexander Rojas
Acceso no autorizado	30	OPTIMIZAAPP OPTIMIZADB ECUORABD01	Implementar políticas de FW propias del sistema y llevar a cabo la ejecución de un Ethical Hacking (al menos una vez al año)	Alexander Rojas
Avería de origen físico o lógico	32,4	PERDC01	Implementar la virtualización del servidor y generar respaldos de la máquina virtual	Héctor Gutierrez
Suplantación de identidad del usuario	36	ECUMITROL01 COLMIT01 COLMITBD01	Revisar las políticas de contraseñas del sistema Mitrol	Alexander Rojas
Fallo de servicios de co-municaciones	40	MITE1X-PC COLMITBD01	Planiftcar y cotizar la compra de una tarjeta de cotizaciones.Incluir en el plan de respaldos el servidores la base de datos Mitrol Colombia	Héctor Gutierrez - Alexander Rojas
Destrucción de la información	30	COLMIT01 COLMITBD01	Evaluar en conjunto con el proveedor el plan de respaldos de estos equipos	Alexander Rojas - Héctor Rincón
Corte del suministro eléctrico	40	PERDC01	Evaluar el tiempo de suministro de energía eléctrica de respaldo y deftnir el plan de acción en base a esa identiftcación	Edu Gil - José Antonio

Tabla 54: Salvaguardas de activos en la categoría Servidores

Las salvaguardas se encuentan en el **ANEXO F.**

CAPÍTULO 5

Conclusiones y Recomendaciones

Conclusiones

- El realizar el levantamiento de los principales activos y sistemas informáticos, permitió conocer cada uno de ellos y su participación en más de un servicio, ayudando a la priorización de los mismos en función a los servicios en los que interviene.
- En base a los requerimientos se determino la metodología Magerit como la óptima para la gestión de riesgos en la empresa Plasticaucho Industrial, ya que se ajusto a las especificaciones por sus características de generación de información cualitativa y cuantitativa, de manera que a futuro su aplicación cuantitativa generando datos precisos para facilitar la toma de decisiones a los directivos de la organización.
- La metodología plantea un sin número de amenazas, por lo que al realizar el análisis de las mismas, se seleccionó únicamente las que afectan a los activos y sistemas informáticos en la empresa, no solo por la infraestructura interna sino también por el medio en el que desarrolla sus actividades, además de incluir algunas amenazas no contempladas en la metodología pero que son igual de importantes.
- Sin un plan de riesgos para poder contener o bajar el impacto de las amenazas, tomaría mucho tiempo detectar las amenazas y poder mitigarlas recuperando la continuadad del negocio.

Recomendaciones

- Para darle un mayor alcance al Plan de Riesgos, se recomienda realizar el levantamiento del resto de activos de la empresa, ya no solo los que conforman el Acuerdo de Servicio, y de igual manera aplicar el proceso, conociendo las amenazas a los que están expuestos y los servicios en los que son participes.

- Se recomienda utilizar una metodología en la elaboración del Plan de Riesgos y Contingencias Informáticas, ya que contemplan los aspectos esenciales que hay que cuidar y tomar en cuenta, también es importante el criterio del autor para determinar aspectos que se complementen a la misma e incluirlos.
- Se recomienda revisar y actualizar periódicamente las amenazas que están actualmente en el documento ya que pueden evolucionar o incrementar otras con el tiempo, especialmente cuando se integre un nuevo servicio a la empresa o exista un nuevo proceso para no dejar ningún activo sin considerarlo.
- El Plan elaborado en este proyecto da lugar a una segunda etapa, en la cual se recomienda incluir los demás activos que en este estudio no fueron considerados por no formar parte del acuerdo de nivel de servicios de la empresa, pero que sin embargo son igual de importantes para la gestión diaria de los colaboradores y así complementar al documento Plan de Riesgos y Contingencias Informáticas.
- Se recomienda realizar un correcto seguimiento de las fechas en la que se acordaron en entregar las salvaguardas por parte de los responsables.

Bibliografia

[1] D. Bravo, "Ecuador se muestra vulnerable a ciberataques," *El Comercio*, 2015.

[2] C. E. Padilla Pacha, "Análisis y gestión de riesgos informáticos para la protección de sistemas de información en el área de tecnologías informáticas del gobierno provincial de tungurahua," *Facultad de Ingeniería en Sistemas Electrónica e Industrial*, 2012.

[3] G. C. T. A. D. F. Llanca Salcan, "Estudio e implementación de una metodología de prevención de intrusos para redes lan," *Faculta de Informática y Electrónica de la Escuela Superior Politécnica del Chimborazo*, 2010.

[4] R. F. y B. M. Khan Olid, "A short review for selecting the best tools and techniques to perform software risk management,," *European Journal of Advances in Engineering and Technology*, p. 7, 2016.

[5] F. R. G. y. D. C. A. Espinosa Criollo, "Centro de gestión de riesgos para monitoreo de redes," *Escuela Politécnica Nacional*, 2012.

[6] C. S. y. H. C. R. K. Rainer, "Risk analysis for information technology," *Journal of Management Information Systems*, vol. VIII, p. 1, 2015.

[7] J. Pérez, "Qué significa lineamiento," *Definicion.de*, 2018.

[8] D. Marrugos, "Análisis tecnológico (diagnóstico tecnológico)," in *Herramienta de toma de desiciones, inteligencia empresarial y gestión del conocimiento.*, 2016.

[9] M. C. B. F. N. J. Solarte, E. R. Enriquez, "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma iso/iec 27001," *Revista Tecnológica Espol*, vol. 28, no. 5, pp. 492–507, 2015.

[10] W. Atehortua, "Proyecto de principio, política y lineamientos de consultas de información de la "maestra de usuarios," *Facultad de Ingeniería y Ciencias Básicas*, 2015.

[11] C. J, *La Seguridad Informática en la PYME, Situación actual y mejores prácticas*. Cornella de Llobregat, eni ed., May 2016.

[12] L. M. Romeral, "Gestión de los riesgos tecnológicos,"

[13] O. Cardona, *Los desastres no son naturales*. Editoral, 1993.

[14] J. J. P. Ruiz, "Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca," *Escuela de Ciencias Básicas Tecnología e Ingeniería Especialización en Seguridad Informática*, 2014.

[15] K. del Rocío Gaona Vásquez, "AplicaciÓn de la metodologÍa magerit para el anÁlisis y gestiÓn de riesgos de la seguridad de la informaciÓn aplicado a la empresa pesquera e industrial bravito s.a. en la ciudad de machala," *UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA*, 2013.

[16] B. Andersson, "Ecuador y casi 100 paises sufren ciberataque extorsivo," *Expreso.ec*, May 2017.

[17] C. Gerencial, "Plan estratégico 2015 - 2018 de plasticaucho industrial.".

[18] M. A. Amutio Gómez and J. Candau, *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Ministerio de Hacienda y Administraciones Públicas, 2012.

Anexos y Apéndices

Anexo A

Acuerdos de Nivel de Servicios (SLA) Plasticaucho.

A.1. OBJETIVO:

Detallar los tiempos de indisponibilidad de los servicios tecnológicos ante eventualidades de la infraestructura y telecomunicaciones de la Empresa o sus proveedores.

