

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

**Plan de gestión de seguridad de la información para la empresa
ALPHA TECHNOLOGIES CIA. LTDA con la norma ISO/IEC
27001:2011.**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN**

PATRICIO KEVIN MENDOZA PUERTAS

patricio.mendoza@epn.edu.ec

DARIO ALEXANDER NARANJO MORENO

dario.naranjo@epn.edu.ec

DIRECTOR: Msc. RODRIGO CHANCUSIG.

rodrigo.chancusig@epn.edu.ec

CODIRECTOR: MSc. CARLOS MONTENEGRO.

carlos.montenegro@epn.edu.ec

Quito, 11 de marzo de 2020

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue desarrollado por Patricio Kevin Mendoza Puertas y Darío Alexander Naranjo Moreno, bajo nuestra dirección y supervisión, en la facultad de ingeniería de sistemas en la Escuela Politécnica Nacional.



MSc. Rodrigo Chancusig.
DIRECTOR DE PROYECTO

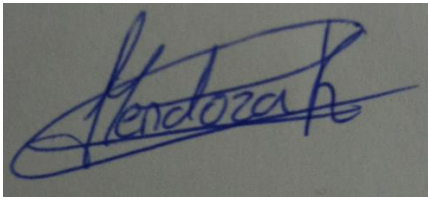


MSc. Carlos Montenegro.
CODIRECTOR DE PROYECTO

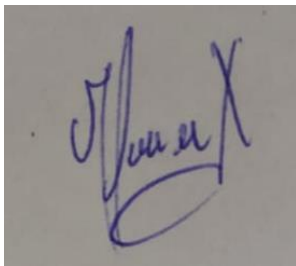
DECLARACIÓN

Nosotros, Patricio Kevin Mendoza Puertas y Darío Alexander Naranjo Moreno, declaramos bajo juramento que el trabajo de titulación es de nuestra autoría; el cual no ha sido previamente presentado para ningún grado; y que las referencias bibliográficas fueron consultadas para incluirlas en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo de titulación, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Patricio Kevin Mendoza Puertas



Darío Alexander Naranjo Moreno

DEDICATORIA

A mi familia.

El presente proyecto de titulación va dedicado a las tres personas que más amo y admiro en mi vida, mi madre, mi padre y mi hermano; ya que su apoyo a lo largo de esta etapa fue fundamental para que pueda lograrlo de mejor manera y a mi familia en general por siempre creer en mí.

A mis amigos.

Va dedicado también para todos mis amigos que me acompañaron en este largo camino.

Patricio Kevin Mendoza Puertas

AGRADECIMIENTO

Agradezco primeramente a Dios por permitirme vivir esta experiencia y más que nada poder lograrla.

Quiero agradecer a las tres personas más importantes en mi vida, a mi madre (Isabel Puertas) a mi padre (Patricio Mendoza) y a mi hermano (Steven Mendoza), quienes siempre estuvieron conmigo apoyándome, dándome consejos, asegurándose que nunca me falte nada, gracias por siempre confiar en mí, yo soy quien soy gracias a ustedes y nunca voy a defraudarlos siempre quiero que estén orgullosos de mí y trabajare duro por ustedes y por mí, ustedes son mi vida los amo mucho; quiero agradecer a mi tía Norma Mendoza y a Carmen Cano por siempre formar parte de mi familia ya que siempre hemos vivido juntos los 5.

A mis amigos:

Agradezco a mis amigos del conjunto que son como mis hermanos, ya que llevamos casi 15 años de amistad y sé que esta amistad es para siempre, aunque cada uno tome caminos diferentes, gracias por darme la mejor infancia de la vida y gracias por formar parte de mi vida ahora que somos adultos, gracias, Gianni Argüello, Bryan Silva, David Esparza, Alex Osorio y Andrés Oñate.

Agradezco también a todos mis amigos que conocí en este ciclo de la universidad ya que con ustedes viví toda esta etapa, les agradezco todos los momentos vividos, los momentos de estudio, de estrés, de diversión y todas las aventuras que tuvimos, y gracias por su ayuda cuando lo necesite, gracias Paola Benítez, Wilmer Guevara, Andrés Samaniego, Julia Recalde, Jonathan Pachacama, Cristian Remache, Evelyn Regalado y a todas las personas que conocí y aportaron un granito de arena en esta etapa de mi vida, tuve la suerte de que la vida me de amigos como ustedes.

Agradezco a los ingenieros Rodrigo Chancusig y Carlos Montenegro por su guía en esta etapa de la universidad, gracias por los consejos y ayuda en este proyecto de titulación, agradezco también a todos los ingenieros quienes compartieron sus conocimientos para que pueda llegar a ser la persona que soy el día de hoy.

Agradezco a la universidad Escuela Politécnica Nacional por convertirme en el profesional que soy ahora.

Patricio Kevin Mendoza Puertas

DEDICATORIA

A mis Padres.

Este trabajo de titulación está dedicado a Margoth y Hugo, los cuales han sido la principal fuente de apoyo y motivación para poder llegar hasta este punto de mi vida, siempre creyendo en mí y brindándome su amor.

A mis hermanos.

Fernando, Vanessa y Danny, que siempre han sabido entenderme y han estado a mi lado.

Darío Alexander Naranjo Moreno

AGRADECIMIENTO

Agradezco principalmente a Dios, por permitirme llegar a culminar esta etapa de mi vida y le agradezco principalmente por permitirme compartir este momento con mi familia.

Mi familia ha sido la motivación y la fuerza que eh necesitado a lo largo de mi vida no solo para alcanzar esta meta, sino para todo lo que logrado en mi vida. Mis padres con su apoyo incondicional en todo momento, con su esfuerzo y con su cariño. Mis hermanos estando conmigo y creyendo en mí. Agradezco que puedan compartir conmigo este momento, y agradezco saber que siempre cuento con ustedes en todo momento.

Agradezco a las personas que he conocido a lo largo de esta etapa de mi vida, personas con las he compartido muchos gratos momentos, a lo largo de la universidad con las que nos hemos apoyado mutuamente para salir adelante. Gracias por permitirme formar parte de sus grupos y por permitirme contar su aprecio.

Y agradezco a la vida por permitirme conocer a una persona muy especial en esta etapa, a la cual llegue a admirar por ser la mejor persona que he conocido, de la cual aprendí muchas cosas y con la que pase muchos momentos felices a su lado siendo su amigo.

Finalmente quiero agradecer por el apoyo brindado, por sus consejos, por su guía a los ingenieros Rodrigo Chancusig y Carlos Montenegro, sin el cual este trabajo no se podría haber realizado.

Y la Escuela Politécnica Nacional y mi Facultad de Sistemas que es el lugar donde comienza y culmina este momento de vida y donde viví muchas experiencias que tengo como lecciones de vida.

Darío Alexander Naranjo Moreno

ÍNDICE DE CONTENIDO

DECLARACIÓN	II
DEDICATORIA	III
AGRADECIMIENTO	IV
DEDICATORIA	V
AGRADECIMIENTO	VI
ÍNDICE DE CONTENIDO	VII
RESUMEN	X
ABSTRACT	XI
1. INTRODUCCIÓN	1
1.1. Planteamiento de Problema	1
1.2. Objetivos	1
1.2.1. Objetivo General	1
1.2.2. Objetivos Específicos	2
1.3. Alcance	2
1.4. Reconocimiento de empresa	2
1.4.1. Historia	2
1.4.2. Plan Estratégico	2
1.4.2.1. Misión	2
1.4.2.2. Visión	3
1.4.2.3. Valores	3
1.4.2.4. Servicios y productos	3
1.4.3. Estructura organizacional de Alphatechnologies	4
1.4.3.1. Organigrama	4
1.4.4. Área de Tecnología (TIC)	7
1.4.4.1. Recurso humano	7
1.4.4.2. Componentes del Área de Tecnología	7
1.4.4.2.1. Aplicaciones de Software	8
1.4.4.2.2. Servidores	9
1.5. Uso de estándar y metodologías para la evaluación y gestión de riesgos 10	
1.5.1. Norma NTE INEN-ISO/IEC 27001:2011	10
1.5.2. Metodologías	10
1.5.2.1. RISK IT	11
1.5.2.2. OCTAVE	11
1.5.2.3. NIST 800-30	11

1.5.2.4.	MAGERIT	12
1.5.3.	Uso de la metodología Magerit.	12
1.6.	Situación actual de la seguridad de la información en la empresa Alpha Technologies CIA. LTDA.	13
1.6.1.	Análisis de la situación actual	13
1.6.1.1.	Resultados de las medidas de defensa	16
1.6.2.	Estado de cumplimiento actual	21
2.	APLICACIÓN DE LA METODOLOGÍA	35
2.1.	Análisis y evaluación de riesgos	35
2.2.	Pasos para la evaluación de riesgos según la metodología Magerit	36
2.2.1.	Caracterización de los activos	36
2.2.2.	Identificación de amenazas.	36
2.2.3.	Reconocimiento de vulnerabilidades.	37
2.2.4.	Análisis del riesgo	37
2.2.4.1.	Valoración de la probabilidad	37
2.2.4.2.	Valoración del impacto	38
2.2.4.3.	Determinación del riesgo	39
2.2.5.	Plan de tratamiento de Riesgos.	40
2.2.5.1.	Eficacia de la protección	41
2.3.	Evaluación de riesgos según la metodología MAGERIT	42
2.3.1.	Caracterización de los activos	42
2.3.2.	Identificación de amenazas.	42
2.3.3.	Reconocimiento de vulnerabilidades.	44
2.3.4.	Análisis del riesgo.	52
2.3.5.	Análisis de Salvaguardias	61
2.3.5.1.	Recomendación de controles	62
2.3.5.2.	Evaluación de riesgo residual	65
2.3.5.3.	Declaración de aplicabilidad	68
3.	RESULTADOS Y DISCUSIÓN	68
3.1.	Plan de Gestión de Seguridad de la Información	68
3.2.	Alcance y Limites de SGSI	70
3.3.	Elaboración del Plan de Gestión de Seguridad de la Información.	70
3.4.	Guía de Implementación	74
3.5.	Aplicabilidad de la propuesta	76
4.	CONCLUSIONES Y RECOMENDACIONES	78
4.1.	Conclusiones	78
4.2.	Recomendaciones	78
5.	BIBLIOGRAFÍA	79

ANEXOS	80
---------------	-----------

RESUMEN

En la actualidad, la empresa ALPHA TECHNOLOGIES CIA. LTDA no cuenta con un plan de Gestión de la Seguridad de la Información. Para lo cual se plantea el presente proyecto de titulación, el cual consta de cuatro partes:

Introducción: La primera sección definirá el planteamiento del problema, la segunda define los objetivos del proyecto, la tercera define el alcance del proyecto, la cuarta evalúa a la empresa, enfocado al área de tecnología, la quinta habla de las metodologías para el análisis y gestión de riesgos, y la sexta considera el diagnóstico de la situación actual de la empresa con las herramientas Check List y MSAT.

Aplicación de la Metodología: La primera sección trata sobre el plan de acción que se ejecuta para el análisis de riesgos, la segunda describe cada uno de los pasos de la metodología Magerit, y la tercera muestra la ejecución del análisis de riesgos, obteniendo como resultado la matriz de riesgos, logrando definir el plan de tratamiento para seleccionar los controles.

Resultados y Discusión: La primera sección muestra lo que es un SGSI, la segunda define el alcance y límites del plan de Gestión de la Seguridad de la información, la tercera muestra los pasos para la elaboración del plan de Gestión de Seguridad de la Información, la cuarta plantea una guía de implementación, y finalmente en la quinta muestra la implementación.

Conclusiones y Recomendaciones: contiene las conclusiones y recomendaciones obtenidas, en donde se destacan los puntos más importantes de todo el plan de Gestión de la Seguridad de la Información.

Palabras clave: Seguridad de la información, metodología Magerit, riesgos, herramientas, controles

ABSTRACT

Currently, the company ALPHA TECHNOLOGIES CIA. LTDA doesn't have an Information Security Management plan. For which the present project of qualification is proposed, which consists of four parts:

Introduction: The first section will define the approach of the, the second defines the objectives of the project, the third defines the scope of the degree project, the fourth evaluates the company, focused in more detail in the area of Information Technology, the fifth speaks of the methodologies for the analysis and risk management in an ISMS. Finally, the sixth considers the diagnosis of the current situation of the company together with the Check List and MSAT tools.

Application of the Methodology: The first section deals with the action plan that is executed for the risk analysis, the second describes each of the steps to be followed according to the Magerit methodology and the third is the execution of the risk analysis, where with the help of tools such as Nessus, Nmap and the check list itself identify the possible threats and vulnerabilities that critical assets are affected, obtaining as a result the risk matrix, managing to define the treatment plan to select the controls, where the security criteria of Magerit are taken into account to finally show the results obtained in the risk assessment report.

Results and Discussion: The first section shows what is an Information Security Management System, the second is where the scope and limits of the Information Security Management, the third shows the steps that must be taken for the preparation of the Information Security Management plan, the fourth section presents an implementation guide for carry out if the heads of the technology area of the company accept the execution of this plan, and finally in the fifth section the implementation of the proposal is made comparing the status of current compliance and the status of expected compliance.

Conclusions and Recommendations: it contains the conclusions and recommendations obtained, which highlights the most important points of the entire Information Security Management plan that must be taken into account within the company.

Keywords: Information security, Magerit methodology, risks, tools, controls.

1. INTRODUCCIÓN

1.1. Planteamiento de Problema

La información es un recurso vital para toda organización, y el buen uso de ésta puede significar la diferencia entre el éxito o el fracaso de la misma. El éxito de una organización ya no depende sólo de la manera en que cada persona maneja sus recursos materiales, sino que es más importante el buen aprovechamiento de los activos intangibles [1].

La seguridad de la información tiene como pilares básicos la integridad, la disponibilidad, la confidencialidad y la auditoria, en todo sistema informático. Para las empresas dicha seguridad es muy importante, por eso en el mercado existen diferentes soluciones para un mantenimiento informático que asegure la preparación de los sistemas ante posibles eventualidades que puedan afectar al crecimiento de una empresa. Se cuentan con Sistemas de Gestión de Seguridad de la Información (SGSI), los cuales incluyen diferentes temas como políticas de seguridad, aseguramiento de los recursos empresariales o la planificación de la seguridad, y se compone de tres procesos diferenciados: Planificación, Implementación y la Verificación con actualización [2].

Actualmente la empresa ALPHA TECHNOLOGIES CIA. LTDA. a pesar de ofrecer servicios y productos relacionados a seguridad informática, no cuenta con una guía para la gestión de la seguridad de la misma [3], lo cual genera por un lado el desconocimiento de los riesgos de la seguridad de la información y las posibles consecuencias que estos riesgos pueden generar, por ello, el presente trabajo de titulación propone “Diseñar un Plan de Gestión de Seguridad de la Información para la empresa ALPHA TECHNOLOGIES CIA. LTDA. basando en la serie de estándares ISO/IEC 27000, mismo que permitirá a la entidad tener definido políticas para la seguridad de la información, brindando la oportunidad de comenzar el proceso para certificaciones internacionales que den a la empresa un mayor prestigio [4] [5].

1.2. Objetivos

1.2.1. Objetivo General

Desarrollar un Plan de Gestión de Seguridad de la Información para el área de Tecnologías de la Información en la empresa ALPHA TECHNOLOGIES CIA. LTDA.

1.2.2. Objetivos Específicos

- Analizar la situación actual de la Empresa Alpha Technologies CIA. LTDA para caracterizar el problema de la falta de gestión en la seguridad de la información.
- Identificar los activos críticos de información, sus amenazas y vulnerabilidades estableciendo métricas de análisis en base a la metodología escogida.
- Diseñar un plan de seguridad de la información para los activos críticos de la Empresa Alpha Technologies CIA. LTDA con la documentación necesaria en base al análisis realizado.

1.3. Alcance

El proyecto de titulación tiene como objetivo inicial, conocer las deficiencias que se presentan en la empresa actualmente en relación a la seguridad de la información, para lo cual se realizarán entrevistas, revisión de documentos y/o información proporcionadas por la empresa, usar una metodología que permita determinar los riesgos presentados, conocer el estado actual de la seguridad en base a la norma NTE INEN-ISO/IEC 27001:2011; seguidamente, con los resultados obtenidos se identificará los controles de seguridad adecuados y que sean acordes a las necesidades de la empresa. Finalmente se diseñará el plan del sistema de gestión de la seguridad de la información (SGSI), estableciendo una serie de actividades a seguir por la empresa, cabe recalcar que la implementación de dicho plan no será parte del presente proyecto de titulación.

1.4. Reconocimiento de empresa

1.4.1. Historia

Alpha Technologies CIA. LTDA es una empresa ecuatoriana de seguridad informática establecida en Quito en el año 2001, especializada en la seguridad de datos, seguridad web y medios digitales. Sus productos y servicios son parte del día a día del trabajo de importantes entidades bancarias, comerciales y estatales del País. Es Partner Regional Certificado de GlobalSign y distribuidores autorizados Zimbra y McAfee [6].

1.4.2. Plan Estratégico

1.4.2.1. Misión

“Brindar apoyo constante a nuestros clientes en el ámbito de la seguridad informática, a través de nuestros productos brindando soluciones inmediatas”.

1.4.2.2. Visión

“Ser la empresa líder en seguridad informática, reconocida por nuestros clientes por medio de nuestros servicios de calidad e innovación”.

1.4.2.3. Valores

La Empresa Alpha Technologies CIA. LTDA promueve los siguientes valores:

- Honestidad
- Responsabilidad
- Integridad
- Compromiso
- Solidaridad
- Trabajo en Equipo
- Excelencia y calidad
- Respeto.

1.4.2.4. Servicios y productos

La Alpha Technologies CIA. LTDA. describe los servicios y productos de Alpha Technologies CIA. LTDA.

Servicios seguridad informática	
AT Firewall	Evita los ataques externos con una solución integral de seguridad perimetral. Junto al correcto criterio de nuestros expertos aplicarán políticas correctas para la prevención de ataques a sus sistemas.
AT Proxy	Controla la navegación y optimiza tus recursos. Solución corporativa para administrar los recursos de navegación junto con un filtro de contenido inteligente, se integra a las necesidades de toda corporación. Controla y filtra grandes cantidades de correo basura.
Mail Inspector	Usa técnicas automáticas de avanzadas en la filtración de correo y su administración es sencilla. Es compatible con cualquier servidor de correo Exchange, Lotus, Zimbra, etc.