A.2. ALCANCE:

Desde la clasificación de los sistema críticos y de alto impacto a la empresa hasta la medición de los indicadores de disponibilidad. No se considera para este acuerdo los tiempos de restauración ante siniestros, estos estarán contenidos en el plan de riesgos.

A.3. DEFINICIONES:

A.3.1. Data Center

Centro de cómputo que alberga servidores y equipos activos de red que permiten hospedar los servicios tecnológicos.

A.3.2. Office 365

Servicio de ofimática y colaboración que reemplaza a la suite Microsoft Office

A.3.3. Switch

Equipo dedicado a mantener las comunicaciones en una red de datos.

A.3.4. Servidor

Equipo de computación de alta capacidad de procesamiento y almacenamiento que permite albergar los servicios tecnológicos.

A.4. ADMINISTRACIÓN DE LOS SERVICIOS TECNOLÓGICOS:

Catálogo de Servicios Tecnológicos.

El área de TI dispone de un catálogo de servicios tecnológicos que permite a los usuarios internos de la empresa cumplir sus funciones y responsabilidades. En base a los procesos de la cadena de valor de la organización se ha podido clasificar e identificar los servicios tecnológicos críticos para la empresa, los cuales se detallan en las siguientes tablas:

N°	Aplicacion	Criticidad	Descripción
1	Servicio de Acceso a la red corporativa Servicio de Acceso a la red corporativa	Alto	Es un servicio que permite la creación, modificación o desactivación de usuarios de la red corporativa.
2	Acceso al aplicativo SAP	Alto	Garantiza la disponibilidad en el uso del aplicativo SAP en todos los procesos de la compañía.
3	Servicios de Internet	Alto	Se da acceso a la red de Internet de acuerdo a un filtrado de contenido web que se especifica en el perfil tecnológico de cada cargo.
4	Servicio de correo electrónico	Alto	Servicio que permite el acceso a las herramientas de comunicación y colaboración como son Correo, mensajería instantánea y One drive.
5	Acceso al aplicativo Mitrol	Alto	Garantiza la disponibilidad en el uso del aplicativo Mitrol para el uso del Contact Center.
6	Servicio de Impresión	Alto	Dar el soporte técnico requerido para que usuarios de la empresa puedan imprimir la información requerida. El servicio incluye los formatos A4 y etiquetas tanto a color como blanco y negro.
7	Servicio de acceso al aplicativo de movilidad	Alto	Servicio que me permite la toma de pedidos y recaudos por parte de los asesores comerciales.
8	Acceso al aplicativo BI	Alto	Dar el soporte requerido para el acceso y el uso de la herramienta de Inteligencia de Negocio.
9	Acceso al aplicativo Nómina (Squarenet, CGUNO, OSIS)	Medio	Garantiza la disponibilidad en el uso del aplicativo de nómina de los diferentes países.
10	Servicio de Respaldos y Restauración de Información	Alto	Servicio que permite a los usuarios de la compañía solicitar al área de TI que la información crítica de la organización sea respaldada en repositorios seguros.

Tabla 55: Servicios Tecnológicos de Criticidad Alta

N°	Aplicación	Criticidad	Descripción
1	Seguridad / Antivirus	Medio	Permite garantizar la seguridad de los Equipos contra amenazas de malware.
2	Servicios de telefonía	Medio	Servicio que permite la habilitación de extensiones telefónicas así como funcionalidades asociadas.
3	Servicio de Videoconferencia	Medio	Servicio que brinda el soporte técnico necesario para el uso de las salas de videoconferencia.
4	Aplicaciones ofimática	Medio	Servicio que garantiza la disponibilidad de las Herramientas Office 365 que se utilizan en oficinas para optimizar, automatizar y mejorar los procedimientos o tareas cotidianas de los usuarios.
5	Instalación y mantenimiento de equipos de cómputo y periféricos	Medio	Servicio que garantiza la disponibilidad de Equipos Hardware para el desempeño diario de sus funciones.
6	Servicio de Acceso a la Intranet	Medio	Servicio que permite el acceso a la intranet, de acuerdo a la ubicación geográfica el acceso será a Ecunet o Intranet para Ecuador y Colombia respectivamente.

Tabla 56: Servicios Tecnológicos de Criticidad Media

N°	Aplicación	Criticidad	Descripción
1	Acceso al aplicativo Financial	Bajo	Dar soporte y facilitar el acceso al aplicativo tanto a los usuarios de la Cooperativa como a la empresa proveedora.
2	Acceso al aplicativo Médico SGM	Bajo	Dar el soporte técnico y garantizar la disponibilidad del aplicativo para la gestión de Dispensario Médico, tanto de PIA como Catiglata.
3	Servicio de pedidos asesores de agentes	Bajo	Proveer el servicio de pedidos online a los asesores de las agencias de Envigado y Montería para que puedan ejercer su labor diaria.
4	Servicios de instalación de utilitarios autorizados por TI	Bajo	Este servicio permite la instalación de varios tipos de software que no sean parte de la infraestructura tecnológica pero se requiere para diferentes procesos de la organización. Por ejemplo ECUAPASS, DIMM, PLE, PDT.
5	Validación técnica y asesoramiento para la compra de Hardware y Software	Bajo	Se valida las necesidades en cuanto a Hardware y Software que los usuario pueden ir necesitando en el trabajo diario.

Tabla 57: Servicios Tecnológicos de Criticidad Baja

A.5. Gestión de la disponibilidad de los servicios tecnológicos

El área de TI pretende medir de manera permanente la disponibilidad de los servicios tecnológicos que ofrece. En una primera etapa se iniciará con los servicios considerados críticos para la empresa. Cuadro A.1, A.2, A.3.

La Gestión de la disponibilidad hace referencia a la característica de un servicio tecnológico para que esté disponible y funcione correctamente cuando un usuario desee hacer uso del mismo.

La forma de medir el indicador es en porcentaje y se calcula en base a la cantidad de horas que un servicio estuvo disponible al mes sobre la cantidad de horas totales del mes.

Disponibilidad del servicio = Cantidad de horas disponibles del servicio tecnológico / Cantidad total de horas en el mes.

A.6. Acuerdo de Nivel de Servicio.

En base a un análisis de los equipos servidores y equipos de comunicación se determina el estado actual de los servicios tecnológicos y la expectativa de tiempo disponible al mes que se puede ofrecer. En base a lo anterior se ha elaborado los Acuerdos de nivel de servicio comprometidos para los servicios tecnológicos de la empresa. El estado de situación actual de los equipos de computación y activos de red se lo puede encontrar en el **Anexo B** del presente documento.
Los niveles de servicio que se ofrecen contempla la operación normal de la infraestructura tecnológica y errores menores que se puedan dar, por ejemplo: sobrecarga en el consumo de recursos computacionales como memoria RAM, procesador, utilización de disco duro o ancho de banda en servidores y equipos activos de red. En caso de existir errores mayores como daño permanente e irreversible en equipos de red o servidores, sean en la infraestructura de Plasticaucho o de los proveedores se los deberá tratar como un proceso de recuperación de desastres y saldrá de este acuerdo de nivel de servicio.
Incidentes de mayor impacto pueden ser considerados como un desastre y tendrán su propio tratamiento y tiempo de respuestas diferentes, los mismos que se indican a continuación:

Recuperación de desastres.

Como se ha mencionado anteriormente, la respuesta ante incidentes graves puede variar el tiempo de recuperación de un servicio tecnológico que incluso puede llegar a no cumplir el nivel de servicio comprometido.
Los incidentes que pueden ser considerados graves y ser catalogados como desastres son:

- Daño de Hardware o Sistema Operativo irreparable de un servidor que provee algún servicio tecnológico.
- Daño de Hardware o Software de los equipos de red.
- Infección de virus a un servidor que provee algún servicio tecnológico.
- Problemas eléctricos o de aire acondicionado en el data center, que obligue al apagado de servidores.
- Fallos humanos.
- Desastres Naturales.

SERVICIO	DESCRIPCIÓN	DISP.	T. DE TOLERANCIA	FORMA DE MEDIR (Tiempo disponible / Tiempo total mes)
Acceso a la red	Servicio que permite que un computador de la empresa tenga acceso a la red empresarial. La no disponibilidad de este servicio afecta a todos los demás servicios (SAP, Nómina, Correo, Internet.	**99,16 %**	6 HORAS	Máximo tiempo de caída de los dispositivos de red (al mes) Datacenter por País.
SAP	Servicio que permite acceso al ERP empresarial.	**99,58 %**	3 HORAS	Este indicador corresponde a la disponibilidad del servidor SAP alojado en el Data Center del proveedor. Se excluye la medición del acceso a la red o problemas de telecomunicaciones.
Internet	Servicio que permite el acceso a la red de Internet con las restricciones de navegación descritas en las políticas de la empresa y en el perftl tecnológico.	**99,30 %**	5 HORAS	Este indicador corresponde a la disponibilidad del enlace de datos provisto por el proveedor de Internet.
Correo Electrónico	Servicio que permite el acceso al envío y recepción de mensaje electrónico internos y con dominios externos.	**99,30 %**	5 HORAS	Este indicador corresponde a los reportes "Estado del Servicio" provisto por la nube Office365. Se excluye la medición de problemas de la red local o enlace de Telecomunicaciones (incluido Internet).
Telefonía Contact Center (MITROL)	Servicio de Acceso a las comunicaciones telefónicas desde los agentes de contact center hacia clientes.	**99,16 %**	6 HORAS	Este indicador corresponde a la disponibilidad del acceso a llamadas telefónicas usando herramientas como mitrol o extensiones telefónicas de líneas analógicas o digitales.
Movilidad	Servicio de acceso a la herramienta tecnológica que permite a los agentes vendedores la toma de pedidos en sus vistas a campo.	**99,16 %**	6 HORAS	Este indicador corresponde a la disponibilidad del servidor de Movilidad alojado en el Data Center de Level 3 en Colombia.
Servicio de Impresión	Servicio que permite la impresión de documentos y etiquetas.	**99,44 %**	4 HORAS	El indicador corresponde al tiempo de disponibilidad para poder realizar impresiones.
SAP BW	Servicio que permite acceso al sistema de reportes de Business Intelligence.	**99,58 %**	3 HORAS	Este indicador corresponde a la disponibilidad del servidor SAP BW alojado en el Data Center del proveedor.
Sistema Nómina	Servicio que permite el acceso al sistema de Nómina de la Empresa.	**99,16 %**	6 HORAS	Este indicador corresponde a la disponibilidad del servidor de Base de Datos y Aplicaciones alojado en el data center del Parque Industrial.
Servicio de Respaldos	Servicio que permite almacenar información en el data center proporcionando respaldo ante fallos de los equipos de usuario.	**99,16 %**	6 HORAS	La disponibilidad se mide sobre los equipos synology ubicados en el Data center de PIA y Catiglata.

Tabla 58: Acuerdos comprometidos con el nivel de servicio.

En base a la infraestructura tecnológica y recursos que dispone el área de Tecnología se ha elaborado un cuadro de los servicios tecnológicos críticos con los tiempos estimados de recuperación ante fallos:

Nota: Para las siguientes tablas se manejarán una convención de colores que identifiquen a cada oficina distribuida en los tres países:

Figura 25: Convención de colores que identifiquen a cada oficina distribuida

SERVICIO	DESCRIPCIÓN	TIEMPO DE RECUPERACIÓN ANTE UN DESASTRE		OBSERVACIONES
Acceso a la red	Servicio que permite que un computador de la empresa tenga acceso a la red empresarial. La no disponibilidad de este servicio afecta a todos los demás servicios.	12 horas		12 Horas para reconfigurar un nuevo servidor de Active Directory WR en Ecuador
		72 horas		72 horas tomaría conseguir un nuevo equipo switch Core y reemplazarlo ante un fallo
		24 horas		24 en conseguir un nuevo equipo para configurarlo como Active Directory RO
SAP	Servicio que permite acceso al ERP empresarial (SAP)	8 horas		Este indicador corresponde al tiempo de restablecimiento máximo permitido al servidor SAP en el Acuerdo Nivel de Servicio con Level 3, o la red de comunicación hacia el data center Colombia.
		8 horas		
		8 horas		
Internet	Servicio que permite el acceso a la red de Internet con las restricciones de navegación descritas en las políticas de la empresa y en el perfil tecnológico.	8 horas		El acceso a Internet es complementario a disponer de acceso a la red corporativa por eso se sujeta a los mismos tiempos y condiciones del servicio "Acceso a la Red" Punto uno de este cuadro.
		8 horas		
		8 horas		
Correo Electrónico	Servicio que permite el acceso al envío y recepción de mensaje electrónico internos y con dominios externos.	6 horas		Este indicador corresponde al tiempo de restablecimiento máximo permitido al servidor de office 365 medido en los servidores de Microsoft. En caso de caída de la red Local el acceso a correo electrónico podría ser a través de cualquier acceso a Internet.
		6 horas		
		6 horas		
Telefonía Contact Center (MITROL)	Servicio de Acceso a la herramienta tecnológica de Atención al Cliente, que gestiona indicadores que permiten el aumentar la retención de clientes y la rentabilidad de la empresa.	72 horas		Tiempo de reemplazo del servidor y/o tarjeta de telefonía en el aplicativo de comunicaciones.
		72 horas		Tiempo de reemplazo del servidor y/o tarjeta de telefonía en el aplicativo de comunicaciones.
Movilidad	Servicio de acceso a la herramienta tecnológica que permite a los agentes vendedores la toma de pedidos en sus vistas a campo.	8 horas		Hace referencia al tiempo de restauración de los servidor de movilidad, albergados en el data center de Level 3 en Colombia.
		8 horas		Hacer referencia al tiempo de reemplazo del switch CORE en caso de daño permanente.
		8 horas		Hace referencia al tiempo de restauración de los servidor de movilidad, albergados en el data center de Level 3 en Colombia.
Servicio de Impresión	Servicio que permite la impresión de documentos y etiquetas.	24 horas		El servicio es tercerizado y el tiempo depende del proveedor de cambio de los equipos que se dañen.
		48 horas		
		N/A		
SAP BW	Servicio que permite acceso al sistema de reportes de Business Intelligence	8 horas		Este indicador corresponde al tiempo de restablecimiento máximo permitido al servidor SAP en el Acuerdo Nivel de Servicio con Level 3, en el data center Colombia.
		8 horas		
		8 horas		
Sistema Nómina	Servicio que permite el acceso al sistema de Nómina de la Empresa.	24 horas		Tiempo de restauración de los backups del servidor y base de datos del sistema de nómina
		72 horas		Tiempo de restauración de los backups del servidor y base de datos del sistema de nómina
		48 horas		Este indicador corresponde al tiempo de restablecimiento máximo permitido al servidor SAP en el Acuerdo Nivel de Servicio con Level 3, en el data center Colombia.
Servicio de Respaldos Synology	Servicio que permite almacenar información en el data center proporcionando respaldo ante fallos de los equipos de usuario	72 horas		Tiempo de restaurar información entre los sitios alternos (PIA-Catiglata)