AT Mailing	<p>Envíe correos a grandes bases de datos sin caer en listas negras.</p> <p>Arquitectura de envío de correo masivo con capacidad de más de UN MILLÓN de correos diarios.</p> <p>Ofrezca tickets de navegación a sus clientes e invitados.</p>
AT Hotspot	<p>Con AT HOTSPOT creamos una zona segura de acceso inalámbrico en tu corporación de acuerdo a sus necesidades.</p> <p>La solución óptima para el balanceo de carga.</p>
AT Logic	<p>Una arquitectura de clúster que cumple con las funciones deseadas balanceo de carga, alto rendimiento y alta disponibilidad.</p>

1.4.3. Estructura organizacional de Alphatechnologies

1.4.3.1. Organigrama

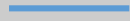
Alphatechnologies cuenta con una estructura organizacional de 4 niveles jerárquicos, los cuales han sido establecidos de acuerdo a las necesidades y al personal con el que cuenta la organización, tanto el área de tecnología como el área administrativa se encuentran en el mismo nivel jerárquico en comunicación directa para una mejor comunicación y realización de procesos, y estas dos áreas a su vez poseen una comunicación directa con la alta gerencia para un compromiso mayor por todas las partes.

A continuación, se muestra la simbología usada para el entendimiento del organigrama de Alpha technologies CIA.LTDA.





DEPARTAMENTOS DE APOYO Y GESTIÓN



COMUNICACIÓN DIRECTA



COMUNICACIÓN CONSTANTE

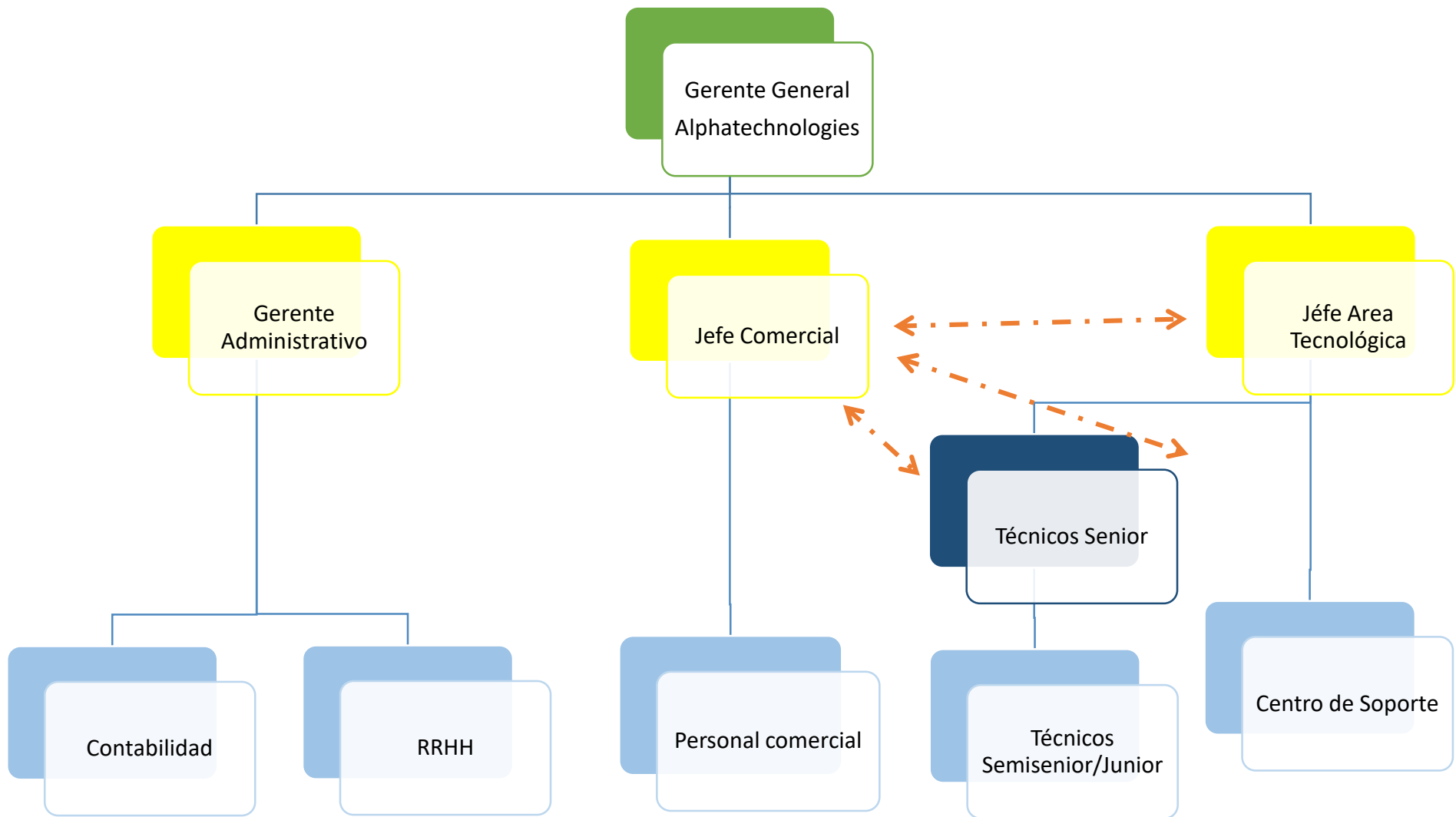


Figura 1.1: Organigrama empresa Alpha Technologies CIA. LTDA

1.4.4. Área de Tecnología (TIC)

El departamento de tecnología de Alpha Technologies CIA. LTDA es el encargado de brindar los servicios TIC para toda la empresa, gestionando de manera eficiente todos los productos a sus clientes.

1.4.4.1. Recurso humano

El personal que actualmente cuenta la empresa dentro del área de tecnología se muestra en la **¡Error! No se encuentra el origen de la referencia.2.**

Nombre	Cargo	Funciones	Profesión
Jhonatan Benalcázar	Gerente de soporte técnico	Responsable de la organización, administración y supervisión del área técnica.	Ingeniero de Sistemas
Pablo Tamayo	Técnico Senior de soporte/Desarrollador	Soporte especializado en sistemas y servicios Linux y Windows. Especialista en seguridad digital.	Ingeniero de Sistemas
Cristian Echeverria	Técnico Senior	Mantenimiento y soporte a las aplicaciones de la entidad y clientes.	Ingeniero de Sistemas
Omar García	Centro de soporte	Responsable de realizar el levantamiento de información para el respectivo soporte solicitado.	Tecnólogo
Dario Naranjo	Técnico	Mantenimiento y soporte a las aplicaciones de la entidad y clientes.	Egresado

Fuente: Elaborado por los autores con información proporcionada por el Jefe del área de Tecnología.

1.4.4.2. Componentes del Área de Tecnología

En la actualidad, la empresa Alpha Technologies CIA. LTDA cuenta con 12 computadores y/o laptops distribuidas en todas las instalaciones de la organización (2 pisos), que cuentan con garantías y sus respectivos seguros. En cuanto a los sistemas operativos instalados se tiene: CentOS6, CentOS7, CentOS8, Windows 7, y Windows 10 Pro, Windows Server 2012 R2, todos con sus respectivas licencias.

1.4.4.2.1. Aplicaciones de Software

Las aplicaciones de software son utilizadas para el monitoreo y control de las actividades de los usuarios, también sirven para facilitar la gestión de los procesos que se siguen en la organización. A continuación, se presentan con detalle las aplicaciones alojadas en los servidores analizados.

AT-Firewall

Software para la seguridad perimetral de la organización, en donde se administran reglas de accesos y bloqueos de navegación de los usuarios, así como se puede observar en tiempo real la cantidad de banda ancha usada por los usuarios.

	IP	Sistema Operativo	Características
AT-Firewall	192.168.X.X	CentOS Linux 7.6.1810	Servidor Procesador: Intel(R) Xeon(R) CPU E3-1225 v5 @ 3.30GHz X4 RAM: 8 GB 64 bits Disco: 1T

AT-Proxy

Software complementario al Firewall para el monitoreo y control de la navegación de los usuarios, en base a repositorios, servicios y puertos configurados. Este software se integra con el directorio activo de la organización para un control más transparente.

	IP	Sistema Operativo	Características
AT-Proxy	192.168.X.X	CentOS Linux 7.6.1810	Máquina virtual Procesador: Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz X4 RAM: 8 GB 64 bits Disco: 100 GB

CRM-Alphaside

Software para la gestión de los procesos necesarios en la organización. Permite entre otras cosas registrar las actividades del personal técnico de la atención dada a los clientes, para su posterior procesamiento por el área Administrativa.

	IP	Sistema Operativo	Características
CRM- Alphaside	192.168.X.X	CentOS release 6.10	Máquina virtual
			Procesador: Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz X4
			RAM: 4 GB
			64 bits
			Disco: 150 GB

1.4.4.2.2. Servidores

Además de los servidores en los cuales se alojan los aplicativos mencionados anteriormente, se tienen también servidores adicionales para las actividades que se detallaran a continuación.

No.	Servidor	IP	Función	Sistema Operativo	Características
1	Directorio Activo	192.168.X.X	Gestionar la creación de usuarios para los empleados de la organización, Servidor DNS, DHCP	Microsoft Windows Server 2012 R2	Máquina Virtual Procesador: Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz X4 64 bits RAM: 12GB Disco: 100GB
2	Certificados VPN	192.168.X.X	Creación y almacenamiento de certificados para los usuarios de conexión VPN	Red Hat Linux release 9 (Shrike)	Máquina virtual Procesador: Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz X1 RAM: 6GB 64 bits

					Disco: 4GB
3	Pivote de conexión	192.168.X.X	Punto de acceso seguro para la conexión a los clientes	CentOS Linux 7.6.1810	Máquina virtual Procesador: Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz X1 RAM: 2GB 64 bits Disco: 20GB

1.5. Uso de estándar y metodologías para la evaluación y gestión de riesgos

La información es el conjunto de datos organizados, y a la vez se consideran como el activo más importante en las entidades, independientemente de cómo se la guarde o transmita (almacenada de manera física o electrónica, imágenes, correos, fax, entre otras). Hablar sobre seguridad de la información, involucra los pilares confidencialidad, disponibilidad e integridad; de la misma manera, se establecen procesos documentados desde un enfoque de riesgo empresarial, lo cual se identifica como un SGSI [4].

1.5.1. Norma NTE INEN-ISO/IEC 27001:2011

La ISO/IEC 27001 es un estándar internacional para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información, SGSI.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información, que permite a la organización el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar de manera eficiente el acceso a la información, minimizando los riesgos de seguridad [6].

1.5.2. Metodologías.

Existen varias metodologías usadas para el análisis de riesgo y que se encuentran enmarcadas en la norma ISO 27001, para la implementación del SGSI, las cuales se detallan a continuación.

1.5.2.1. RISK IT.

La metodología Risk IT (Publicada por ISACA) brinda una visión completa y única de riesgos que están relacionados con la tecnología de la información, que pueden provocar a las entidades pérdidas considerables en ingresos y oportunidades. Los riesgos son inherentes a todas las entidades, pero se debe mantener cierto control para evitar la destrucción del valor y asegurar que las oportunidades para la creación de valores no se pierdan. Esta metodología trata de ayudar en todos los niveles gerenciales en la administración de riesgos para así poder tener los mayores beneficios [7].

1.5.2.2. OCTAVE.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una de las metodologías de análisis de riesgos que más se usan en las empresas. Esta metodología se centra en describir un conjunto de criterios para poder desarrollar métodos que se asocien a guías específicas de administración y evaluación de riesgos. Octave se encarga de evaluar los riesgos de seguridad de la información y propone un plan para poder mitigarlos dentro de una entidad. Los objetivos de OCTAVE se enfocan básicamente en concientizar a la entidad que la seguridad informática no es un asunto solamente técnico, y presenta los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos. Esta metodología realiza algunos procesos, en el cual inicia con una evaluación de los activos relacionados con la información, para después asignarles un valor estimado para la entidad y de esta manera, Octave analiza y estudia la infraestructura de la información, definiendo así los elementos más importantes para la entidad [8].

1.5.2.3. NIST 800-30.

NIST SP 800 – 30 (National Institute of Standards and Technology) es una Guía de gestión de riesgo para sistemas de tecnología de la información. Es una guía que brinda un conjunto de actividades y recomendaciones para una eficiente gestión de riesgos; sin embargo, no es suficiente, pues se necesita del apoyo de toda la entidad para que los objetivos y alcance de la gestión de riesgos concluyan de manera exitosa. La Metodología NIST SP 800-30 está compuesta por 9 pasos básicos para el análisis de

riesgo, los cuales son: Caracterización del sistema, identificación de amenaza, identificación de vulnerabilidades, control de análisis, determinación del riesgo, análisis de impacto, determinación del riesgo y recomendaciones de control. El objetivo final de NIST 800-30 es el poder ayudar a las entidades a gestionar de mejor manera los riesgos mediante la evaluación, mitigación, análisis y evaluación del riesgo [8].

1.5.2.4. **MAGERIT**

MAGERIT es la metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica. En la introducción de MAGERIT se tienen dos objetivos principales, el primero estudia los riesgos que soporta un sistema de información y su entorno asociado, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, y el segundo relacionado con recomendar las medidas apropiadas que se deberían adoptar para conocer, prevenir, mitigar o controlar los riesgos investigados [8].

1.5.3. **Uso de la metodología Magerit.**

La metodología que se escogió para el presente proyecto de titulación es Magerit, se la escogió ya que implementa un proceso de gestión de riesgo dentro de un marco de trabajo, para que las entidades tomen buenas decisiones, teniendo en cuenta los riesgos que conllevan el uso de las tecnologías de la información, por lo que esta metodología tiene un alto nivel de satisfacción en los elementos de TI, tales como hardware, software, bases de datos, redes y comunicación, recursos humanos y servicios.

El análisis de riesgos con Magerit sigue estos pasos:

Tabla 1.3: Pasos para el análisis de riesgo Magerit.

Magerit	
Paso 1	Caracterización de los activos
Paso 2	Identificación de amenazas
Paso 3	Reconocimiento de vulnerabilidades.
Paso 4	Análisis del riesgo
Paso 5	Plan de tratamiento de Riesgos

1.6. Situación actual de la seguridad de la información en la empresa Alpha Technologies CIA. LTDA.

Esta sección muestra la información obtenida en las visitas realizadas a la empresa, las reuniones con el jefe del área de TI en Alpha Technologies CIA. LTDA, ubicada en la ciudad de Quito, en donde se llevó a cabo las evaluaciones con las herramientas Microsoft Security Assessment Tool (MSAT), NMAP, Nessus y con Check List de Auditoría “Manejo de la Seguridad de la Información”.

Esta información permite conocer el estado actual en el que se encuentra la empresa y de esta manera poder observar el cumplimiento basado en el estándar NTE INEN-ISO/IEC 27001, para conocer los problemas que tiene la entidad en cuanto a la seguridad de la información.

1.6.1. Análisis de la situación actual

Para el análisis de la situación actual de la empresa se usará la herramienta Microsoft Security Assessment Tool (MSAT), misma que permitirá conocer el estado actual en el que se encuentra la empresa, en el ámbito de la seguridad de las tecnologías de la información. Esta herramienta ayuda a las organizaciones en la evaluación del entorno, encontrando las deficiencias de seguridad de TI, proporcionando una lista de problemas y una guía de ayuda para minimizar el riesgo.

La herramienta de evaluación de seguridad de Microsoft está diseñada para ayudar a identificar y abordar los riesgos de seguridad en un entorno informático. La herramienta emplea un enfoque holístico para medir su postura de seguridad cubriendo temas de personas, procesos y tecnología. MSAT se compone de más de 200 preguntas que abarcan la infraestructura, aplicaciones, operaciones y usuarios, donde los resultados se combinan con orientación prescriptiva y esfuerzos de mitigación recomendados, incluidos enlaces a más información para obtener orientación adicional según sea necesario. Estos recursos pueden ayudar a aprender más sobre las herramientas y métodos específicos que pueden ayudar a cambiar la postura de seguridad de su entorno de TI [9].

Una vez finalizado las preguntas de la herramienta MSAT se obtiene los resultados de Perfil de riesgos para la empresa (**Business Risk Profile - BRP**), que es la medida del riesgo al que está expuesta una empresa, según el entorno empresarial y el sector en que compite, para cada área de análisis que son la infraestructura, las aplicaciones,

operaciones, y la gente (**Across analysis of áreas - AoAs**), de igual manera se obtiene el índice de defensa en profundidad (**Defense-in-Depth Index - DiDI**), que es la medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa [10].



Figura 1.2: Resultados obtenidos de BRP y DiDI de la empresa Alpha Technologies CIA. LTDA.

Fuente: Informe de la Herramienta MSAT (ANEXO I -Msat_Alphatechnologies-resumido).

Tener una puntuación alta en el BRP significa un aumento en el riesgo al que posiblemente está expuesto el negocio según el área analizada, hay que tener en cuenta que obtener una puntuación de cero es imposible, ya que siempre implica un nivel de riesgo dedicarse a una actividad comercial y porque hay riesgos comerciales que no se pueden controlar directamente. Mientras que tener una puntuación alta en el DiDI significa un entorno en el cual se tomó más medidas para implementar estrategias de defensa en el área de análisis específica, pero hay que tener en cuenta que no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno.

Cuando los valores del BRP y DiDI son comparados, se obtiene la distribución de defensa del riesgo; en un principio, una puntuación baja del BRP y alta del DiDI significa un resultado deseable, pero no siempre es así, ya que una disparidad significativa entre BRP y DiDI significa que se recomienda una revisión del área, por lo tanto indica que la estrategia de seguridad de la organización no es la adecuada, ya que es un indicio de

una estrategia general de seguridad que abarca una sola técnica de mitigación, de esta manera si la estrategia de seguridad no abarca el personal, los procesos ni la tecnología, el entorno estará expuesto a un mayor riesgo de ataque, produciendo un ambiente vulnerable dentro de la organización.

La herramienta Microsoft Security Assessment Tool de igual manera muestra la madurez de la seguridad, en donde se incluye los controles físicos y técnicos, la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente mediante la capacidad que posee la empresa para usar de forma eficaz las herramientas disponibles, de forma que se establece un nivel de seguridad sostenible a lo largo de muchas disciplinas. De esta manera la empresa debe esforzarse en alinear su nivel de madurez en el que se encuentra y la estrategia de seguridad asociada, en relación a los riesgos que trae su actividad comercial. Los diferentes niveles de madurez son [10]:

- **Básica:** algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva.
- **Estándar:** Capas múltiples de defensa utilizadas para respaldar una estrategia definida.
- **Optimizada:** Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas.

La Figura 1.3: muestra el estado que se encuentra la empresa con respecto a la distribución de defensa del riesgo y el nivel de madurez de la seguridad.



Figura 1.3: Resultados de Distribución de defensa de riesgos y Madurez de la seguridad.