Figura 26: Servicios tecnológicos críticos con los tiempos estimados de recuperación ante fallos.

Riesgos y posibles Proyectos de Inversión para reducir el tiempo de recuperación ante desastres.

Los dispositivos tecnológicos con los que Plasticaucho cuenta y que no se dispone

de un equipo redundante y prolonga el tiempo de recuperación se lista a continuación:

SERVICIO	PROYECTO PROPUESTO	TIEMPO DE RECUPERACIÓN ANTES DEL PROYECTO	TIEMPO DE RECUPERACIÓN POSTERIOR AL PROYECTO		COSTO ESTIMADO (No presupuestado actualmente)
Acceso a la red	**Proyecto 1.** Sistema de respaldo de servidores incluye Servidor de Active Directory de Ecuador	12 horas	4 horas		$ 30.000
	Proyecto 2. Adquisición y configuración de un switch core con alta disponibilidad (IDC ##)	72 horas	12 horas		$ 8.000
	Proyecto 3. Configuración de servidores virtuales de backup	24 horas	4 horas		$ 3.000
Internet	**Proyecto 1.** Sistema de respaldo de servidores Servidor de Active Directory (incluye storage)	12 horas	4 horas		$ 30.000
	Proyecto 4. Enlace de Internet Redundante para Ecuador	12 horas	1 hora		$ 250
	Proyecto 2. Adquisición y configuración de un switch core con alta disponibilidad	72 horas	4 horas		$ 8.000
	Proyecto 5. Enlace de Internet Redundante para Colombia	12 horas	1 hora		$ 250 mensuales
	Proyecto 3. Configuración de servidores virtuales de backup	24 horas	4 horas		$ 3.000
Telefonía Contact Center (MITROL)	**Proyecto 6.** Compra de un servidor de backup para el servicio de Mitrol en Ecuador	72 horas	12 horas		$ 5.000
	Proyecto 7. Compra de un servidor de backup para el servicio de Mitrol en Ecuador	72 horas	12 horas		$ 5.000
Sistema Nómina	**Proyecto 1.** Sistema de respaldo de servidores Servidor de Active Directory	24 horas	4 horas		$ 30.000
	Proyecto 2. Adquisición y configuración de un switch core con alta disponibilidad	72 horas	12 horas		$ 6.000
	Proyecto 3. Configuración de servidores virtuales de backup	24 horas	4 horas		$ 3.000
Respaldos de la nube corporativa	**Proyecto.** Alta redundancia en los servidores de respaldos	72 horas	2 horas		$ 14.000

Figura 27: Equipos redundantes y prolongación de tiempo de recuperación.

Anexo B

Diagrama de servicios tecnológicos críticos

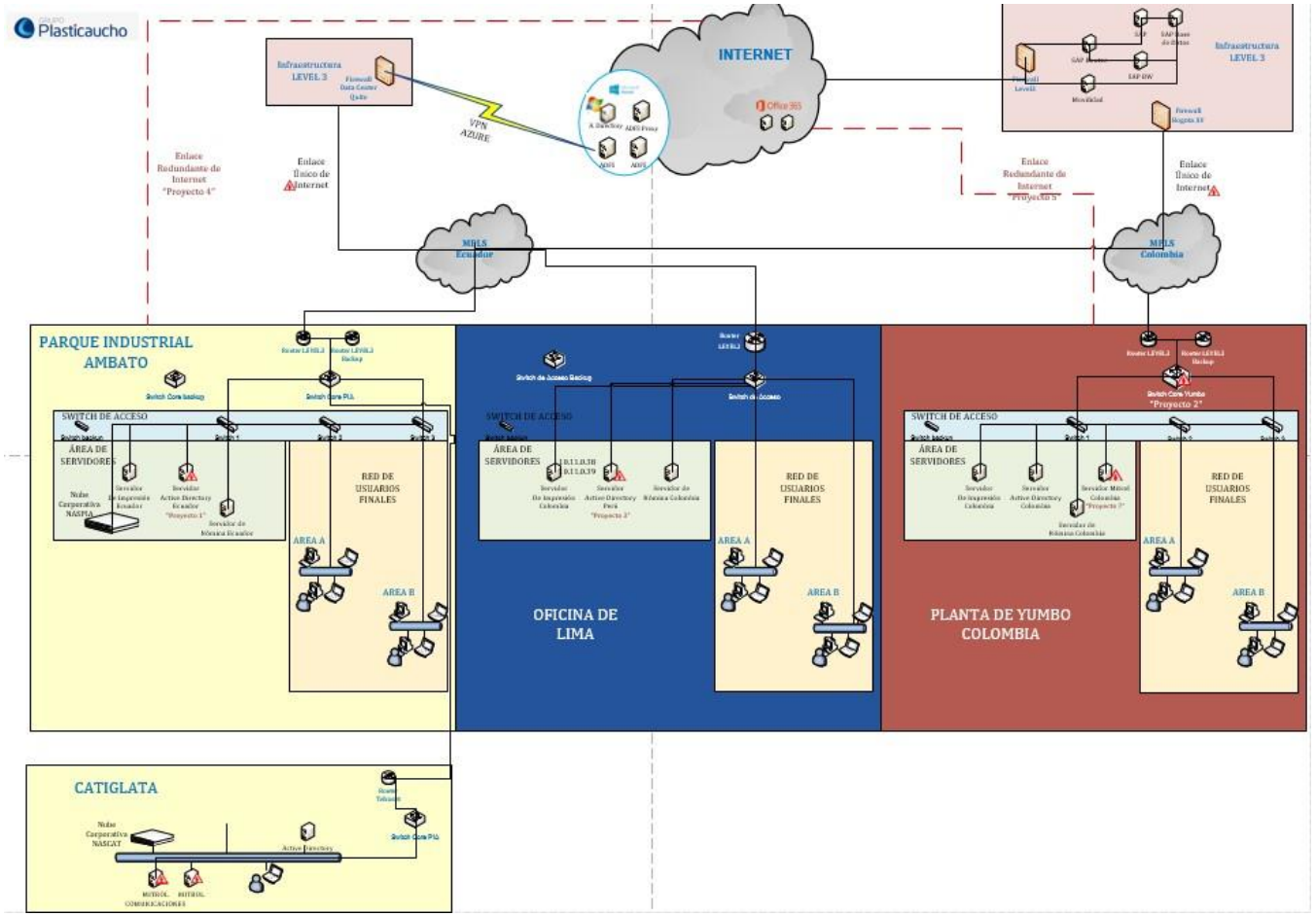


Figura 28: Diagrama de Servicios de Platicaucho Industrial

Anexo C

Entrevista al Encargado de Seguridades de Plasticaucho Industrial

Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Objetivo:
Conocer la situación actual de la empresa Plasticaucho Industrial S.A en tema de seguridades.