Fuente: Informe de la Herramienta MSAT (ANEXO II - Msat_Alphatechnologies-Completo).

Los resultados obtenidos por la herramienta MSAT como la distribución de defensa de riesgos muestra el balance entre los riesgos y las medidas para prevenirlos, de esta

manera se puede observar que en el área de infraestructura se necesita una mejora urgente ya que cuenta con una disparidad significativa, por otro lado en el área de aplicaciones y operaciones necesita una mejora leve y en el área del personal se tiene una disparidad pareja, por lo que se sugiere mantener las medidas que actualmente se han aplicado, para que se logre un equilibrio en el negocio; por otro lado, en cuanto a la madurez de la seguridad se observa que solo en la parte del personal se tiene una madurez estándar, por lo que se necesita un poco más de control en esta área, y las demás áreas se tiene una madurez optimizada, de esta manera de acuerdo a las mejores prácticas la protección actúa de forma correcta.

1.6.1.1. Resultados de las medidas de defensa

Los resultados obtenidos de las medidas de defensa están basados en las respuestas registradas por el jefe del departamento de TI en la herramienta MSAT, los resultados se muestran en la Figura 1.4:

Leyenda:

● Cumple las mejores prácticas recomendadas

● Necesita mejorar

● Carencias severas

Infraestructura	●	Operaciones	●
Defensa del perímetro	●	Entorno	●
Reglas y filtros de cortafuegos	●	Host de gestión	●
Antivirus	●	Host de gestión-Servidores	●
Antivirus - Equipos de escritorio	●	Host de gestión - Dispositivos de red	●
Antivirus - Servidores	●	Directiva de seguridad	●
Acceso remoto	●	Clasificación de datos	●
Segmentación	●	Eliminación de datos	●
Sistema de detección de intrusiones (IDS)	●	Protocolos y servicios	●
Inalámbrico	●	Uso aceptable	●
Autenticación	●	Gestión de cuentas de usuarios	●
Usuarios administrativos	●	Regulación	●
Usuarios internos	●	Directiva de seguridad	●
Usuarios de acceso remoto	●	Gestión de actualizaciones y revisiones	●
Directivas de contraseñas	●	Documentación de la red	●
Directivas de contraseñas-Cuenta de administrador	●	Flujo de datos de la aplicación	●
Directivas de contraseñas-Cuenta de usuario	●	Gestión de actualizaciones	●
Directivas de contraseñas-Cuenta de acceso remoto	●	Gestión de cambios y configuración	●
Cuentas inactivas	●	Copias de seguridad y recuperación	●
Gestión y control	●	Archivos de registro	●
Informes sobre incidentes y respuesta	●	Planificación de recuperación ante desastres y reanudación de negocio	●
Creación segura	●	Copias de seguridad	●
Seguridad física	●	Dispositivos de copia de seguridad	●
Aplicaciones	●	Copias de seguridad y restauración	●
Implementación y uso	●	Personal	●
Equilibrio de carga	●	Requisitos y evaluaciones	●
Clústeres	●	Requisitos de seguridad	●
Aplicación y recuperación de datos	●	Evaluaciones de seguridad	●
Fabricante de software independiente (ISV)	●	Directiva y procedimientos	●
Desarrollado internamente	●	Comprobaciones del historial personal	●
Vulnerabilidades	●	Directiva de recursos humanos	●
Diseño de aplicaciones	●	Relaciones con terceros	●
Autenticación	●	Formación y conocimiento	●
Directivas de contraseñas	●	Conocimiento de seguridad	●
Autorización y control de acceso	●	Formación sobre seguridad	●
Registro	●		
Validación de datos de entrada	●		
Metodologías de desarrollo de seguridad de software	●		
Almacenamiento y comunicaciones de datos	●		
Cifrado	●		
Cifrado - Algoritmo	●		

Figura 1.4: Resultados de las medidas de defensa

Fuente: Informe de la Herramienta MSAT (ANEXO II - Msat_Alphatechnologies-Completo).

A continuación, se presentan los resultados de las medidas de defensa de cada área. El informe completo de la evaluación de la herramienta MSAT se encuentra en el ANEXO II - Msat_Alphatechnologies-Completo.

Infraestructura

Esta área se centra en el análisis del funcionamiento de la red, los procesos comerciales (internos y externos) que se deben implementar, cómo se implementan y utiliza los hosts, y la gestión y almacenamiento adecuado de la red. Al tener un diseño de la infraestructura que todos puedan comprender y seguir, se podrá identificar en la empresa las áreas de riesgo e implementar métodos para reducir las amenazas.

Análisis:

- Todas las oficinas tienen instalado cortafuegos, de igual manera usan software de cortafuegos basados en hosts para protección de los servidores.
- Todos los equipos de escritorio cuentan con soluciones de antivirus, pero no cuentan con estas soluciones los servidores de correo electrónico ni en los hosts del perímetro de red.
- En cuanto al acceso remoto se utiliza tecnología VPN que permiten el acceso a los empleados y/o socios para conectarse remotamente a la red interna, sin embargo, no se utiliza la autenticación multifactor como una segunda protección.
- Los servicios que ofrece la empresa en internet se alojan en la red del negocio, se presenta más de un segmento de red dentro de la empresa.
- Existe conexión inalámbrica a la red, utiliza el cifrado WAP en el entorno inalámbrico.
- Los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo, se requiere autenticación de contraseñas complejas para el acceso administrativo a dispositivos y hosts.
- Se requiere la autenticación de contraseñas complejas para acceder a la red interna y a los hosts.

- Las cuentas de administrador y las de usuarios usan directivas de contraseña.
- Existen directivas para las actualizaciones de virus en el entorno.

Aplicaciones

Esta área se centra sobre un conocimiento a profundidad de la arquitectura de las aplicaciones, de igual manera de un conocimiento sólido sobre la base de la aplicación del usuario, de esta manera se puede comenzar a identificar las amenazas existentes. La evaluación ayuda con la revisión de aplicaciones de la empresa para poder valorarlas desde el punto de vista de la seguridad y la disponibilidad. También se examinan las tecnologías para usarlas en la empresa para poder mejorar la defensa profunda; dicha evaluación revisa los procedimientos que la empresa puede realizar para la mitigación de riesgos.

Análisis:

- En la empresa se usa la agrupación en clúster.
- Tiene una línea de aplicaciones empresariales.
- El equipo interno de desarrollo de software ofrece revisiones y actualizaciones de seguridad.
- Las aplicaciones principales de la empresa limitan el acceso a datos y funciones confidenciales según los privilegios de la cuenta.
- Se registran los intentos fallidos de autenticación, los errores de las aplicaciones, los accesos correctos y denegados a los diferentes recursos, los cambios de datos y los cambios en las cuentas de usuario.
- Se validan todos los datos de entrada que proceden de un feed de datos.
- No dispone de herramientas de prueba de software de seguridad como parte del proceso de desarrollo de seguridad.
- No dispone de personal de desarrollo formado en una metodología de seguridad de software para ayudar a desarrollar código seguro.

Operaciones

Esta área se centra en la seguridad de la organización donde depende de los procedimientos operativos, procesos y pautas que se aplican al entorno, donde se mejora la seguridad de una organización al incluir más que solo defensas tecnológicas. Se establece que la documentación y las directrices precisas del entorno son fundamentales para la capacidad del equipo operativo de respaldar y mantener la seguridad.

Análisis:

- No cuenta con ningún modelo para la asignación de niveles de gravedad a cada componente del entorno informático.
- No se encarga a empresas independientes las evaluaciones de los medios de seguridad.
- La empresa gestiona su propio entorno informático.
- No cuenta con ningún programa de divulgación de las medidas de seguridad en la empresa.

Personal

Esta área revisa los procesos de la empresa que manejan las directivas corporativas y los procesos de recursos humanos. El área de análisis del personal también se centra en la seguridad, ya que relaciona las tareas diarias operativas. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar los riesgos del personal.

Análisis:

- Las evaluaciones de la seguridad de la empresa las realiza el personal interno.
- Existe una directiva formal para los empleados que dejan la empresa de forma hostil.
- Los sistemas se configuran por parte del personal interno.
- Existen directivas para regular las relaciones con terceros.

1.6.2. Estado de cumplimiento actual

Una vez que se ha completado el Check List, que contiene los 11 dominios de la norma NTE INEN-ISO/IEC 27001 con los objetivos y controles (ver **ANEXO III Auditoria Check List NTE INEN-ISO-IEC 27001-2011 - Manejo de Seguridad de la Información**) los resultados se obtuvieron de acuerdo a las respuestas dadas por el Jefe del área de TI, por lo tanto, cuando un control se cumple de manera correcta se le asigna el valor de “1” en la columna “**Cumple**”, cuando el control se cumple pero no en su totalidad ya sea porque no se tiene una documentación adecuada o porque hace falta alguna actividad para cumplirlo en su totalidad, en este caso se le asigna el valor de “1” en la columna “**Cumple Parcialmente**”, y cuando el control no se cumple ya sea porque no se lo lleva a cabo dentro de la empresa o porque se considera que está en estado crítico se asigna el valor de “1” en la columna “**No cumple**”, de esta manera al tener asignado todos los valores “1” en las columnas, se realiza una suma por cada columna y así obtener los porcentajes de “**Cumple**”, “**Cumple Parcialmente**” y “**No Cumple**” para cada dominio. La Figura 1.5: muestra un ejemplo de lo descrito anteriormente. Las tablas de valoración de todos los dominios para el análisis de los porcentajes se encuentran en el ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.6 Aspectos organizativos de la seguridad de la información	Cumple	Cumple parcialmente	No cumple
Organización interna			
Compromiso de la dirección con la seguridad de la información	0	1	0
Coordinación de la seguridad de la información	0	1	0
La asignación de responsabilidades relativas a la seguridad de la información	0	1	0
Proceso de autorización de recursos para el tratamiento de la información	0	1	0
Acuerdos de confidencialidad	1	0	0
Contacto con las autoridades	0	1	0
Contacto con grupos de especial interés	1	0	0
Revisión independiente de la seguridad de la información	0	0	1
A terceros			
Identificación de los riesgos derivados del acceso de terceros	1	0	0
Tratamiento de la seguridad en la relación con los clientes	1	0	0
Tratamiento de la seguridad en contratos con terceros	1	0	0
TOTAL	5	5	1

	Totales	Porcentajes
Cumple	5	46%
Cumple Parcialmente	5	45%
No Cumple	1	9%

Figura 1.5: Ejemplo de Análisis del Estado de Cumplimiento Actual según el dominio A.6 Aspectos organizativos de la seguridad de la información.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

Al obtener los resultados de los porcentajes de cumplimiento de los 11 dominios, se elaboró la matriz de cumplimiento actual, esto de acuerdo con la norma NTE INEN-ISO/IEC 27001, misma que se puede observar en la Tabla 1.4.

Tabla 1.4: Matriz de Estado de Cumplimiento Actual por Dominio.

Dominio	% Cumple	% Cumple Parcialmente	% No Cumple
A.5 Políticas de Seguridad	0%	50%	50%
A.6 Aspectos organizativos de la Seguridad de la Información	46%	45%	9%
A.7 Gestión de activos	0%	60%	40%
A.8 Seguridad ligada a los Recursos Humanos	22%	67%	11%
A.9 Seguridad Física y Ambiental	23%	54%	23%
A.10 Gestión de Comunicaciones y Operaciones	19%	37%	44%
A.11 Control de acceso	40%	48%	12%
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	44%	44%	12%
A.13 Gestión de incidentes en la Seguridad de la Información	0%	40%	60%
A.14 Gestión de la Continuidad del Negocio	0%	40%	60%
A.15 Cumplimiento	20%	30%	50%

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

Los porcentajes obtenidos de la columna “% **Cumple**” corresponden a los objetivos de control que se cumplen en cada uno de los 11 dominios, los cuales son controles y/o procedimientos con los que cuenta la empresa. Los porcentajes obtenidos de la columna “% **Cumple Parcialmente**” corresponden a los objetivos de control que se cumplen en cada dominio, pero no en su totalidad, ya sea por no tener una documentación adecuada o a su vez por no tener documentación. Finalmente, los porcentajes obtenidos de la columna “% **No Cumple**” corresponden a los objetivos de control que no poseen control alguno actualmente.

A continuación, se muestran los resultados obtenidos para los 11 dominios con relación al manejo de los objetivos de control dispuestos en la norma ISO/IEC 27001.

A.5 Políticas de Seguridad

No se define un conjunto de políticas para la seguridad de la información, que pueda ser aprobada por la dirección, publicada o comunicada a los empleados y partes externas pertinentes; solamente se cuenta con políticas internas generales.

Al no tener definido la política de seguridad de la información no se revisa a intervalos planificados, ni se producen cambios significativos para asegurar su conveniencia, adecuación y eficacia continuas.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.6:

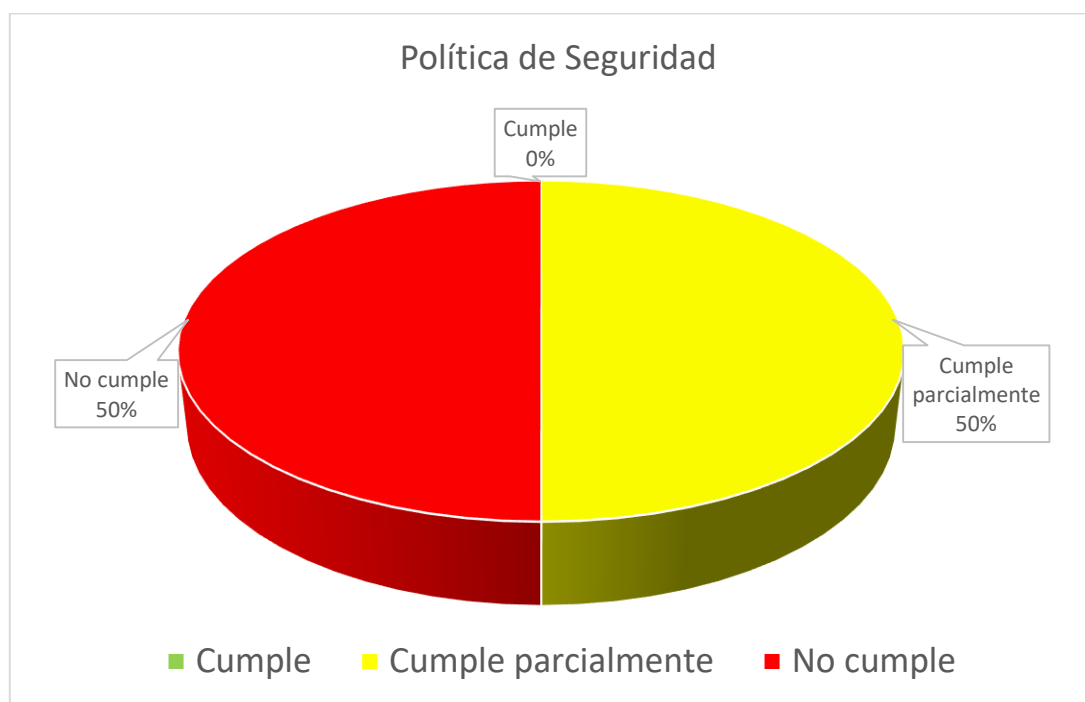


Figura 1.6: Porcentaje de cumplimiento del dominio Política de Seguridad.

Fuente: Elaborado por los autores en base al ANEXO ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.6 Aspectos Organizativos de la Seguridad de la Información

En el caso de la empresa, el área administrativa se encuentra separada del área técnica, que son las dos áreas implicadas en toda la empresa, de igual manera existe una comunicación directa con las autoridades de la empresa. En cuanto a la seguridad de la información se la trata empíricamente ya que actualmente no se realiza una gestión de proyectos. Cuando se requiere realizar teletrabajo existe un proceso a seguir para realizar la conexión a la red interna de la organización.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.7.

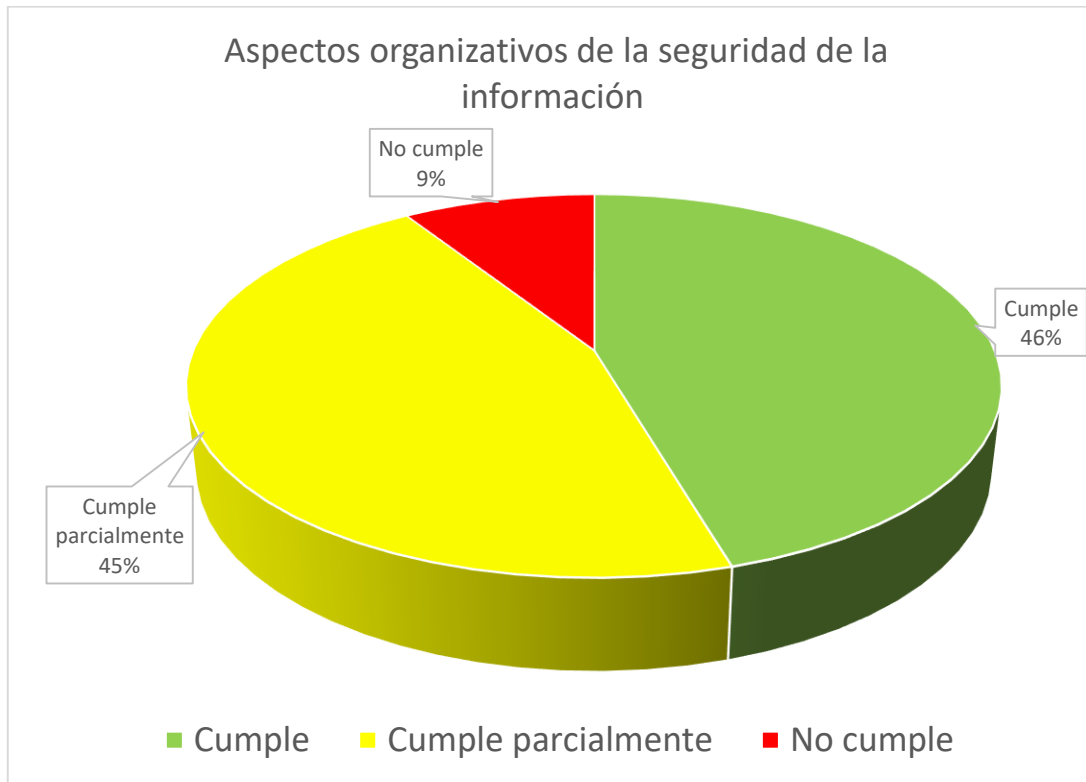


Figura 1.7: Porcentaje de cumplimiento del dominio Aspectos Organizativos de la Seguridad de la Información.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.7 Gestión de Activos

En la empresa no se cuenta con un inventario oficial y específico de activos de información, en general los activos del inventario actual cuentan con una asignación de propietarios, pero oficialmente no se cuenta con documentación de este tipo, sin embargo, se lo realiza empíricamente

Todos los empleados y usuarios de partes externas devuelven todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo, en base a los términos del contrato establecido por el área comercial.

No se cuenta con procesos específicos conforme a la clasificación de la información, no es clasificada en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.8:

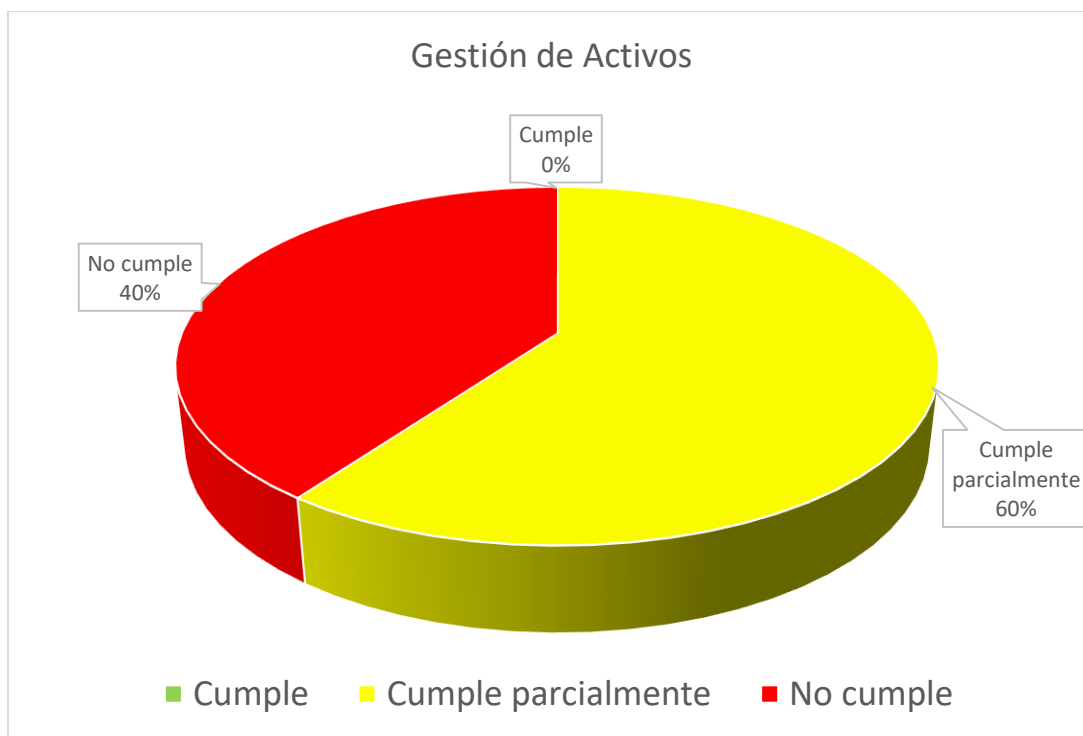


Figura 1.8: Porcentaje de cumplimiento del dominio Gestión de Activos

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.8 Seguridad ligada a los recursos humanos

En la empresa, el área administrativa cuenta con procesos de selección de personal, descripciones y requisitos de puestos. Alphatechnologies establece en los términos del contrato con empleados y contratista, procedimientos para seguridad de la información.

Actualmente, no se cuenta con un proceso disciplinario formal que indique las acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Las responsabilidades de la seguridad de la información que permanecen validas después de la terminación o cambio de contrato son comunicados al empleado o contratista por la persona encargada del área administrativa de la empresa, sin embargo no se realiza un seguimiento del cumplimiento.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.

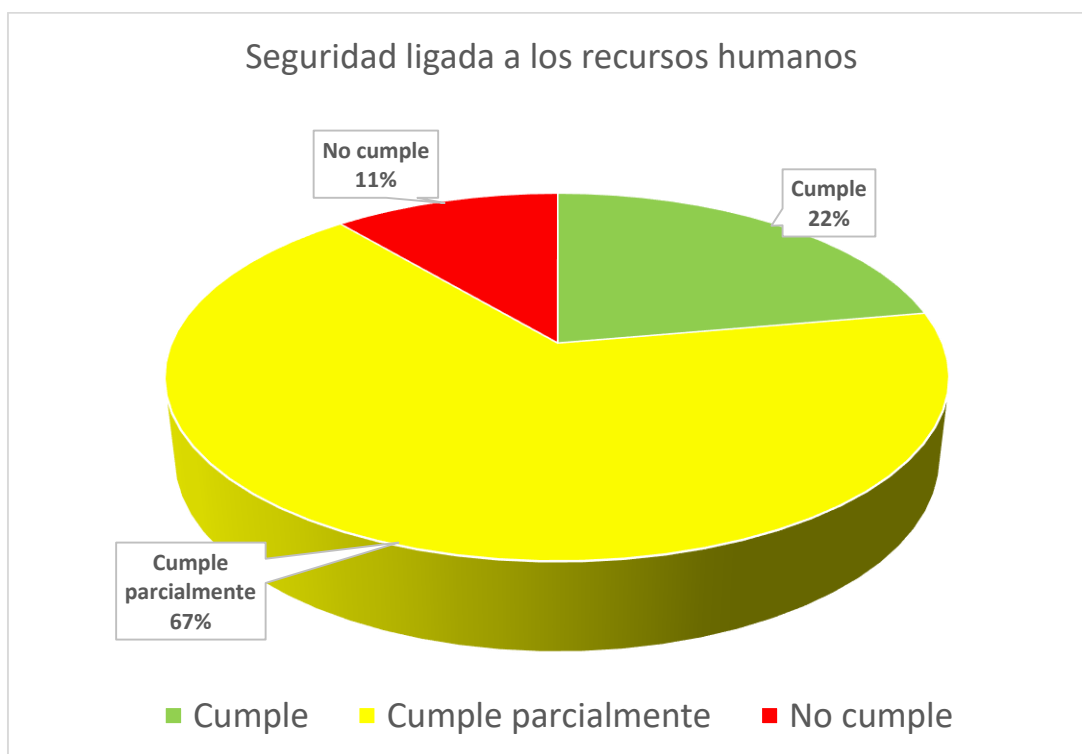


Figura 1.9: Porcentaje de cumplimiento del dominio Seguridad Ligada a los Recursos Humanos.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A. 9 Seguridad Física y Ambiental

Dentro de la empresa existen áreas delimitadas para el control sensible de la información, pero no existen controles de acceso apropiados para personal autorizado en dichas áreas.

En la empresa se diseña y aplica parcialmente protección física contra desastres naturales, ataques maliciosos o accidentes, con un plan de continuidad de negocio, pero no se protegen los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, de igual manera el cableado de potencia y de telecomunicaciones que portan datos o soportan servicios de información se encuentran parcialmente protegido contra interceptación, interferencia o daño.

En cuanto a la salida de equipos fuera de la empresa, no existe una política que permita la salida de equipos, solo en ciertos casos y con previa autorización; pero se lleva un registro y control de estos cuando son retirados de su sitio de trabajo.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.10.

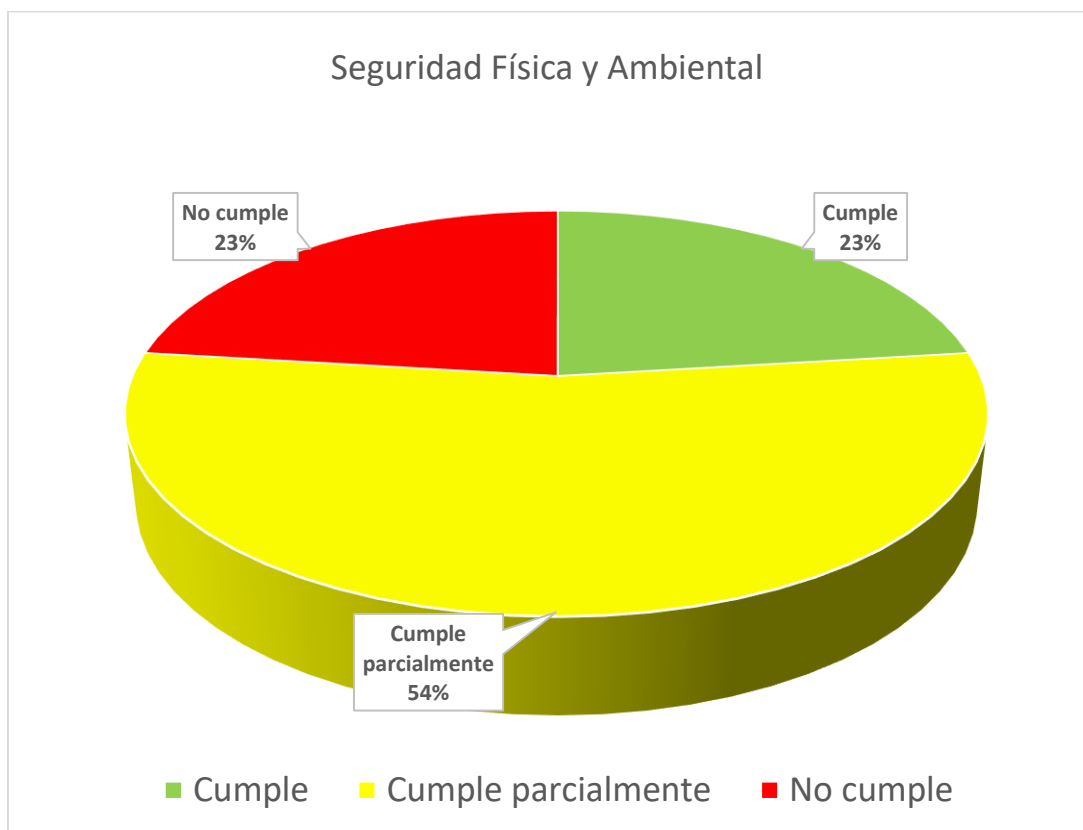


Figura 1.10: Porcentaje de cumplimiento del dominio Seguridad Física y Ambiental.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.10 Gestión de Comunicaciones y Operaciones

Existen manuales que han sido elaborados por la necesidad o por pedidos momentáneos, es decir no se encuentran revisados y/o aprobados por alta gerencia.

Las tareas se encuentran segregadas por roles de usuarios. El ambiente de producción se encuentra separado al ambiente de pruebas.

Se evalúa previamente las capacidades necesarias para la gestión de la capacidad en cuanto a disco, RAM y CPUs para que estén siempre con los criterios aceptables.

Aun cuando no se encuentra escrito la política de backups, si se realizan copias de seguridad de la información del CORE del negocio.

Existen políticas de acceso al internet por medio del proxy, además se manejan: firewall, antivirus y en ciertos casos algoritmos de cifrado.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.11.

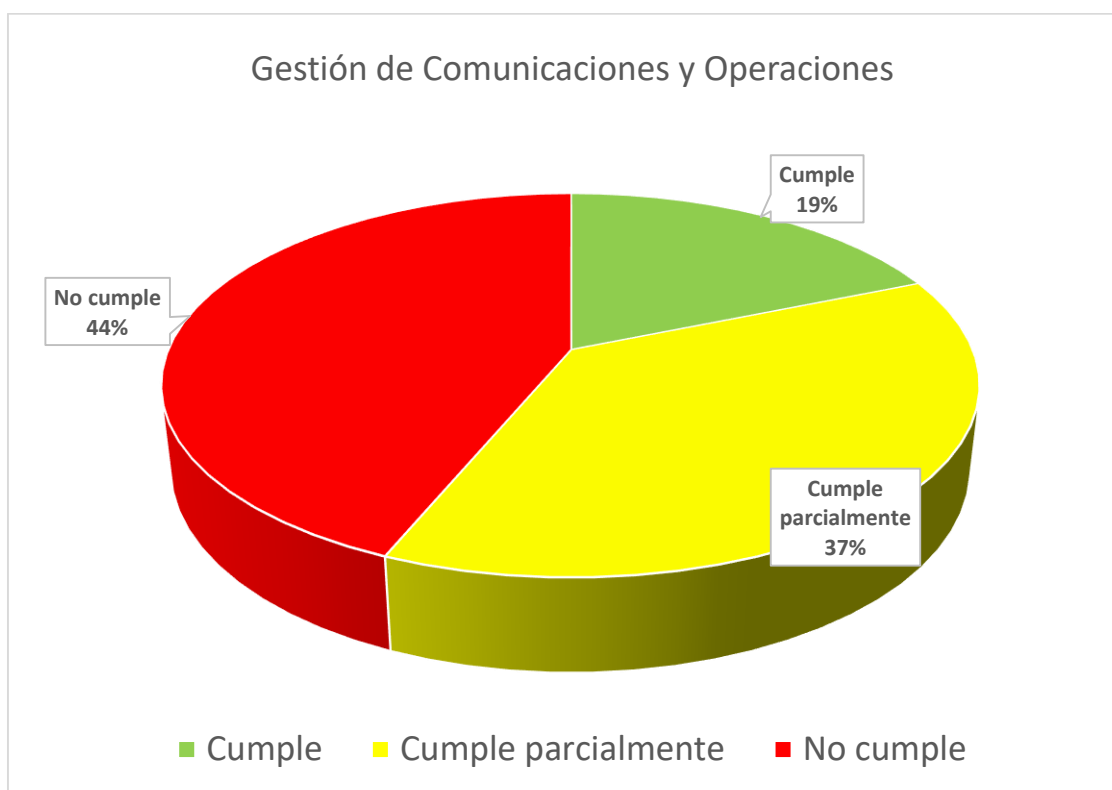


Figura 1.11: Porcentaje de cumplimiento del dominio Gestión de Comunicaciones y Operaciones.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.11 Control de Acceso

Dentro del empresa existe una política de control de acceso, pero solo es difundida de manera verbal, no está documentada, este control de acceso se revisa periódicamente; se establecen perfiles de acceso y solo los usuarios autorizados poseen las credenciales para el control de acceso, de igual manera existen procesos para el control de información secreta que se comparte en la organización.

Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información, son retiradas al terminar su empleo, contrato o acuerdo.

El acceso a los sistemas y aplicaciones es restringido por la política de control de acceso, ya que existe el uso de software para el control de acceso seguro.

Los sistemas de gestión de contraseñas son interactivos y aseguran la calidad de las contraseñas, ya que las contraseñas deben cumplir ciertas políticas para ser generadas.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.1212.

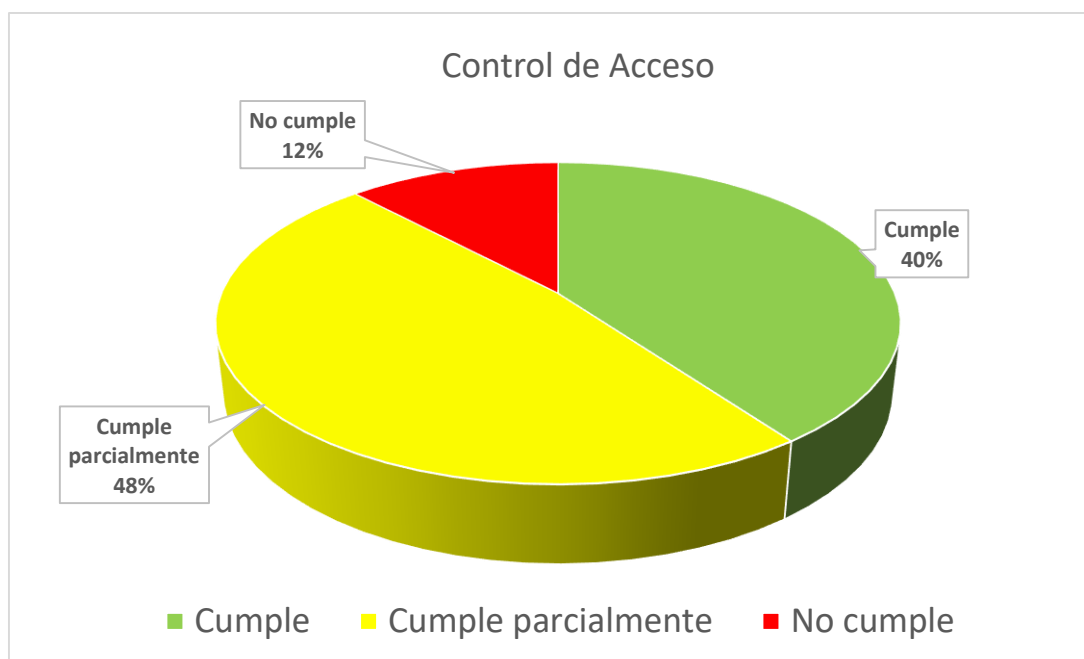


Figura 1.12: Porcentaje de cumplimiento del dominio Control de Acceso.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de información

Dentro de la empresa siempre se tiene presente la seguridad de las partes interesadas en los requisitos de nuevos sistemas, existe un instructivo general de seguridad y uso adecuado de las tecnologías de la información, de igual manera existen las declaraciones de confidencialidad, así como puede ser el caso de firmas digitales.

La empresa supervisa y hace seguimiento de la actividad de desarrollo de sistemas contratados externamente al realizar un monitoreo constante, cuando el cliente en cuestión lo permite con los debidos acuerdos de confidencialidad.

Cuando se cambian las plataformas de operación, se revisan las aplicaciones críticas del negocio, y se ponen a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización, ya que siempre existe un proceso de pruebas tanto de entornos de operación, así como los programas que se deben cambiar.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.13.