Banco de preguntas

1. ¿Qué problemas de seguridad informática ha tenido la empresa en los últimos años Plasticaucho Industrial S.A.?
En los últimos meses tuvimos varios ataques entre los que están el borrado de usuarios del Active Directory, borrado de respaldos y también se cifraron varios archivos.

2. De lo mencionado ¿Cuál considera que fue el ataque más perjudicial para la compañía?
En el que entraron y borraron las grabaciones de Mitrol y algunos archivos importantes de respaldos en el mismo servidor.

3. ¿De qué manera se gestiona actualmente la seguridad informática en la empresa?
Se implemento políticas para que cada mes cambien la contraseña, además esta debe ser como dicen las recomendaciones mínimo de 8 caracteres, deben contener

al menos una mayúscula, una minúscula y un carácter especial. Para las personas clave del negocio se respaldan los archivos en carpetas en el NASPIA. Se enviá comunicados con concejos de seguridad para los usuarios.

4. En el caso de suscitarse un desastre natural, cuenta con un registro de los principales activos que le permita retomar las actividades normales.
No, al momento solo conocemos de memoria algunos de los servidores principales.

5. Actualmente, ¿Posee un proceso de respaldo de información?
Se compro la herramienta Synology para respaldo de la información, con esto a las personas que manejan documentos delicados se les solicito los guarden ahí.

6. En caso de que se sufra un ataque informático, se cuenta con un procedimiento para disminuir el impacto?
La verdad no, simplemente cuando sucede algún ataque lo que hacemos es ver como ayudar a los afectados y corregir para que no ocurra nuevamente.

Alexander Rojas

Encargado de Seguridades

Plasticaucho Industrial

ANEXO D

				Impacto POTENCIAL				
Tipo	**Activo**	**Frec.**	**Valor**	**D**	**I**	**C**	**A**	**T**
S	[S1] Acceso a la Red Corporativa	FM	1	8	8	5	8	0
	[S2] SAP	FM	1	10	8	10	10	0
	[S3]Internet	FM	1	8,1	5,6	7,2	9	0
	[S4] Correo Electrónico	FM	1	8,1	7	9	9	0
	[S5] Mitrol	FM	1	9	7	10	8	0
	[S6] Impresión	FA	10	10	4,2	6,4	9	0
	[S7] Movilidad/Optimiza	FA	10	8	9	8	10	0
	[S8] BI	FM	1	8,1	8	9	10	0
	[S9] Sistema de Nómina	FM	1	9	8	8	10	0
	[S10] Respaldos y Restauración	FM	1	8	7,2	8,1	8,1	0
SW	[SW1] Squarenet	FA	10	9	10	7,5	10	0
	[SW2] Mitrol	FA	10	9	10	7,5	8	0
	[SW3] Hipath Manager	FA	10	7	7	5,3	7	0
HW	[HOST1] Servidor de BDD	FB	0,1	10	5	10	0	0
	[HOST2] Servidor de Virtualización -PIA	FB	0,1	10	2,5	5	0	0
	[HOST3] Servidor de Virtualización - CAT	FB	0,1	10	2,5	5	0	0
	[HOST4] Servidor de Aplicación Mitrol	FB	0,1	9	5	10	0	0
	[HOST5] Servidor de Comunicaciones Mitrol	FB	0,1	10	5	8	0	0
	[HOST6] Servidor de Telefonía IP - CAT	FB	0,1	8	4	6	0	0
	[HOST7] Servidor Administración Telefonia	FB	0,1	4	2	4	0	0
	[HOST8] Servidor Telefonia IP - UIO	FB	0,1	8	4	6	0	0
	[HOST9] Servidor de Impresión	FB	0,1	9	2,5	5	0	0
	[VHOST1] Servidor AD Principal	FB	0,1	10	5	5	0	0
	[VHOST2] Servidor AD Secundario	FB	0,1	9	5	5	0	0
	[VHOST3] Servidor Aplicación SCCM	FB	0,1	5	4	5	0	0
	[VHOST4] Servidor Base SCCM	FB	0,1	5	4	5	0	0
	[VHOST5] Servidor Web Services	FB	0,1	9	4,5	6	0	0
	[VHOST6] Servidor AD Bogotá	FB	0,1	9	5	5	0	0
	[VHOST7] Nube Azure	FB	0,1	9	5	5	0	0
HW	[SWITCH1] SwitchCore - PIA	FM	1	10	2,3	7	0	0
	[SWITCH2] Switchs - PIA	FM	1	8	1,8	5	0	0
	[SWITCH3] SwitchCore - CAT	FM	1	10	2,3	7	0	0
	[SWITCH4] Switchs - CAT	FM	1	8	1,8	5	0	0
	[SWITCH5] Switchs - UIO	FM	1	8	1,8	5	0	0
	[SWITCH6] Switchs - GYE	FM	1	8	1,8	5	0	0
	[SWITCH7] Switchs - STO	FM	1	8	1,8	5	0	0
	[WAP1] AccessPoint - PIA	FM	1	6	1,3	3	0	0
	[WAP2] AccessPoint - CAT	FM	1	6	1,3	3	0	0
	[WAP3] AccessPoint - UIO	FM	1	6	1,3	3	0	0
	[WAP4] AccessPoint - GYE	FM	1	6	1,3	3	0	0
	[WAP5] AccessPoint - STO	FM	1	6	1,3	3	0	0
	[PABX1] Centralita Hipath 3800 - PIA	FM	1	8	2	6	0	0
	[PABX2] Centralita ExpansionBox Hipath 3800	FM	1	7	2	6	0	0
	[PABX3] Centralita Hipath 3800 - CAT	FM	1	8	2	6	0	0
	[PABX4] Base Celular Hypermedia	FM	1	9	2	6	0	0
	[PABX5] Enlace E1	FM	1	8	2	6	0	0