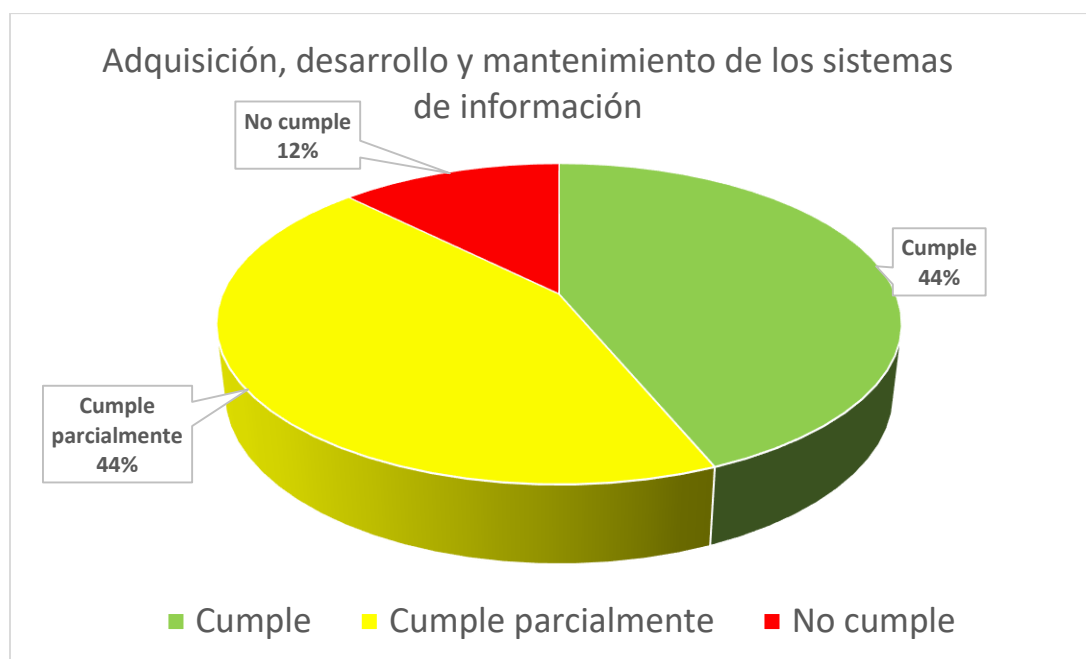


Figura 1.13: Porcentaje de cumplimiento del dominio Adquisición, Desarrollo y Mantenimiento de los Sistemas de información.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.13 Gestión de Incidentes de Seguridad de la Información

En la empresa no se establecen responsabilidades ni procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Se exige a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios, y divulgarlos constantemente a todos los involucrados con la organización.

El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se usa para reducir la posibilidad o el impacto de incidentes futuros, y toda nueva investigación es documentada para mejorar la seguridad de la información.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.1414.

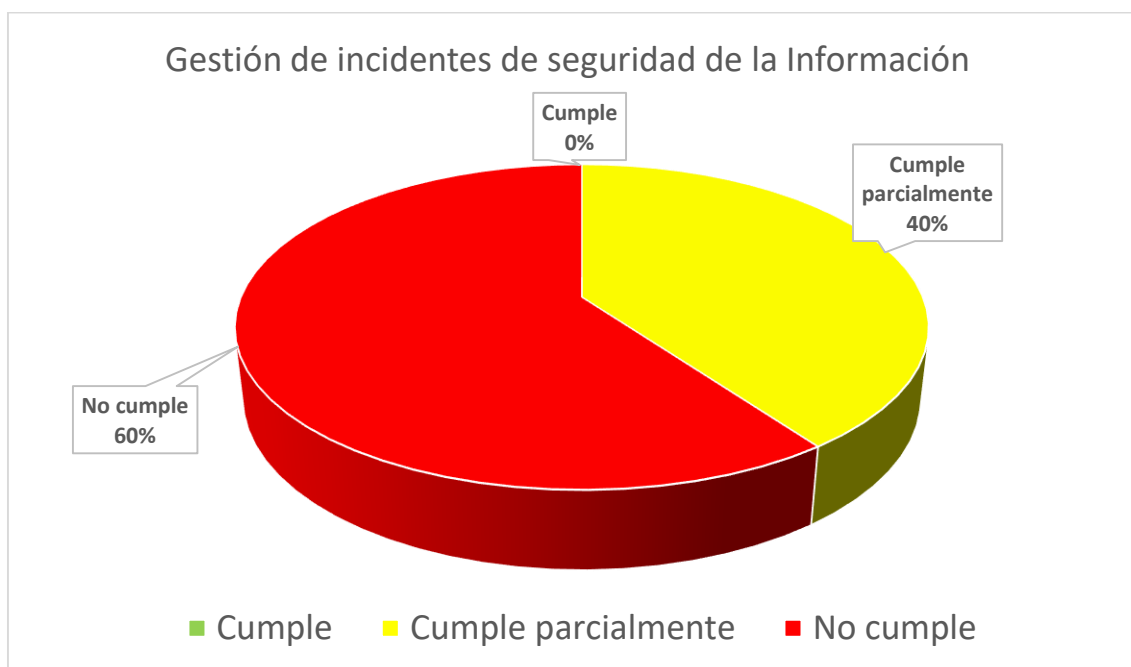


Figura 1.14: Porcentaje de cumplimiento del dominio Gestión de Incidentes de Seguridad de la Información.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.14 Gestión de la Continuidad del Negocio

En la empresa no existe un plan de continuidad del negocio, ni un plan de recuperación durante una crisis o desastre.

Las instalaciones de procesamiento de información dentro de la empresa se implementan con redundancia suficiente para cumplir los requisitos de disponibilidad, ya que cuenta con controles de redundancia.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.152.

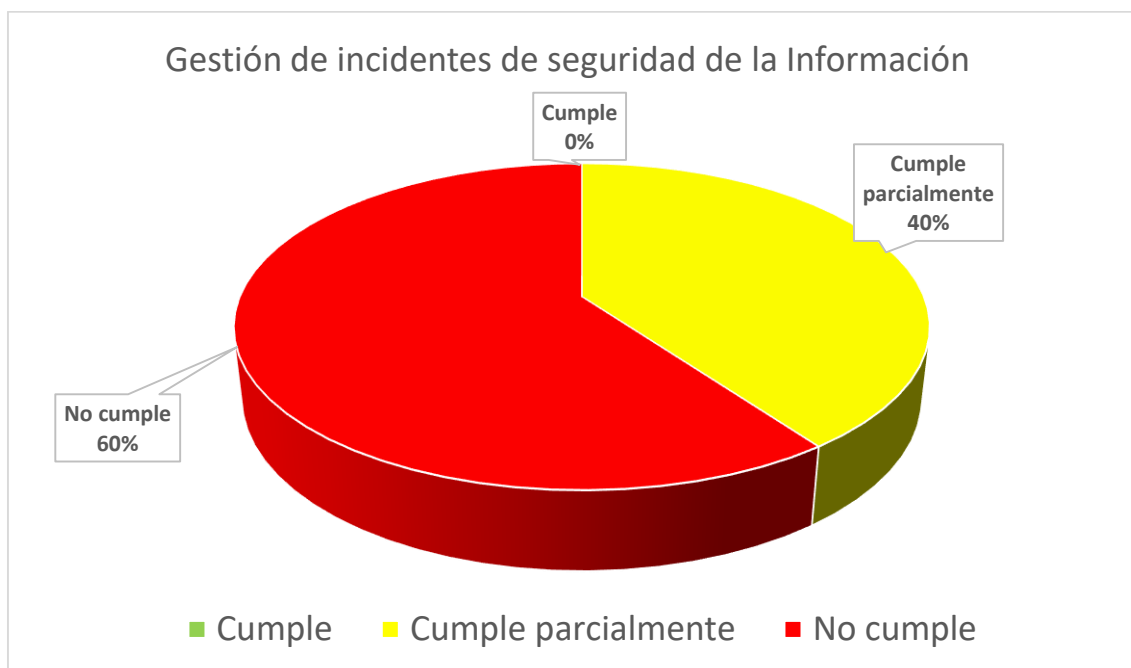


Figura 1.152: Porcentaje de cumplimiento del dominio Gestión de la Continuidad del Negocio.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

A.15 Cumplimiento

Se cumplen parcialmente los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización al tener solo los contratos.

Existe un proceso para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material para los que puede haber derechos de propiedad intelectual y sobre la utilización de productos de software propietario, sin embargo, la empresa procura el uso de software libre.

Los registros importantes de la organización tienen un nivel básico de protección en cuanto a la destrucción y pérdida; no existen etiquetados y no hay procesos definidos para este tratamiento.

El resultado de los porcentajes de cumplimiento de este dominio se puede observar en la Figura 1.3.

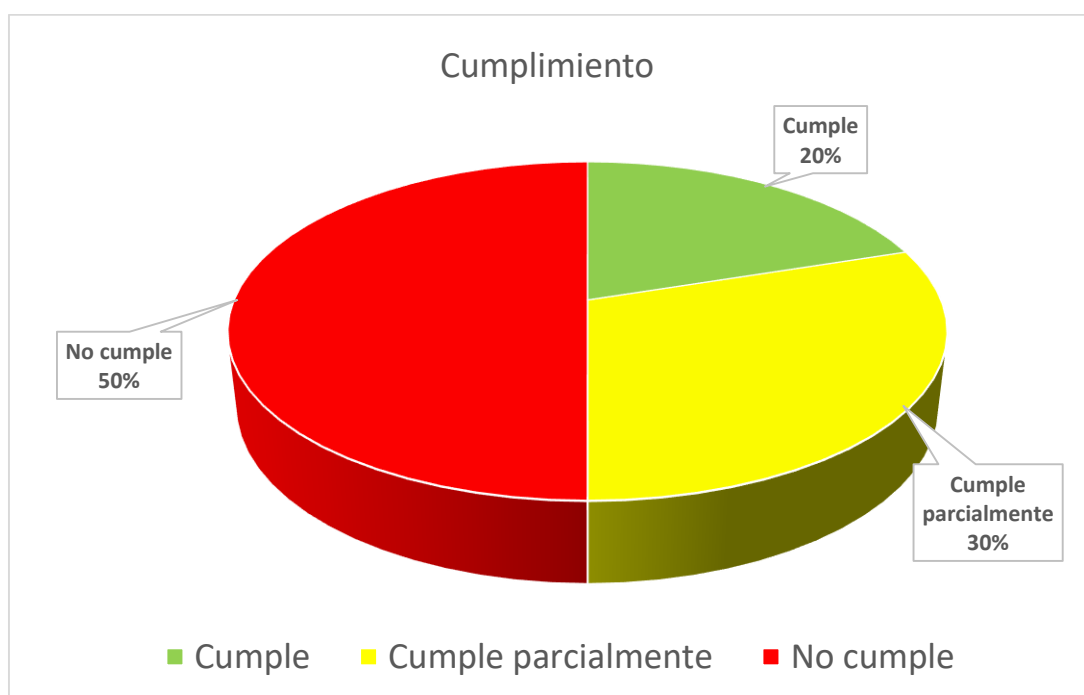


Figura 1.36: Porcentaje de cumplimiento del dominio Cumplimiento.

Fuente: Elaborado por los autores en base al ANEXO IV - Análisis del Estado de Cumplimiento Actual.

2. APLICACIÓN DE LA METODOLOGÍA

2.1. Análisis y evaluación de riesgos

El análisis y evaluación de riesgo se lo puede realizar de diferentes maneras y con diferentes grados de detalle, esto depende de la metodología seleccionada y el valor que posee cada activo involucrado del negocio.

En esta sección se dedicará a realizar el análisis y evaluación de riesgo con el objetivo de identificar las vulnerabilidades existentes en la empresa y las amenazas a las que están expuestos, para así valorar el riesgo existente. Con la información obtenida en esta sección, la alta gerencia junto al área de tecnologías de la información definirá el tratamiento de los riesgos existentes. Cabe recalcar que el análisis y evaluación de riesgo es el punto central para la definición de una estrategia en cuanto a la seguridad, la misma que debe estar alineada con la visión del negocio y el entorno operacional.

De acuerdo con la metodología seleccionada, descrita en la sección 1.5.3 uso de la metodología Magerit, se realizará el análisis y evaluación de riesgos en base a dicha metodología, cuyo proceso se resume en la figura 2.1 [11].

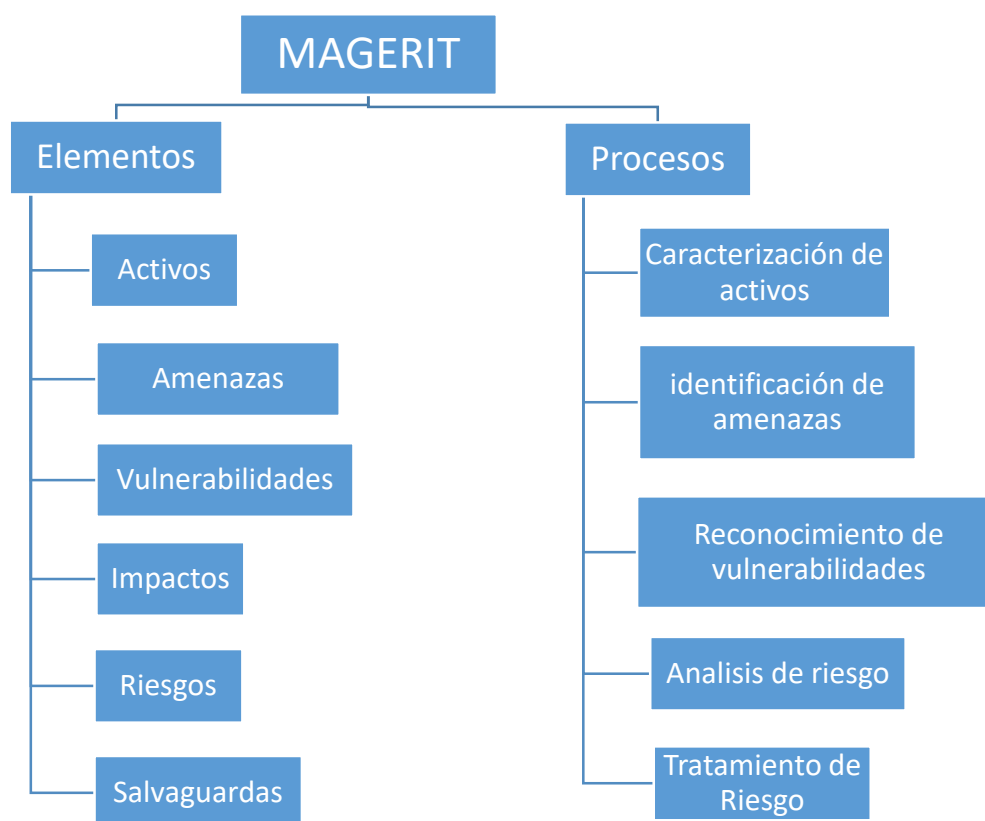


Figura 2.1: Proceso de análisis y evaluación de riesgos Magerit.

2.2. Pasos para la evaluación de riesgos según la metodología Magerit

A continuación, se explica cada uno de los pasos que conforman el proceso de análisis y evaluación de riesgos de la metodología Magerit.

2.2.1. Caracterización de los activos.

Tiene como objetivo identificar todos los activos dentro de la empresa necesarios para que el negocio funcione correctamente. Los activos son aquellos componentes o funcionalidad de un sistema de información que puede ser atacado accidentalmente o de manera deliberada, que puede tener repercusiones para toda la empresa, los activos del negocio son [11]:

- Información.
- Datos.
- Servicios.
- Aplicaciones (software).
- Equipos (hardware).
- Comunicaciones.
- Recursos administrativos.
- Recursos físicos.
- Recursos humanos.

2.2.2. Identificación de amenazas.

Tiene como objetivo determinar las vulnerabilidades y amenazas que pueden perjudicar a los activos (sistemas, recursos, información, entre otros.) de la empresa. Una vulnerabilidad es una debilidad o defecto propio en la implementación u operación de un activo, la cual puede materializarse por la ocurrencia de una amenaza. Las amenazas son cosas que pueden ocurrir de manera accidental o intencional. Existen diferentes tipos de amenazas que pueden ocurrir, las cuales son [11]:

- **De origen natural:** Estas amenazas son ocasionados por accidentes naturales (inundaciones, terremotos, entre otros). Ante estos problemas los sistemas de información son víctimas de manera pasiva.

- **Del entorno (Origen industrial):** Estas amenazas son ocasionados por desastres industriales (fallos eléctricos, contaminación, entre otros). Ante los cuales los sistemas de información son víctimas de manera pasiva.
- **Defectos de las aplicaciones:** Estas amenazas nacen directamente por defectos propios del equipamiento, ya sea por su diseño o por su implementación, provocando consecuencias potencialmente negativas en los sistemas. Estas son denominadas frecuentemente como vulnerabilidades técnicas.
- **Causadas de manera accidental por las personas:** Como su nombre lo dice, estas amenazas son accidentes causadas típicamente por error o por omisión de parte de las personas con acceso a los sistemas.
- **Causadas de manera deliberada por las personas:** Estas amenazas son causadas intencionalmente por las personas, por ataques deliberados, con ánimo de beneficiarse indebidamente o con ánimo de causar daños y perjuicios al negocio.

2.2.3. Reconocimiento de vulnerabilidades.

Para el reconocimiento de vulnerabilidades, Magerit aconseja analizar la situación en la que se encuentran de los activos, con el fin de detectar vulnerabilidades que pueden ser susceptibles, de igual manera las salvaguardas o los controles con los que se cuentan, todo esto se aconseja con el fin de poder evaluar el riesgo de los activos [11].

2.2.4. Análisis del riesgo

2.2.4.1. Valoración de la probabilidad

Cuando se hayan determinado las amenazas que pueden perjudicar a los activos, se identificará el riesgo que existe sobre cada activo crítico identificado, para lo cual se tomará en cuenta la probabilidad de ocurrencia y el impacto que puede llegar a tener sobre el negocio. Para poder determinar la probabilidad de ocurrencia se utilizará una valoración cuantitativa y cualitativa, en donde la valoración cuantitativa servirá para poder obtener los cálculos relacionados con el riesgo, mientras que la valoración cualitativa servirá para facilitar el entendimiento de las personas, donde se tendrá el tiempo y la escala según la probabilidad de ocurrencia, esta valoración cuantitativa y cualitativa se mostrarán en la tabla 2.1 [11].

Tabla 2.1: Valoración de la probabilidad.

Probabilidad de ocurrencia		
Valor	Ocurrencia	Tiempo
1	muy poco frecuente	Siglos
2	Poco frecuente	Cada varios años
3	Normal	Una vez al año
4	Frecuente	Mensualmente
5	Muy frecuente	A diario

Fuente: Elaborado por los autores en base a la metodología Magerit (Libro I – Método)

2.2.4.2. Valoración del impacto

Impacto se le denomina a la medida del daño que causa a un activo crítico, derivado de la materialización de una amenaza y cause vulnerabilidades.

Los aspectos a evaluar serán la integridad, confidencialidad y la disponibilidad del activo crítico en caso de que se materialice la amenaza [11].

- **Integridad:** Se refiere al aseguramiento de validez y exactitud de la información que se maneja en el negocio, controlando y protegiendo las modificaciones de la información, y no permitir alteraciones no autorizadas; la integridad en la información puede ser manipulada o llegar a ser incompleta.
- **Confidencialidad:** Se refiere al aseguramiento de la información con respecto al acceso a la misma, únicamente personas o procesos autorizados pueden acceder los recursos o información, alguien sin autorización atenta contra la confidencialidad y afectaría la confianza de la empresa.
- **Disponibilidad:** Se refiere al uso de un recurso o servicios en el momento en que se requiera, un problema con la disponibilidad dentro de la empresa significaría fallos en la productividad.

Con respecto a estos aspectos que se evaluarán, se implementará una escala para calcular el impacto de acuerdo a una simple respuesta a la siguiente pregunta, “la amenaza afecta o no a los aspectos establecidos”, la respuesta deberá ser **Sí** o **No**, de esta manera se le asignarán a las respuestas los valores **1** y **0** respectivamente, dichos valores se los sumaran de acuerdo a los aspectos para tener el valor real de impacto, al ser tres aspectos el valor máximo que puede tener será **tres** y será asignado como

Impacto Alto; el valor mínimo que puede tener será **cero**, lo cual significa que no afecta a ningún activo crítico y no representa una amenaza, de esta manera se eliminarán estas amenazas; para los valores **uno** y **dos** significaran **Impacto bajo** y **medio respectivamente**; para identificar el impacto que tendrá la amenaza se utilizara la Tabla 2.2.

Tabla 2.2: Valoración del impacto.

Valoración	Impacto
1	Bajo
2	Medio
3	Alto

Fuente: Elaborado por los autores.

Se tomarán en consideración 3 niveles de impacto como se muestra en la tabla 2.2, los cuales serán detallados a continuación:

- **Impacto Alto:** Un nivel alto de impacto puede causar daños severos, lo cual puede provocar una pérdida considerable de información importante y confiable, afectando a la continuidad del negocio, lo cual podría provocar una suspensión de actividades del negocio de manera indefinida.
- **Impacto medio:** Un nivel medio de impacto puede provocar que el negocio deje de prestar servicios en un periodo de tiempo corto, lo cual de igual manera provocaría una perdida en producción hasta que sus procesos vuelvan a ser implementados con normalidad.
- **Impacto Bajo:** Un nivel bajo de impacto no causa daños significativos dentro de la empresa, al ser así, la empresa puede seguir brindando sus servicios,

2.2.4.3. Determinación del riesgo

Para determinar la severidad del riesgo, se tomará en cuenta el siguiente cálculo:

Tabla 2.3: Cálculo del riesgo.

$$\text{Riego} = \text{Probabilidad} \times \text{Impacto}.$$

Probabilidad	Riesgo = Probabilidad x Impacto		
5	5	10	15
4	4	8	12
3	3	6	9
2	2	4	6
1	1	2	3

	1	2	3
	Impacto		

Fuente: Elaborado por los autores.

De esta manera se determinará el riesgo teniendo en cuenta 3 categorías, las cuales se muestran en la Tabla 2.4.

Tabla 2.4: Niveles de riesgo.

Niveles de riesgo	Valor
Riesgo Bajo	1 a 3
Riesgo Medio	4 a 6
Riesgo Alto	8 a 15

Fuente: Elaborado por los autores.

- **Riesgo Bajo:** A este nivel pertenecen los riesgos que tienen un valor de 1 a 2, de acuerdo a la fórmula de riesgo. Estos riesgos en caso de materializarse no causan daño a la empresa, al no interrumpir sus actividades diarias ni causando daño a los usuarios.
- **Riesgo Medio:** A este nivel pertenecen los riesgos que tienen un valor de 3 a 6, de acuerdo con la fórmula de riesgo. Estos riesgos son los que pueden causar daño al negocio afectando menormente los objetivos de la empresa.
- **Riesgo Alto:** En este nivel pertenecen los riesgos que tienen un valor de 7 a 15, de acuerdo con la fórmula de riesgo. Estos riesgos son los que afectarían de manera severa la continuidad del negocio, provocando pérdidas significativas a toda la organización.

2.2.5. Plan de tratamiento de Riesgos.

Para el tratamiento del riesgo se debe iniciar con la identificación de salvaguardas o controles, las cuales deben definir la eficacia de su implementación contra los riesgos encontrados.

Los controles se enfocan principalmente en atacar a un riesgo, lo cual lo hace desde 2 perspectivas [11]:

- Reducir la probabilidad de las amenazas, impidiendo que la amenaza se materialice (mitigar la ocurrencia de la amenaza).
- Limitando el daño, las amenazas en este caso se materializan; pero se limita las consecuencias que pueden provocar (mitigar el daño causado).

La metodología Magerit presenta diferentes tipos de protección prestados por los controles o salvaguardas para el tratamiento del riesgo, las cuales se muestran en la Tabla 2.5 [11].

Tabla 2.5: Tipos de protección.

Tipo de Protección	Descripción
[PR] Prevención	Reduce las oportunidades de que un incidente ocurra.
[EL] Eliminación	Elimina un incidente cuando impide que este tenga lugar.
[IM] Minimización del impacto	Minimiza o limita el impacto cuando acota las consecuencias de un incidente.
[CR] Corrección	Repara el daño producido por la amenaza, este actúa después de que ocurrió el incidente y por lo tanto reducen los daños.
[MN] Monitorización	Trabaja monitorizando lo que está ocurriendo o lo que ha ocurrido, de esta manera actúa según la situación.
[DC] Detección	Detecta un ataque cuando informa que está ocurriendo; no impide el ataque pero permite que operen otras medidas que minimicen el daño.
[AW] Concienciación	Formación de las personas que pueden tener influencia sobre el sistema.
[AD] Administración	Está relacionada a los componentes de seguridad del sistema.

Fuente: Elaborado por los autores, Fuente: Magerit libro I –Método.

2.2.5.1. Eficacia de la protección

En el tratamiento de riesgo las salvaguardas o los controles se caracterizan por su eficacia al tratar contra el riesgo. En la Tabla 2.6 se puede observar el grado de eficacia de un control o salvaguarda considerando los aspectos de escala de la madurez.

Tabla 2.6: Nivel de madurez.

Efectividad	Nivel	Significado
0%	L0	Inexistente
5%	L1	Inicial / Ad-hoc
25%	L2	Reproducibile, pero intuitivo
50%	L3	Proceso definido
75%	L4	Gestionado y medible
100%	L5	Optimizado

Fuente: Elaborado por los autores, Fuente: Magerit libro I –Método.

2.3. Evaluación de riesgos según la metodología MAGERIT

El objetivo del presente proyecto de titulación es realizar una evaluación de riesgos dentro de la empresa Alpha Technologies CIA. LTDA., para medir las consecuencias de los daños causados por las amenazas existentes, las causas de los daños a la información, y el conocer qué hacer ante estos problemas de la empresa.

Para la presente evaluación de riesgo se realizaron revisiones de documentos de la empresa, entrevistas con el jefe del área de tecnología, levantamiento de información de la empresa, escaneos de vulnerabilidades con las herramientas Nessus y Nmap, y el uso de herramientas como Msat y Check List.

2.3.1. Caracterización de los activos.

La caracterización, análisis y evaluación de los activos, la información y los recursos tecnológicos de la empresa se encuentra descrita en la sección **1.4 Reconocimiento de** y en el **ANEXO A - Activos principales de información Alphatechnologies.**

2.3.2. Identificación de amenazas.

Al tener identificados los activos de información que pertenecen a la empresa Alpha Technologies CIA. LTDA, el siguiente paso es reconocer las amenazas que pueden afectar dichos activos. Se usó el libro II de Magerit como referencia para facilitar este proceso, en donde se indica que dependiendo del tipo de activo se definieron amenazas que pueden afectarlos. En la Tabla 2.7 se detallan las amenazas que los activos de la empresa están más expuestos, identificadas en las visitas y entrevistas con el personal del área de Tecnología de la empresa.

Tabla 2.7: Amenazas.

Desastres naturales
Estas amenazas pueden ocurrir sin intervención de las personas como causa directa o indirecta.
<ul style="list-style-type: none">• Fuego• Daños por Agua• Desastres Naturales
De origen industrial

Estas amenazas pueden ocurrir de forma accidental, causados por actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- Corte de suministro eléctrico
- Condiciones inadecuadas de temperatura y/o humedad
- Desastres Industriales
- Contaminación mecánica
- Avería de origen físico o lógico
- Fallo de servicio de comunicaciones

Errores o fallos no intencionados

Estas amenazas pueden ocurrir a causa de errores en las personas de forma no intencional.

- Errores de los usuarios
- Errores del administrador
- Errores de monitorización (Log)
- Errores de configuración
- Alteración accidental de la información
- Destrucción de información
- Divulgación de información (fuga)
- Fugas de Información
- Vulnerabilidades de los programas (software)
- Errores de mantenimiento /actualización de equipos (hardware)
- Caída del sistema por agotamiento de recursos
- Indisponibilidad del personal

Ataques intencionados

Estas amenazas pueden ocurrir a causa de las personas de forma intencional, con el propósito es causar afectación.

- Manipulación de la configuración
- Suplantación de la Identidad del usuario
- Abuso de privilegios de acceso
- Difusión de software dañino
- Acceso no autorizado
- Modificación de la información
- destrucción de la información
- Divulgación de Información
- Manipulación de equipos
- Manipulación de programas
- Denegación de servicio
- Interceptación de información (escucha)
- Ingeniería Social

Fuente: Elaborado por los autores, Fuente: Magerit libro II, ver **ANEXO V - Identificación de Amenazas**

2.3.3. Reconocimiento de vulnerabilidades.

Las vulnerabilidades son las debilidades que poseen los activos, las cuales pueden ser aprovechadas por las amenazas, de esta manera se puede decir que las vulnerabilidades están directamente relacionadas con las amenazas.

Los resultados del escaneo de vulnerabilidades con las herramientas Nessus y Nmap se las puede ver en el ANEXO V – Escaneo de Vulnerabilidades con las herramientas NMAP Y NESSUS.

Para obtener las vulnerabilidades lógicas se usaron las herramientas Nessus y Nmap, se realizó el escaneo en los 6 servidores, las vulnerabilidades encontradas se las puede visualizar en la Tabla 2.8.

Tabla 2.8: Vulnerabilidades lógicas.

Severidad	Vulnerabilidad	Descripción
Crítica	ISC BIND <9.2.2 Funciones de resolución de DNS Desbordamiento remoto	El servidor DNS remoto de BIND 9, de acuerdo con su número de versión, es vulnerable a un desbordamiento de búfer que puede permitir que un atacante obtenga un shell en este host o deshabilite este servidor.
Alta	Protocolo SSH Versión 1 Recuperación de clave de sesión	El demonio SSH remoto admite conexiones realizadas con la versión 1.33 y / o 1.5 del protocolo SSH. Estos protocolos no son completamente criptográficamente seguros, por lo que no deben usarse.
Alta	Detección de protocolo SSL versión 2 y 3	Un atacante puede explotar estos defectos para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.
Media	Reenvío de IP habilitado	El host remoto tiene habilitado el reenvío de IP. Un atacante puede explotar esto para enrutar paquetes a través del host y potencialmente omitir algunos firewalls / enrutadores / filtros NAC.
Media	No se puede confiar en el certificado SSL	No se puede confiar en el certificado X.509 del servidor
Media	HTTP TRACE / TRACK Métodos permitidos	El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

Media	Suites de cifrado SSL de resistencia media compatibles (SWEET32)	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa el conjunto de encriptación 3DES.
Media	Certificado auto-firmado SSL	La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.
Media	Divulgación de información remota por el DNS Caché Snooping	El servidor DNS remoto responde a consultas de dominios de terceros que no tienen establecido el bit de recursividad. Esto puede permitir que un atacante remoto determine qué dominios se han resuelto recientemente a través de este servidor de nombres y, por lo tanto, qué hosts se han visitado recientemente.
Media	Divulgación de información de transferencia de zona del servidor DNS (AXFR)	El servidor de nombres remoto permite realizar transferencias de zona DNS. Una transferencia de zona permite a un atacante remoto llenar instantáneamente una lista de objetivos potenciales
Media	Servicios de Terminal Server no usa autenticación de nivel de red (NLA)	Los Servicios de Terminal Server remotos no están configurados para usar solo la Autenticación de nivel de red (NLA). NLA usa el protocolo de Credential Security Support Provider (CredSSP) para realizar una autenticación de servidor sólida, ya sea a través de mecanismos TLS / SSL o Kerberos, que protegen contra los ataques de intermediarios
Media	El nivel de cifrado de servicios de terminal es medio o bajo	El servicio remoto de Terminal Services no está configurado para usar criptografía sólida. El uso de criptografía débil con este servicio puede permitir que un atacante escuche las comunicaciones con mayor facilidad y obtenga capturas de pantalla y / o pulsaciones de teclas.

Media	Debilidad en el Servidor de protocolo de escritorio remoto de Microsoft Windows	El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información confidencial transmitida, incluidas las credenciales de autenticación.
Media	Certificado SSL firmado con algoritmo de hash débil	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1).
Media	Divulgación de información del encabezado de Apache Server ETag	El servidor web remoto se ve afectado por una vulnerabilidad de divulgación de información debido a que el encabezado ETag proporciona información confidencial que podría ayudar a un atacante.
Media	SSH Algoritmos débiles compatibles	Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.
Media	Directorios web navegables	Directorios web navegables
Baja	Detección de servidor DHCP	Este script se pone en contacto con el servidor DHCP remoto (si existe) e intenta recuperar información sobre el diseño de la red. Algunos servidores DHCP proporcionan información confidencial, como el nombre de dominio NIS, o información de diseño de red, como la lista de servidores web de red, etc.
Baja	Cifrado del modo CBC del servidor SSH habilitados	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.
Baja	SSL RC4 Cipher Suites compatibles (Bar Mitzvah)	El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, por lo que se introduce una gran variedad de pequeños sesgos en la secuencia, lo que disminuye su aleatoriedad.

Baja	Módulo SSL / TLS Diffie-Hellman <= 1024 Bits (Logjam)	El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en poco tiempo (dependiendo del tamaño del módulo y los recursos del atacante). Esto puede permitir a un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.
Baja	El nivel de cifrado de Servicios de Terminal Server no cumple con FIPS-140	La configuración de cifrado utilizada por el servicio de Terminal Services remoto no cumple con FIPS-140.
Baja	SSH Algoritmos débiles de MAC habilitados	El servidor SSH remoto está configurado para permitir algoritmos MAC MD5 o de 96 bits, los cuales se consideran débiles.

Fuente: Elaborado por los autores, Fuente: Nessus, ver **ANEXO VII – Análisis de vulnerabilidades**

Para obtener las vulnerabilidades físicas se realizaron reuniones y entrevistas con el jefe del área de tecnología, en dichas reuniones se usaron las herramientas Msat y Check List de auditoria (ANEXO III Auditoria Check List NTE INEN-ISO-IEC 27001-2011 - Manejo de Seguridad de la Información), las vulnerabilidades encontradas se las puede visualizar en la Tabla 2.9.

Tabla 2.9: Vulnerabilidades físicas.

Vulnerabilidad	Descripción
No existe segmentos DMZ	No tiene ningún segmento DMZ para proteger los recursos corporativos.
No se comprueban los cortafuegos	Los cortafuegos no se comprueban regularmente para asegurarse de que funciona correctamente.
Servidores de correo electrónico sin antivirus	No hay ningún software antivirus instalado en los servidores de correo electrónico.
Hosts del perímetro de red sin antivirus	No hay ningún software antivirus instalado en los hosts del perímetro de red.
Servidores sin antivirus	No se utilizan soluciones antivirus en el nivel de los servidores.

No se tiene autenticación multifactorial para conexión remota a la red interna	No utiliza autenticación multifactorial como un segundo escudo protector, para empleados y/o socios que se conectan remotamente a la red interna.
Difusión del SSID activado	No se ha desactivado la difusión del SSID en el punto de acceso.
No se usa restricción MAC	No se utiliza la restricción por MAC en el entorno inalámbrico.
Usuarios con acceso administrativo	Los usuarios tienen habilitados accesos administrativos a sus estaciones de trabajo.
No se utilizan directivas de contraseñas	Las cuentas de acceso remoto no utilizan directivas de contraseñas.
Sin proceso formal para cuentas inactivas	No dispone de un proceso formal para revisar cuentas de usuarios inactivas.
Creación de estaciones de trabajo sin planeación	Las estaciones de trabajo no se crean conforme a ninguna documentación ni simulación formal.
Software de cifrado de discos inexistente	No se utiliza ningún software de cifrado de discos en el entorno.
Sistema de alarma para intrusos inexistente	No se ha instalado ningún sistema de alarma para detectar ni informar de intrusiones.
No tienen ninguna identificación de control de entrada a la empresa	No están implementados tarjetas de identificación para empleados y visitantes, registros de visitantes y ningún control de entrada.
Los equipos de red no están en habitaciones seguras	Los equipos de la red no se hallan en ninguna habitación cerrada con acceso restringido.
Los servidores no están en habitaciones seguras	Los servidores no se hallan en ninguna habitación cerrada con acceso restringido.
Estaciones de trabajo sin protección	Las estaciones de trabajo no están protegidas con cables de seguridad.
Ordenadores portátiles sin protección	Los ordenadores portátiles no están protegidos con cables de seguridad.
No tienen equilibradores de carga	No se utilizan equilibradores de carga en el entorno.
No realizan pruebas de recuperación	No se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.
Sin control de contraseñas en las aplicaciones principales	La caducidad de las contraseñas no se controla en todas las aplicaciones principales.
No validan datos de entrada usuarios finales	No se validan los datos de entrada de los usuarios finales.
No validan datos de entrada aplicaciones	No se validan los datos de entrada de las aplicaciones del cliente.
Sin herramientas de prueba de seguridad	No utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad.

Sin cifrado de datos en aplicaciones	Las aplicaciones no cifran los datos cuando están almacenados o se están transmitiendo.
Sin modelo de asignación de niveles de gravedad a equipos	No se tiene ningún modelo para la asignación de niveles de gravedad a cada componente del entorno informático.
Sin encargado de la seguridad de la empresa	No se ha asignado a ningún empleado o área, la seguridad de la empresa.
Sin programas contra la divulgación de información	No existe ningún programa de divulgación de las medidas de seguridad en la empresa.

Fuente: Elaborado por los autores, Fuente: Msat, ver **ANEXO II -**

Msat_Alphatechnologies-Completo

La Tabla 2.10 muestra a continuación las vulnerabilidades encontradas que están asociadas a las amenazas descritas en la Tabla 2.7: Amenazas.

Tabla 2.20: Amenazas y vulnerabilidades.