	[ROUTER1] Router Level3	FM	1	10	2,3	9	0	0
	[ROUTER2] Router Telconet	FM	1	9	2,3	9	0	0
	[FIREWALL1] Web Filter (Fierwall) Level3	FM	1	9	1,3	6	0	0
COM	[LAN1][LAN2][LAN3][LAN4][LAN5] Red Local	FB	0,1	8	2,1	2,5	6	0
	[WAN1][WAN2][WAN3][WAN4][WAN5] Enlaces	FB	0,1	10	3	5	9	0
	[WIFI1][WIFI2][WIFI3][WIFI4][WIFI5] Red Inalámbrica	FB	0,1	6	1,5	1,5	4	0
	[IEX1][IEX2][IEX3][IEX4][IEX5] Internet	FB	0,1	9	2,4	4	9	0
	[IPPHONE1][IPPHONE2][IPPHONE3] Telefonia IP	FB	0,1	8	2,4	3	6	0
Med	[NAS1][NAS2][NAS3][NAS4] Equipos de Respaldo	FB	0,1	10	7,5	10	0	0
AUX	[UPS1] UPS	FB	0,1	10	0	0	0	0
	[AC1] Aire Acondicionado	FB	0,1	9	0	0	0	0
	[CABLING1] Cableado LAN	FB	0,1	8	3,5	5	0	0
	[WIRE1] Cableado Eléctrico	FB	0,1	10	0	0	0	0
	[FIBER1] Fibra óptica	FB	0,1	9	0	0	0	0
	[FORNITURE1] Racks	FB	0,1	8	0	0	0	0
P	[OP1] Operadores	FB	0,1	0	0	0	0	0
	[ADM1] Jefe Sistemas	FB	0,1	0	0	0	0	0
	[COM1] Administrador infraestructura y Redes	FB	0,1	0	0	0	0	0
	[SEC1] Agente de Seguridades	FB	0,1	0	0	0	0	0
	[ADM2] Consultores Internos	FB	0,1	0	0	0	0	0
	[DES1] Analistas Programadores	FB	0,1	0	0	0	0	0
P	[UI1] Usuarios Internos	FB	0,1	0	0	0	0	0

ANEXO E

				Riesgo				
Tipo	**Activo**	**Frec.**	**Valor**	**D**	**I**	**C**	**A**	**T**
S	[S1] Acceso a la Red Corporativa	FM	1	8	8	5	8	0
	[S2] SAP	FM	1	10	8	10	10	0
	[S3]Internet	FM	1	8,1	5,6	7,2	9	0
	[S4] Correo Electrónico	FM	1	8,1	7	9	9	0
	[S5] Mitrol	FM	1	9	7	10	8	0
	[S6] Impresión	FA	10	100	42	64	90	0
	[S7] Movilidad/Optimiza	FA	10	80	72	72	80	0
	[S8] BI	FM	1	8,1	8	9	10	0
	[S9] Sistema de Nómina	FM	1	9	8	8	10	0
	[S10] Respaldos y Restauración	FM	1	8	7,2	8,1	8,1	0
SW	[SW1] Squarenet	FA	10	90	100	75	100	0
	[SW2] Mitrol	FA	10	90	100	75	80	0
	[SW3] Hipath Manager	FA	10	70	70	52,5	70	0
HW	[HOST1] Servidor de BDD	FB	0,1	1	0,5	1	0	0
	[HOST2] Servidor de Virtualización -PIA	FB	0,1	1	0,25	0,5	0	0
	[HOST3] Servidor de Virtualización - CAT	FB	0,1	1	0,25	0,5	0	0
	[HOST4] Servidor de Aplicación Mitrol	FB	0,1	0,9	0,5	1	0	0
	[HOST5] Servidor de Comunicaciones Mitrol	FB	0,1	1	0,5	0,8	0	0
	[HOST6] Servidor de Telefonía IP - CAT	FB	0,1	0,8	0,4	0,6	0	0
	[HOST7] Servidor Administración Telefonia	FB	0,1	0,4	0,2	0,4	0	0
	[HOST8] Servidor Telefonia IP - UIO	FB	0,1	0,8	0,4	0,6	0	0
	[HOST9] Servidor de Impresión	FB	0,1	0,9	0,25	0,5	0	0
	[VHOST1] Servidor AD Principal	FB	0,1	1	0,5	0,5	0	0
	[VHOST2] Servidor AD Secundario	FB	0,1	0,9	0,5	0,5	0	0
	[VHOST3] Servidor Aplicación SCCM	FB	0,1	0,5	0,4	0,5	0	0
	[VHOST4] Servidor Base SCCM	FB	0,1	0,5	0,4	0,5	0	0
	[VHOST5] Servidor Web Services	FB	0,1	0,9	0,45	0,6	0	0
	[VHOST6] Servidor AD Bogotá	FB	0,1	0,9	0,5	0,5	0	0
	[VHOST7] Nube Azure	FB	0,1	0,9	0,5	0,5	0	0
HW	[SWITCH1] SwitchCore - PIA	FM	1	10	2,25	7	0	0
	[SWITCH2] Switchs - PIA	FM	1	8	1,75	5	0	0
	[SWITCH3] SwitchCore - CAT	FM	1	10	2,25	7	0	0
	[SWITCH4] Switchs - CAT	FM	1	8	1,75	5	0	0
	[SWITCH5] Switchs - UIO	FM	1	8	1,75	5	0	0
	[SWITCH6] Switchs - GYE	FM	1	8	1,75	5	0	0
	[SWITCH7] Switchs - STO	FM	1	8	1,75	5	0	0
	[WAP1] AccessPoint - PIA	FM	1	6	1,25	3	0	0
	[WAP2] AccessPoint - CAT	FM	1	6	1,25	3	0	0
	[WAP3] AccessPoint - UIO	FM	1	6	1,25	3	0	0
	[WAP4] AccessPoint - GYE	FM	1	6	1,25	3	0	0
	[WAP5] AccessPoint - STO	FM	1	6	1,25	3	0	0
	[PABX1] Centralita Hipath 3800 - PIA	FM	1	8	2	6	0	0
	[PABX2] Centralita ExpansionBox Hipath 3800	FM	1	7	2	6	0	0
	[PABX3] Centralita Hipath 3800 - CAT	FM	1	8	2	6	0	0
	[PABX4] Base Celular Hypermedia	FM	1	9	2	6	0	0
	[PABX5] Enlace E1	FM	1	8	2	6	0	0

	[ROUTER1] Router Level3	FM	1	10	2,25	9	0	0
	[ROUTER2] Router Telconet	FM	1	9	2,25	9	0	0
	[FIREWALL1] Web Filter (Fierwall) Level3	FM	1	9	1,25	6	0	0
COM	[LAN1][LAN2][LAN3][LAN4][LAN5] Red Local	FB	0,1	0,8	0,21	0,25	0,6	0
	[WAN1][WAN2][WAN3][WAN4][WAN5] Enlaces	FB	0,1	1	0,3	0,5	0,9	0
	[WIFI1][WIFI2][WIFI3][WIFI4][WIFI5] Red Inalámbrica	FB	0,1	0,6	0,15	0,15	0,4	0
	[IEX1][IEX2][IEX3][IEX4][IEX5] Internet	FB	0,1	0,9	0,24	0,4	0,9	0
	[IPPHONE1][IPPHONE2][IPPHONE3] Telefonia IP	FB	0,1	0,8	0,24	0,3	0,6	0
Med	[NAS1][NAS2][NAS3][NAS4] Equipos de Respaldo	FB	0,1	1	0,75	1	0	0
AUX	[UPS1] UPS	FB	0,1	1	0	0	0	0
	[AC1] Aire Acondicionado	FB	0,1	0,9	0	0	0	0
	[CABLING1] Cableado LAN	FB	0,1	0,8	0,35	0,5	0	0
	[WIRE1] Cableado Eléctrico	FB	0,1	1	0	0	0	0
	[FIBER1] Fibra óptica	FB	0,1	0,9	0	0	0	0
	[FORNITURE1] Racks	FB	0,1	0,8	0	0	0	0
P	[OP1] Operadores	FB	0,1	0	0	0	0	0
	[ADM1] Jefe Sistemas	FB	0,1	0	0	0	0	0
	[COM1] Administrador infraestructura y Redes	FB	0,1	0	0	0	0	0
	[SEC1] Agente de Seguridades	FB	0,1	0	0	0	0	0
	[ADM2] Consultores Internos	FB	0,1	0	0	0	0	0
	[DES1] Analistas Programadores	FB	0,1	0	0	0	0	0
P	[UI1] Usuarios Internos	FB	0,1	0	0	0	0	0

ANEXO F

SALVAGUARDAS

CORTE DEL SUMINISTRO ELÉCTRICO

Objetivos	Evaluar el tiempo de suministro de energía eléctrica de respaldo y definir si es suficiente para la infraestructura instalada.
Descripción	Se realizará un mantenimiento preventivo del sistema de UPS que se tiene en las oficinas de Perú, en base al mantenimiento el proveedor emitirá un informe con el estado actual y sus recomendaciones, las mismas nos permitirán evaluar si el tiempo de energía de respaldo ante un eventual corte es suficiente o se necesita ampliar.
Beneficios	• Evitar daños a nivel de hardware y software. • Mantener la disponibilidad de los servicios de red e infraestructura.
Activos Involucrados	• PERDC01 (Controlador de Dominio) • PE_ROUTER_LIM (Router Level3)
Riesgo a Mitigar	• Corte del suministro eléctrico
Conclusión	Del informe técnico se resume que el tiempo de respaldo de energía disponible es de 5 horas, adicionalmente en base al tiempo de vida útil de las baterías se recomienda renovar las mismas para el año 2018.
Definición	Se propondrá la renovación de las baterías a José Antonio Hernandez

AVERÍA DE ORIGEN FÍSICO O LÓGICO

FALLO DE SERVICIOS DE COMUNICACIONES

Objetivos	Evaluar y determinar el tiempo de vida útil del equipo para conocer si se disponen de soporte por el fabricante o caso contrario proponer una solución ante un incidente.
Descripción	Se revisará la documentación oficial por parte del fabricante que nos permitirá conocer si el equipo dispone de soporte en el caso de presentarse cualquier eventualidad de hardware o software.
Beneficios	• Mantener la disponibilidad de los servicios de comunicaciones. • Proponer una recomendación para la renovación del equipo.
Activos Involucrados	• CO_ROUTER_YUM_TEL (Router de comunicaciones Colombia)
Riesgo a Mitigar	• Avería de origen físico o lógico • Fallo de servicios de comunicaciones
Conclusión	Después de revisar el documento oficial, la fecha de EOL de soporte para la serie 2800 (serie del equipo) terminó el 31 de Octubre del 2016, el equipo se vendió hasta el 01 de noviembre del 2011. Por lo que se recomienda identificar el siguiente modelo para adquirirlo en caso de un fallo del equipo y respaldar la configuración del mismo. El respaldo se encuentra en el sitio de Infraestructura TI en la ecunet. Enlace1_Documentación Enlace2_Documentación
Definición	Se debe plantear un proyecto de renovación para el siguiente año

ERRORES DEL ADMINISTRADOR

Objetivos	Analizar los permisos otorgados a los usuarios para el acceso a los servidores de optimiza y los roles que manejan en los mismos.
Descripción	Se validarán los usuarios con acceso a Optimiza con la ayuda del consultor de Movilidad y se documentarán los mismos.
Beneficios	• Llevar un control de acceso a los servidores en mención. • Controlar los permisos y privilegios en los servidores de optimiza.
Activos Involucrados	• OPTIMIZAAPP (Servidor de Aplicaciones) • OPTIMIZADB (Servidor de Base de Datos)
Riesgo a Mitigar	• Errores del Administrador
Conclusión	Se realiza la validación de los usuarios que necesitan conectarse por escritorio remoto al servidor de aplicaciones, estos usuarios tienen únicamente el permiso de “Conexión Remota” ya que el servidor se encuentra en el dominio y se aplican las mismas políticas, adicionalmente para la administración y gestión se colocó como administradores del equipo a los usuarios del proveedor de Optimiza (optimiza01 y optimiza02) y al consultor de movilidad (tchapal). El documento se encuentra en el sitio de Infraestructura TI en la ecunet.
Definición	Se llevará un control de usuarios con acceso en el documento publicado en la Ecunet

FALLO DE SERVICIOS DE COMUNICACIONES

Objetivos	Buscar un medio de respaldo de hardware que permita mantener la disponibilidad del equipo de comunicaciones Mitrol.
Descripción	Se solicitará al proveedor la cotización de una tarjeta de comunicaciones para el servidor correspondiente y se solicitará la aprobación para la adquisición.
Beneficios	• Disponer de un plan de contingencia ante una eventualidad en el servidor de comunicaciones Mitrol. • Mantener la disponibilidad del servicio.
Activos Involucrados	• MITE1X-PC (Servidor de Comunicaciones Mitrol)
Riesgo a Mitigar	• Fallo de servicios de comunicaciones.
Conclusión	El administrador de redes gestiona la cotización con el proveedor, sin embargo nos indican que las tarjetas como tal no son comercializables, si se quiere buscar una forma de respaldo incluiría todo el servidor de comunicaciones. El mail se sube al sitio de Infraestructura en la ecunet.
Definición	Dadas las circunstancias se traerá el servidor de comunicaciones de las oficinas de Colombia para tenerlo como backup. Esta actividad se la tratará en el mes de Diciembre.

AVERÍA DE ORIGEN FÍSICO O LÓGICO

Objetivos	Migrar el servidor de dominio a un servidor virtual a través de la plataforma Hyperv
Descripción	Se realizará la migración del equipo a una máquina virtual levantada en hyperv, el equipo físico dispondrá de mejores prestaciones.
Beneficios	• Mantener la disponibilidad del servicio. • Mejorar el rendimiento del controlador de dominio.
Activos Involucrados	• PERDC01 (Controlador de Dominio de Perú)
Riesgo a Mitigar	• Avería de origen físico o lógico.
Conclusión	Se realizó la migración del equipo, se instalaron las aplicaciones adicionales y se genera un snapshot del mismo, al ser un Controlador de Dominio de lectura no se realizan cambios constantes.
Definición	Se exporta el respaldo del Máquina Virtual al NAS de Perú.

DESTRUCCIÓN DE LA INFORMACIÓN

Objetivos	Evaluar en conjunto con el proveedor el plan de respaldos de estos equipos
Descripción	Se evaluará con el proveedor el plan de respaldos de los servidores de Mitrol ante la materialización de alguna amenaza.
Beneficios	• Mantener la disponibilidad del servicio.
Activos Involucrados	• COLMIT01 • COLMITBD01
Riesgo a Mitigar	• Destrucción de la información.
Conclusión	Debido a la reestructuración realizada en Colombia se prescinde de estos equipos.
Definición	Se genera un respaldo de la BDD de mitrol y se guarda la misma en el equipo NASYUMBO01.