Desastres naturales	
Amenaza	Vulnerabilidad
Fuego	<ul style="list-style-type: none"> Creación de estaciones de trabajo sin planeación
Daños por agua	
Desastres naturales	
<ul style="list-style-type: none"> De origen industrial 	
Amenaza	Vulnerabilidad
Avería de origen físico o lógico	<ul style="list-style-type: none"> Falta de proceso formal de mantenimiento de equipos
Corte de suministro eléctrico	<ul style="list-style-type: none"> Estaciones de trabajo sin protección
Condiciones inadecuadas de temperatura y/o humedad	<ul style="list-style-type: none"> Los equipos de red no están en habitaciones seguras
Desastres Industriales	<ul style="list-style-type: none"> Creación de estaciones de trabajo sin planeación
Contaminación mecánica	<ul style="list-style-type: none"> Los equipos de red no están en habitaciones seguras
	<ul style="list-style-type: none"> Los servidores no están en habitaciones seguras
Fallo de servicio de comunicaciones	<ul style="list-style-type: none"> Los equipos de red no están en habitaciones seguras
<ul style="list-style-type: none"> Errores o fallos no intencionados 	

Amenaza	<ul style="list-style-type: none"> • Vulnerabilidad
Errores de los usuarios	<ul style="list-style-type: none"> • Falta de proceso formal para revisión de privilegios de acceso
	<ul style="list-style-type: none"> • Sin protector de pantalla con contraseña
	<ul style="list-style-type: none"> • No se utilizan directivas de contraseñas
	<ul style="list-style-type: none"> • Usuarios con acceso administrativo
Alteración accidental de la información	<ul style="list-style-type: none"> • Sin encargado de la seguridad de la empresa
Destrucción de información	<ul style="list-style-type: none"> • Sin cifrado de datos en aplicaciones
	<ul style="list-style-type: none"> • sin modelo de asignación de niveles de gravedad a equipos
Fugas de Información	<ul style="list-style-type: none"> • Sin programas contra la divulgación de información
Errores del Administrador	<ul style="list-style-type: none"> • Sin herramientas de prueba de seguridad
	<ul style="list-style-type: none"> • Sin cifrado de datos en aplicaciones
Errores de mantenimiento /actualización de equipos (hardware)	<ul style="list-style-type: none"> • Sin modelo de asignación de niveles de gravedad a equipos
Vulnerabilidades de los programas (software)	<ul style="list-style-type: none"> • Sin herramientas de prueba de seguridad
Caída del sistema por agotamiento de recursos	<ul style="list-style-type: none"> • No tienen equilibradores de carga
	<ul style="list-style-type: none"> • Servidores sin antivirus
	<ul style="list-style-type: none"> • No realizan pruebas de recuperación
Errores de configuración	<ul style="list-style-type: none"> • Difusión del SSID activado
	<ul style="list-style-type: none"> • Sin control de contraseñas en las aplicaciones principales
Indisponibilidad del personal	<ul style="list-style-type: none"> • Sin encargado de la seguridad de la empresa
<ul style="list-style-type: none"> • Ataques intencionales 	
Amenaza	<ul style="list-style-type: none"> • Vulnerabilidad
Interceptación de información (escucha)	<ul style="list-style-type: none"> • Detección de protocolo SSL versión 2 y 3
	<ul style="list-style-type: none"> • El nivel de cifrado de servicios de terminal es medio o bajo

	<ul style="list-style-type: none"> • Divulgación de información remota por el DNS Caché Snooping
Modificación de la información	<ul style="list-style-type: none"> • Certificado auto-firmado SSL
	<ul style="list-style-type: none"> • Debilidad en el Servidor de protocolo de escritorio remoto de Microsoft Windows
	<ul style="list-style-type: none"> • Sin control de contraseñas en las aplicaciones principales
Destrucción la información	<ul style="list-style-type: none"> • No realizan pruebas de recuperación
Manipulación de programas	<ul style="list-style-type: none"> • Sin control de contraseñas en las aplicaciones principales
Divulgación de Información	<ul style="list-style-type: none"> • Sin programas contra la divulgación de información
	<ul style="list-style-type: none"> • Divulgación de información de transferencia de zona del servidor DNS (AXFR)
	<ul style="list-style-type: none"> • Divulgación de información del encabezado de Apache Server ETag
Manipulación de equipos	<ul style="list-style-type: none"> • Estaciones de trabajo sin protección
	<ul style="list-style-type: none"> • Ordenadores portátiles sin protección
Denegación de servicio	<ul style="list-style-type: none"> • Funciones de resolución del DNS, Desbordamiento remoto
	<ul style="list-style-type: none"> • No tienen equilibradores de carga
Ingeniería Social	<ul style="list-style-type: none"> • No tienen ninguna identificación de control de entrada a la empresa
	<ul style="list-style-type: none"> • Sistema de alarma para intrusos inexistente
Manipulación de la configuración	<ul style="list-style-type: none"> • Reenvío de IP habilitado
	<ul style="list-style-type: none"> • HTTP TRACE / TRACK Métodos permitidos
Suplantación de la Identidad del usuario	<ul style="list-style-type: none"> • No se utilizan directivas de contraseñas
	<ul style="list-style-type: none"> • No se tiene autenticación multifactorial para conexión remota a la red interna
	<ul style="list-style-type: none"> • Sin protector de pantalla con contraseña
	<ul style="list-style-type: none"> • Sin control de contraseñas en las aplicaciones principales

Abuso de privilegios de acceso	• Sin protector de pantalla con contraseña
	• Usuarios con acceso administrativo
Difusión de software dañino	• Servidores sin antivirus
	• Servidores de correo electrónico sin antivirus
	• Hosts del perímetro de red sin antivirus
Acceso no autorizado	• No se usa restricción MAC
	• Sin control de contraseñas en las aplicaciones principales
	• Usuarios con acceso administrativo

Fuente: Elaborado por los autores

2.3.4. Análisis del riesgo.

Se le llama riesgo a la medida del daño probable sobre un sistema. Al conocer el impacto de las amenazas que tienen sobre los activos y la probabilidad de ocurrencia se puede conocer el riesgo [11]. De esta manera el riesgo expone como afecta o daña a un activo si no es protegido de manera adecuada.

Tabla 2.11 presenta los resultados obtenidos al realizar el análisis del riesgo – Matriz de riesgo.

Tipo de amenaza	Amenaza	Vulnerabilidad	Probabilidad de la amenaza		Impacto			Impacto de la vulnerabilidad		Nivel de Riesgo		Id Riesgo
					Disponibilidad	Integridad	Confidencialidad					
Desastres Naturales	Fuego	Creación de estaciones de trabajo sin planeación	2,0	Poco frecuente	1	0	0	1	Bajo	2	Riesgo bajo	R1
	Daños por agua		2,0	Poco frecuente	1	0	0	1	Bajo	2	Riesgo bajo	R2
	Desastres naturales		2,0	Poco frecuente	1	0	0	1	Bajo	2	Riesgo bajo	R3
De origen industria	Avería de origen físico o lógico	Falta de proceso formal de mantenimiento de equipos	3,0	Normal	1	1	0	2	Medio	6	Riesgo medio	R4

Errores o fallos no intencionados	Corte de suministro eléctrico	Estaciones de trabajo sin protección	3,0	Normal	1	1	0	2	Medio	6	Riesgo medio	R5
	Condiciones inadecuadas de temperatura y/o humedad	Los equipos de red no están en habitaciones seguras	3,0	Normal	1	1	0	2	Medio	6	Riesgo medio	R6
	Desastres Industriales	Creación de estaciones de trabajo sin planeación	2,0	Poco frecuente	1	0	0	1	Bajo	2	Riesgo bajo	R7
	Contaminación mecánica	Los servidores no están en habitaciones seguras	5,0	Muy frecuente	1	0	0	1	Bajo	5	Riesgo medio	R8
		Los equipos de red no están en habitaciones seguras			1	0	0	1	Bajo	5	Riesgo medio	R9
	Fallo de servicio de comunicaciones	Los equipos de red no están en habitaciones seguras	2,0	Poco frecuente	1	1	0	3	Alto	6	Riesgo medio	R10
	Alteración accidental de la información	Sin encargado de la seguridad de la empresa	3,0	Normal	0	1	1	2	Medio	6	Riesgo medio	R11

	Errores de los usuarios	Falta de proceso formal para revisión de privilegios de acceso	4,0	Frecuente	0	0	1	1	Bajo	4	Riesgo medio	R12
		No se utilizan directivas de contraseñas			0	0	1	1	Bajo	4	Riesgo medio	R13
		Usuarios con acceso administrativo			0	1	1	2	Medio	8	Riesgo alto	R14
	Destrucción de información	Sin cifrado de datos en aplicaciones	3,0	Normal	1	1	1	3	Alto	9	Riesgo alto	R15
		sin modelo de asignación de niveles de gravedad a equipos			0	0	1	1	Bajo	3	Riesgo bajo	R16
	Fugas de Información	Sin programas contra la divulgación de información	3,0	Normal	0	1	1	2	Medio	6	Riesgo medio	R17
	Errores del Administrador	Sin herramientas de prueba de seguridad	4,0	Frecuente	1	1	1	3	Alto	12	Riesgo alto	R18
		Sin cifrado de datos en aplicaciones			0	1	1	2	Medio	8	Riesgo alto	R19

	Errores de mantenimiento /actualización de equipos (hardware)	Sin modelo de asignación de niveles de gravedad a equipos	4,0	Frecuente	1	0	0	1	Bajo	4	Riesgo medio	R20
	Vulnerabilidades de los programas (software)	Sin herramientas de prueba de seguridad	3,0	Normal	1	1	1	3	Alto	9	Riesgo alto	R21
	Caída del sistema por agotamiento de recursos	No tienen equilibradores de carga	4,0	Frecuente	1	1	0	2	Medio	8	Riesgo alto	R22
		Servidores sin antivirus			1	1	1	3	Alto	12	Riesgo alto	R23
		No realizan pruebas de recuperación			1	1	0	2	Medio	8	Riesgo alto	R24
	Errores de configuración	Difusión del SSID activado	4,0	Frecuente	1	0	1	2	Medio	8	Riesgo alto	R25
		Sin control de contraseñas en las aplicaciones principales			1	0	1	2	Medio	8	Riesgo alto	R26
	Indisponibilidad del personal	Sin encargado de la seguridad de la empresa	2,0	Poco frecuente	1	0	0	1	Bajo	2	Riesgo bajo	R27

Ataques intencionales	Interceptación de información (escucha)	Detección de protocolo SSL versión 2 y 3	3,0	Normal	0	1	1	2	Medio	6	Riesgo medio	R28
		El nivel de cifrado de servicios de terminal es medio o bajo			0	1	1	2	Medio	6	Riesgo medio	R29
		Divulgación de información remota por el DNS Caché Snooping			0	1	1	2	Medio	6	Riesgo medio	R30
	Modificación de la información	Certificado auto-firmado SSL	3,0	Normal	0	1	1	2	Medio	6	Riesgo medio	R31
		Debilidad en el Servidor de protocolo de escritorio remoto de Microsoft Windows			0	1	1	2	Medio	6	Riesgo medio	R32
		Sin control de contraseñas en las aplicaciones principales			0	1	1	2	Medio	6	Riesgo medio	R33
	Destrucción la información	No realizan pruebas de recuperación	3,0	Normal	1	1	1	3	Alto	9	Riesgo alto	R34

	Manipulación de programas	Sin control de contraseñas en las aplicaciones principales	3,0	Normal	0	1	1	2	Medio	6	Riesgo medio	R35
	Divulgación de Información	Sin programas contra la divulgación de información	3,0	Normal	0	1	1	2	Medio	6	Riesgo medio	R36
		Divulgación de información de transferencia de zona del servidor DNS (AXFR)			0	1	1	2	Medio	6	Riesgo medio	R37
		Divulgación de información del encabezado de Apache Server ETag			0	1	1	2	Medio	6	Riesgo medio	R38
	Manipulación de equipos	Estaciones de trabajo sin protección	3,0	Normal	1	1	1	3	Alto	9	Riesgo alto	R39
		Ordenadores portátiles sin protección			1	1	1	3	Alto	9	Riesgo alto	R40
	Denegación de servicio	Funciones de resolución del DNS, Desbordamiento remoto	2,0	Poco frecuente	1	0	1	2	Medio	4	Riesgo medio	R41
		No tienen equilibradores de carga			1	0	0	1	Bajo	2	Riesgo bajo	R42

	Ingeniería Social	No tienen ninguna identificación de control de entrada a la empresa	3,0	Normal	0	0	1	1	Bajo	3	Riesgo bajo	R43
		No tienen ninguna identificación de control de entrada a la empresa			0	0	1	1	Bajo	3	Riesgo bajo	R44
		Sistema de alarma para intrusos inexistente			0	0	1	1	Bajo	3	Riesgo bajo	R45
	Manipulación de la configuración	Reenvío de IP habilitado	3,0	Normal	1	0	1	2	Medio	6	Riesgo medio	R46
		HTTP TRACE / TRACK Métodos permitidos			1	0	1	2	Medio	6	Riesgo medio	R47
	Suplantación de la Identidad del usuario	No se utilizan directivas de contraseñas	2,0	Poco frecuente	0	1	1	2	Medio	4	Riesgo medio	R48
		No se tiene autenticación multifactorial para conexión remota a la red interna			0	1	1	2	Medio	4	Riesgo medio	R49
		Sin control de contraseñas en las aplicaciones principales			0	1	1	2	Medio	4	Riesgo medio	R50

	Abuso de privilegios de acceso	Usuarios con acceso administrativo	3,0	Normal	0	1	1	2	Medio	0	Riesgo medio	R51
	Difusión de software dañino	Servidores sin antivirus	2,0	Poco frecuente	1	1	1	3	Medio	6	Riesgo medio	R52
		Hosts del perímetro de red sin antivirus			1	0	1	2	Medio	4	Riesgo medio	R53
	Acceso no autorizado	No se usa restricción MAC	4,0	Frecuente	0	1	1	2	Medio	8	Riesgo alto	R54
		Sin control de contraseñas en las aplicaciones principales			0	1	1	2	Medio	8	Riesgo alto	R5
		Usuarios con acceso administrativo			0	1	1	2	Medio	8	Riesgo alto	R56

Fuente: Elaborado por los autores, ver **ANEXO VIII - Matriz de riesgos**

2.3.5. Análisis de Salvaguardias

Según Magerit un control o salvaguarda es una medida de protección para hacer frente a amenazas y de esta forma reducir el riesgo ocasionado por estas, las salvaguardas pueden establecerse a modo de políticas, procedimientos o soluciones de seguridad técnicas físicas o lógicas. [11]

En base a reuniones, entrevistas y documentación entregada por la organización se ha podido establecer controles ya implementados de seguridad sobre sus activos. De igual manera existen salvaguardias para los activos que son establecidas con las partes externas a la organización. En ciertos casos estos controles son llevados a cabo de manera informal, sin seguir una documentación y/o procedimientos establecidos. Por lo que estos controles no tienen un estudio sobre su efectividad en reducir la probabilidad del impacto de las amenazas, sin embargo, estos controles permiten tener una seguridad empírica sobre los activos.

A continuación, se detalla estos controles con su descripción en la organización.

Tabla 2.12: Controles implementados actualmente.

Controles Implementados	Descripción
Seguridad física	<ul style="list-style-type: none">- Se cuenta con un monitoreo por cámaras de vigilancia las 24 horas del día.- Un encargado de vigilar las cámaras
Control de acceso a archivos	<ul style="list-style-type: none">- Acceso a archivos por correo empresarial, ubicados en la nube y compartidos solo con el personal que lo requiere.
Almacenamiento restringido	<ul style="list-style-type: none">- Almacenamiento de certificados digitales en un servidor específico con acceso restringido.
Firewall	<ul style="list-style-type: none">- Protección perimetral para protección del tráfico no deseado hacia la organización, sin embargo, no revisa periódicamente
Proxy	<ul style="list-style-type: none">- Control sobre la navegación de los usuarios, sin embargo, no se revisa periódicamente.
Seguridad en red	<ul style="list-style-type: none">- Puntos de acceso separados por áreas- Control de acceso con clave de fuerte seguridad.
SLA con proveedores	<ul style="list-style-type: none">- Acuerdos con proveedores para garantizar el nivel de servicio.
Enlace secundario de salida a internet	<ul style="list-style-type: none">- Se encuentra separada la salida a internet de los usuarios con los principales servidores de la organización por enlaces diferentes.
Acuerdos de confidencialidad	<ul style="list-style-type: none">- Acuerdos con clientes y proveedores para garantizar la confidencialidad
Auditorías pedidas por terceros	<ul style="list-style-type: none">- Ciertos clientes solicitan auditorías a nivel administrativo.

Documentos firmados digitalmente	- La organización cuenta con firmas digitales para asegurar la integridad de los documentos de vital importancia para la organización. Las firmas son provistas por una entidad certificadora internacional
----------------------------------	---

Fuente: Elaborado por los autores.

2.3.5.1. Recomendación de controles

A continuación, se presentan los controles seleccionados de la Norma ISO 27002 según los riesgos definidos para realizar el tratamiento, cabe recalcar que este tratamiento del riesgo se lo realizará solo a los que tengan nivel alto en riesgo; estos controles nos ayudarán a prevenir, detectar y responder a los riesgos encontrados en el análisis (para el informe completo ver ANEXO IX - Valoración del riesgo).

Tabla 2.13: Selección de controles.

Amenaza	Vulnerabilidad	Nivel de Riesgo	Id Riesgo	Control Seleccionado
Errores de los usuarios	Usuarios con acceso administrativo	Riesgo alto	R14	8.1.2 Propiedad de los activos, 8.1.3 Uso aceptable de los activos, 8.2.2 Etiquetado y manipulado de la información, 9.4.1 Restricción del acceso a la información, 9.4.4 Uso de herramientas de administración de sistemas. y 16.1.3 Notificación de puntos débiles de la seguridad.
Destrucción de información	Sin cifrado de datos en aplicaciones	Riesgo alto	R15	12.5.1 Instalación del software en sistemas en producción, 14.2.1 Política de desarrollo seguro de software, 14.2.2 Procedimientos de control de cambios en los sistemas, 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas y 14.2.9 Pruebas de aceptación
Errores del Administrador	Sin herramientas de prueba de seguridad	Riesgo alto	R18	8.1.2 Propiedad de los activos, 8.1.3 Uso aceptable de los activos, 8.2.2 Etiquetado y manipulado de la información, 9.4.1 Restricción del acceso a la información, 9.4.4 Uso de herramientas de administración de sistemas. y 16.1.3 Notificación de puntos débiles de la seguridad.
	Sin cifrado de datos en aplicaciones	Riesgo alto	R19	A. 10.1.1 Política sobre el uso de controles criptográficos y A 10.1.2 Gestión de claves.