ERUPCIÓN VOLCÁNICA

Objetivos	Proteger los equipos tecnológicos ante repercusiones de una posible erupción.
Descripción	Se levantará un procedimiento de contingencia ante una eventual erupción volcánica al estar dentro de una zona de afectación.
Beneficios	• Protección de Equipos tecnológicos.
Activos Involucrados	• EC_SW_COREPIA • EC_ROUTER_PIA • ECUORABD01
Riesgo a Mitigar	• Erupción Volcánica.
Conclusión	De acuerdo al Plan de Continuidad de la empresa se toman en consideración los pasos a seguir de acuerdo al nivel de alerta que se presente.

Definición	*Alerta Amarilla*
	• Mantenerse informados de la situación actual de emergencia, que se emitirá por los medios de comunicación de Plasticaucho Industrial.
	• Disponer de protectores para componentes tecnológicos que permitan asegurar las comunicaciones.
	• Validar que los respaldos de servidores se estén ejecutando correctamente de acuerdo a los últimos logs de errores.
	
	Alerta Naranja
	• *Detener los sistemas de ventilación y enfriamiento de las áreas dando prioridad a los Centros de Procesamiento de Datos previa notificación del comité de emergencia.*
	• *Paralizar las actividades de acuerdo a las indicaciones del comité de emergencia.*
	  ○ *Se realizará el apagado de los servidores virtuales y físicos y se desconectaran las tomas eléctricas.*
	  ○ *Se desconectaran los dispositivos de comunicaciones tales como switchs, routers y centrales telefónicas.*

	• *Proteger equipos internos y externos según su criticidad.* ○ *Se colocarán los protectores en los equipos de acuerdo a su criticidad.* *Alerta Roja* La actividad del volcán es recurrente, la erupción se dará en corto plazo. Es momento de evacuar a los refugios temporales dispuestos por las autoridades. *Restablecimiento de Actividades* • Se esperara que las áreas correspondientes realicen la limpieza externa a interna y se validará previo al encendido de los equipos. • Se encenderán los equipos de redes y comunicaciones. • Se procederá al encendido de los servidores físicos y posteriormente los virtuales. • Se estabilizará cualquier eventualidad que afecte la disponibilidad de los servicios tecnológicos.

RESPALDOS

Objetivos	Elaborar un respaldo de la configuración ante una posible erupción volcánica.
Descripción	Precautelar las configuraciones que tiene el switch CORE de la red en PIA.
Beneficios	• Disponer de un respaldo de la configuración.
Activos Involucrados	• EC_SW_COREPIA
Riesgo a Mitigar	• Erupción Volcánica.
Conclusión	Es necesario disponer de un respaldo de la configuración pues se dispone de un swtich de backup ante un posible incidente.
Definición	Se genera el backup y se sube el mismo a la Ecunet.

ACCESO NO AUTORIZADO

Objetivos	Proteger los equipos tecnológicos identificados como críticos ante el acceso no autorizado a los mismos.
Descripción	Definir el alcance del Firewall que manejan los equipos a través del Sistema Operativo.
Beneficios	• Precautelar la autenticidad de la información. • Definir políticas de accesos.
Activos Involucrados	• OPTIMIZAAPP • OPTIMIZADB • ECUORABD01
Riesgo a Mitigar	• Acceso no autorizado
Conclusión	Los equipos OPTIMIZAAPP y OPTIMIZADB se encuentran hosteados en Level3 quienes administran un FW perimetral tanto para la red interna como hacia internet por lo que no es necesario levantar el FW del S.O. El equipo ECUORABD01 se encuentra en la red interna sin un FW perimetral por lo que es necesario levantar el FW propio del sistema.
Definición	Se investiga el funcionamiento del Firewall de Seguridad Avanzada de Windows, se levantan reglas de entrada y de salida. Se procede a levantar el FW. Adicionalmente se ejecuta un análisis de vulnerabilidades en los equipos tanto de Optimiza como al servidor interno de BDD. Los reportes se adjuntan en la Ecunet.

SUPLANTACIÓN DE IDENTIDAD DEL USUARIO

Objetivos	Precautelar operaciones fraudulentas en los clientes del sistema Mitrol.
Descripción	Revisar las políticas de contraseñas del sistema Mitrol para seguir las buenas prácticas.
Beneficios	• Evitar el robo de contraseña. • Validar la autenticidad en el sistema.
Activos Involucrados	• ECUMITROL01 • COLMIT01 • COLMITBD01
Riesgo a Mitigar	• Suplantación de identidad del usuario.
Conclusión	Los equipos de Mitrol en las oficinas de Colombia se darán de baja pues ya no se lleva el proceso de Contact Center. En Ecuador se buscará una alternativa pues no se dispone de un módulo de seguridad.
Definición	Se acuerda con Aracelly para realizar el cambio en la consola de Administración y cada usuario colocará su contraseña, en el caso de que se necesite reiniciar la misma el proceso será gestionado por Aracelly.

ERRORES DEL ADMINISTRADOR

Objetivos	Analizar el nivel de servicio y los incidentes presentados con el proveedor respecto al manejo del Firewall Perimetral.
Descripción	Precautelar la correcta gestión del Firewall Perimetral.
Beneficios	• Evitar incidentes por la incorrecta administración.
Activos Involucrados	• CO_FW_LEVEL3
Riesgo a Mitigar	• Errores del Administrador
Conclusión	Se revisa el acuerdo de nivel de servicio (SLA) presentado por el proveedor y debido a la gestión que se lleva se transfiere el riesgo.
Definición	Se transfiere el riesgo al proveedor.

Objetivos	Elaborar un procedimiento gestión de acceso a proveedores a la infraestructura tecnológica
Descripción	Definir una correcta gestión para que el acceso no sea permanente y de esta manera disminuir el riesgo.
Beneficios	• Adecuada gestión del acceso a través de VPN.
Activos Involucrados	• COLMIT01 • COLMITBD01 • ECUMITBD01
Riesgo a Mitigar	• Errores del Administrador.
Conclusión	Se determina que se habilitará el acceso bajo demanda y se formalizará el acta de entrega de usuario con el proveedor.
Definición	Se comunicó a los usuarios involucrados el procedimiento.

DIFUSIÓN DE SOFTWARE DAÑINO

Objetivos	Precautelar la difusión de Software dañino en los equipos NAS
Descripción	Buscar una solución antimalware para analizar los archivos que se encuentran en los equipos NAS de la empresa a nivel corporativo.
Beneficios	• Prevenir el contagio y difusión de software dañino.
Activos Involucrados	• NASPIA01 • NASCAT01 • NASYUMBO01
Riesgo a Mitigar	• Difusión de Software dañino.
Conclusión	De acuerdo a la información oficial de Synology existe un paquete complementario que ayuda a prevenir la expansión de software malicioso.
Definición	Se procede a instalar el paquete de Antivirus Essential y se programan tareas periódicas para los análisis correspondientes.