Vulnerabilidades de los programas (software)	Sin herramientas de prueba de seguridad	Riesgo alto	R21	12.5.1 Instalación del software en sistemas en producción, 14.2.1 Política de desarrollo seguro de software, 14.2.2 Procedimientos de control de cambios en los sistemas, 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas y 14.2.9 Pruebas de aceptación
Caída del sistema por agotamiento de recursos	No tienen equilibradores de carga	Riesgo alto	R22	11.1.4 Protección contra las amenazas externas y ambientales, 17.1.1 Planificación de la continuidad de la seguridad de la información, 17.1.2 Implantación de la continuidad de la seguridad de la información, 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información y 14.3.1 Protección de los datos utilizados en pruebas.
	Servidores sin antivirus	Riesgo alto	R23	11.2.4 Mantenimiento de los equipos, 18.2.1 Revisión independiente de la seguridad de la información, 16.1.3 Notificación de puntos débiles de la seguridad y 12.2.1 Controles contra el código malicioso
	No realizan pruebas de recuperación	Riesgo alto	R24	11.1.4 Protección contra las amenazas externas y ambientales, 17.1.1 Planificación de la continuidad de la seguridad de la información, 17.1.2 Implantación de la continuidad de la seguridad de la información, 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información y 14.3.1 Protección de los datos utilizados en pruebas.
Errores de configuración	Difusión del SSID activado	Riesgo alto	R25	Registros de navegación en Firewall y proxy
	Sin control de contraseñas en las aplicaciones principales	Riesgo alto	R26	12.5.1 Instalación del software en sistemas en producción, 14.2.1 Política de desarrollo seguro de software, 14.2.2 Procedimientos de control de cambios en los sistemas, 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas y 14.2.9 Pruebas de aceptación
Destrucción la información	No realizan pruebas de recuperación	Riesgo alto	R34	11.1.4 Protección contra las amenazas externas y ambientales, 17.1.1 Planificación de la continuidad de la seguridad de la información, 17.1.2 Implantación de la continuidad de la seguridad de la información, 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información y 14.3.1 Protección de los datos utilizados en pruebas.

Manipulación de equipos	Estaciones de trabajo sin protección	Riesgo alto	R39	14.2.6 Seguridad en entornos de desarrollo, 9.1.1 Política de control de accesos, 9.4.1 Restricción del acceso a la información, 9.4.3 Gestión de contraseñas de usuario, 11.1.3 Seguridad de oficinas, despachos y recursos
	Ordenadores portátiles sin protección	Riesgo alto	R40	14.2.6 Seguridad en entornos de desarrollo, 9.1.1 Política de control de accesos, 9.4.1 Restricción del acceso a la información, 9.4.3 Gestión de contraseñas de usuario, 11.1.3 Seguridad de oficinas, despachos y recursos
Acceso no autorizado	No se usa restricción MAC	Riesgo alto	R54	Registros de conexión en servidores, control de acceso a archivos
	Sin control de contraseñas en las aplicaciones principales	Riesgo alto	R55	
	Usuarios con acceso administrativo	Riesgo alto	R56	

Fuente: Elaborado por los autores.

Con toda la información que se obtuvo anteriormente se puede elaborar los diferentes documentos necesarios para el SGSI, como lo son las políticas y/o salvaguardas, que permitirán minimizar los riesgos encontrados, dichos documentos deberán ser aprobados por el jefe del área de tecnología de la empresa Alpha Technologies CIA.LTDA.

Tabla 2.14: Definición de políticas.

Controles Seleccionado	Políticas
8.1.2 Propiedad de los activos, 8.1.3 Uso aceptable de los activos, 8.2.2 Etiquetado y manipulado de la información, 9.4.1 Restricción del acceso a la información, 9.4.4 Uso de herramientas de administración de sistemas. y 16.1.3 Notificación de puntos débiles de la seguridad.	POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

12.5.1 Instalación del software en sistemas en producción, 14.2.1 Política de desarrollo seguro de software, 14.2.2 Procedimientos de control de cambios en los sistemas, 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas y 14.2.9 Pruebas de aceptación	POLÍTICA DE SEGURIDAD DE APLICACIONES WEB
A. 10.1.1 Política sobre el uso de controles criptográficos y A 10.1.2 Gestión de claves.	POLÍTICA DE CIFRADO ACEPTABLE
11.1.4 Protección contra las amenazas externas y ambientales, 17.1.1 Planificación de la continuidad de la seguridad de la información, 17.1.2 Implantación de la continuidad de la seguridad de la información, 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información y 14.3.1 Protección de los datos utilizados en pruebas.	POLÍTICA PARA LA RECUPERACIÓN DE DESASTRES
11.2.4 Mantenimiento de los equipos, 18.2.1 Revisión independiente de la seguridad de la información, 16.1.3 Notificación de puntos débiles de la seguridad y 12.2.1 Controles contra el código malicioso	POLÍTICA DE SEGURIDAD DEL SERVIDOR
14.2.6 Seguridad en entornos de desarrollo, 9.1.1 Política de control de accesos, 9.4.1 Restricción del acceso a la información, 9.4.3 Gestión de contraseñas de usuario, 11.1.3 Seguridad de oficinas, despachos y recursos	POLÍTICA DE SEGURIDAD DE LA ESTACIÓN DE TRABAJO

Fuente: Elaborado por los autores.

2.3.5.2. Evaluación de riesgo residual

Al tener definidas las salvaguardas y/o políticas, se aplicará a cada riesgo potencial y se calculará el riesgo residual. Esto se realizará para validar como la implementación de los controles y políticas propuestas disminuye el riesgo potencial que pueden afectar a la seguridad de la información dentro de la organización. En la Tabla 2.15 se muestra los riesgos seleccionados junto con en el control y/o política propuesto, cada riesgo ha

sido analizado en base a la efectividad de la implementación de un control de seguridad y se muestra como se reduce el nivel de riesgo de cada vulnerabilidad encontrada.

Tabla 2.15: Matriz de riesgo residual.

ID	Riesgo		Salvaguarda	Estado	Tipo	Efectividad	Probabilidad residual	Impacto residual	Riesgo residual	
R14	8	Alto	Política de uso aceptable de activos	Propuesto	Preventivo	L3	2	1	2	Bajo
R18	12	Alto		Propuesto	Preventivo	L3	2	1.5	3	Bajo
R15	9	Alto	Política de seguridad de aplicaciones web	Propuesto	Preventivo	L3	1,5	1,5	2,25	Bajo
R21	9	Alto		Propuesto	Preventivo	L3	1,5	1,5	2,25	Alto
R26	8	Alto		Propuesto	Correctivo	L3	2	1	3	Bajo
R19	8	Alto	Política de cifrado aceptable	Propuesto	Preventivo	L2	3	1,5	4.5	Medio
R22	8	Alto	Procedimiento para la recuperación de desastres	Propuesto	Preventivo	L3	2	1	2	Bajo
R24	8	Alto		Propuesto	Correctivo	L3	2	1	2	Bajo
R34	8	Alto		Propuesto	Preventivo	L3	1,5	1,5	2,25	Bajo
R23	12	Alto	Política de seguridad del servidor	Propuesto	Preventivo	L3	2	1.5	3	Muy Bajo
R25	8	Alto	Registros de navegación en Firewall y proxy	Implementado	Correctivo	L4	1	0.5	0.5	Bajo
R39	9	Alto	Política de seguridad de la estación de trabajo	Propuesto	Preventivo	L3	1,5	1,5	2.25	Bajo
R40	9	Alto		Propuesto	Correctivo	L3	1,5	1,5	2.25	Bajo
R54	8	Alto	Registros de conexión en servidores, control de acceso a archivos	Implementado	Preventivo	L4	1	0.5	0.5	Bajo
R55	8	Alto		Implementado	Correctivo	L4	1	0.5	0.5	Bajo
R56	8	Alto		Implementado	Correctivo	L4	1	0.5	0.5	Bajo

Fuente: Elaborado por los autores.

2.3.5.3. Declaración de aplicabilidad

El documento donde se define la declaración de la aplicabilidad es de suma importancia para la implementación del sistema de gestión de la seguridad de la información (SGSI), el cual contiene los siguientes puntos:

- Controles implementados actualmente.
- Controles seleccionados que serán implementados.
- Controles que serán excluidos.

Este importante documento permitirá al encargado que implementara el SGSI a validar si los controles definidos están siendo aplicados de manera correcta. Ver **ANEXO X - Declaración de Aplicabilidad**.

3. RESULTADOS Y DISCUSIÓN

3.1. Plan de Gestión de Seguridad de la Información

El presente plan de gestión de la seguridad de la información estará conformado de acuerdo con las necesidades de la empresa Alpha Technologies CIA. LTDA., tomando en cuenta toda la información recolectada en los capítulos anteriores y usando la norma NTE INEN ISO/IEC 27001:2011.

El Sistema de Gestión de la Seguridad de la información (SGSI) es el diseño, la implementación y el mantenimiento de un conjunto de procesos para una administración eficiente de la información, para asegurar la disponibilidad, la integridad y la confidencialidad, mitigando los riesgos encontrados. La norma ISO 27001 incluye un modelo para el desarrollo y mantenimiento para un SGSI, el cual es el ciclo de Deming, como se sabe consiste en planificar, hacer, verificar y actuar (PHVA) o en inglés plan, do, check, act (PDCA), este modelo puede ser aplicado a todos los procesos del SGSI. La Figura 3.1 muestra el modelo PDCA aplicado a los procesos del SGSI [12].

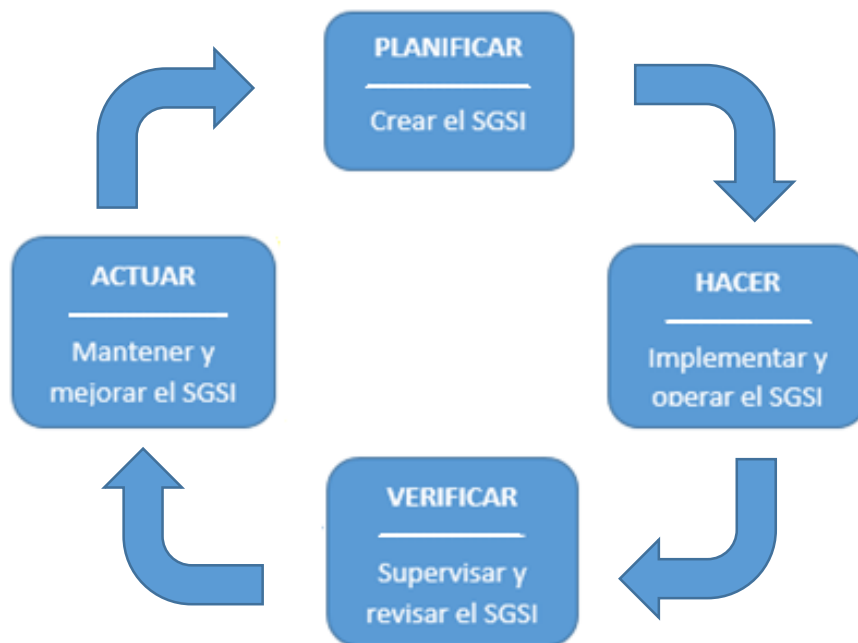


Figura 3.1: Modelo PDCA aplicado a los procesos del SGSI.

Fuente: Elaborado por los autores en bases a NTE-ISO-IEC 27001-2011.

- **Planificar (Plan) [crear el SGSI]**: Se debe establecer las políticas, objetivos, procesos y procedimientos del SGSI asociados a la gestión del riesgo y de esta manera mejorar la seguridad de la información de la empresa [12].
- **Hacer (Do) [implementar y operar el SGSI]**: Se debe Implementar y gestionar el SGSI según sus políticas, controles, procesos y procedimientos seleccionados en la planificación [12].
- **Verificar (Check) [supervisar y revisar el SGSI]**: Se debe verificar, supervisar y revisar las prestaciones de los procesos del SGSI, comprobando que las medidas implementadas surten efecto, para realizarlo se tiene que volver a recolectar datos y monitorizar el comportamiento del sistema [12].
- **Actuar (Act) [mantener y mejorar el SGSI]**: En base a los resultados de la auditoría del SGSI se debe adoptar acciones correctivas y preventivas con el objetivo de mejorar el SGSI. Si el funcionamiento ha sido el esperado, se instalarán de manera definitiva las modificaciones en el sistema [12].

3.2. Alcance y Limites de SGSI

El alcance del presente plan de gestión de seguridad de la información para la empresa Alpha Technologies CIA. LTDA., se definió junto con el área de tecnología de la empresa, en donde se realiza el análisis de los activos considerados como crítico (servidores: Firewall, Proxy, Directorio activo, Pivote de conexión, certificados VPN, Certificados digitales-almacenamiento) y en cuento a lo que se refiere a la infraestructura tecnológica de la empresa se evaluó el área de Tecnología.

En el presente proyecto se excluirán:

- La evaluación en el sitio de la infraestructura de Hosting que posee la empresa.
- La evaluación en el sitio de la infraestructura tecnológica de los proveedores externos.

Cabe recalcar que en el presente proyecto de titulación se llevará acabo únicamente la etapa de planificación (PLAN).

3.3. Elaboración del Plan de Gestión de Seguridad de la Información.

En el presente proyecto de titulación se llevará acabo únicamente la etapa de planificación (PLAN), ya que en el alcance no se especifica la realización de las siguientes etapas (hacer, verificar y actuar).

En la etapa de planificación se debe establecer políticas, objetivos, procesos y procedimientos del SGSI asociados a la gestión del riesgo y de esta manera mejorar la seguridad de la información de la empresa [12], por lo tanto esta etapa contiene 5 fases en donde se debe ir generando la documentación necesaria para llevar acabo el Sistema de Gestión de la Seguridad de la Información (SGSI). La Figura 3.1 muestra las 5 fases de la etapa de planificación según la ISO/IEC 27003.

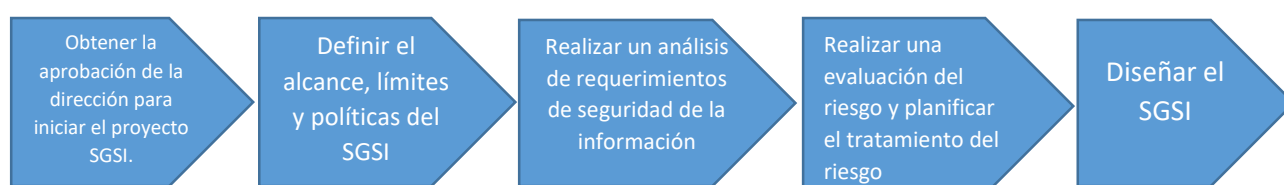


Figura 3.2: Fases de la etapa de planificación [13].

Fuente: Elaborado por los autores en bases a la ISO-IEC 27003

La Tabla 3.1 muestra las 5 fases con sus principales documentos de salida y la documentación generada en todo el proyecto de titulación.

Tabla 3.1: Fases y Documentación del Plan de Seguridad de la Información.

Fase	Objetivo	Documentación establecida por la ISO 27001	Documentación generada en el proyecto de titulación
Aprobación por parte de la dirección para iniciar el proyecto SGSI	Obtener la aprobación y el compromiso de la organización para iniciar el proyecto de SGSI.	<ul style="list-style-type: none"> • Aprobación de la dirección para la iniciación del Proyecto de SGSI. 	Aprobación por parte de la entidad.
Definición del alcance, límite y políticas del SGSI.	Definir el alcance, los límites y políticas del SGSI	<ul style="list-style-type: none"> • El alcance y los límites del SGSI. • Políticas del SGSI 	<ul style="list-style-type: none"> • Documento – Proyecto integrador - Plan de trabajo de titulación. • Sección 3.2 Alcance y Límites del SGSI • Anexo P1 al P15 – Políticas del SGSI.
Realizar el análisis de requerimientos de seguridad de la información.	Definir los requerimientos adecuados para el SGSI. Reconocer los activos de Información. Obtener el estado actual de la empresa en cuanto a la seguridad de la información.	<ul style="list-style-type: none"> • Requerimientos de seguridad de la información. • Activos. • Resultados del estado actual de la evaluación de la seguridad de la información 	<ul style="list-style-type: none"> • Sección 1.4.4. Departamento de Tecnología (TIC). • Sección 1.6. Situación actual de la seguridad de la información en la empresa Alpha Technologies CIA. LTDA. • ANEXO II - Msat_Alphatechnologies-Completo. • ANEXO III - Auditoria Check List NTE INEN-ISO-IEC 27001-2011 - Manejo de Seguridad de la Información. • ANEXO IV - Análisis del Estado de Cumplimiento Actual. • Sección 2.3 .Evaluación de riesgos según la metodología MAGERIT – Paso 2: Identificación de Amenazas. • Sección 2.3 .Evaluación de riesgos según la metodología MAGERIT – Paso 3: Identificación de vulnerabilidades. • ANEXO V - Identificación de Amenazas • ANEXO VI – Escaneo de Vulnerabilidades con las herramientas Nmap y Nessus. • ANEXO VII – Análisis de Vulnerabilidades. • Sección 2.3 .Evaluación de riesgos según la metodología MAGERIT – Paso 4: Análisis de riesgo. • ANEXO VIII - Matriz de riesgos • ANEXO IX - Valoración del riesgo. • ANEXO X - Declaración de Aplicabilidad

Fuente: Elaborado por los autores en base a la ISO/IEC 27003.

<p>Realizar la evaluación del riesgo y planificar el Tratamiento del Riesgo.</p>	<p>Definir la metodología que se usara para la evaluación de riesgo. Identificar, analizar y evaluar los riesgos. Seleccionar los tratamientos del riesgo y los controles.</p>	<ul style="list-style-type: none"> • Aprobación por parte de la dirección para la implementación del SGSI. • Plan del tratamiento de riesgo. • Declaración de aplicabilidad, en donde se incluyen los objetivos y los controles seleccionados. 	<ul style="list-style-type: none"> • El presente proyecto de titulación solo contempla la fase de planificación del SGSI. • Sección 2.3.5.1 Recomendación de controles. • ANEXO IX - Valoración del riesgo. • ANEXO X - Declaración de Aplicabilidad • ANEXO XI - Análisis del Estado de Cumplimiento Esperado
<p>Diseñar el SGSI.</p>	<p>Terminar el plan del SGSI a través del diseño de la seguridad dentro de la empresa.</p>	<ul style="list-style-type: none"> • Plan final de implementación del proyecto SGSI. 	<ul style="list-style-type: none"> • Sección 3.4 Guía de Implementación. • Sección 3.5 Aplicabilidad de la propuesta

En la etapa de planeación la norma ISO/IEC 27001 establece la elaboración de documentos adicionales los cuales son:

- Documento para el procedimiento de control de documentos y registros. (ver **ANEXO P1 – Guía para control de documentos**)
- Documento Política del SGSI (ver **ANEXO P2 - Política de SGSI**)
- Documento declaración de Aplicabilidad (ver **Anexo VIII – Declaración de Aplicabilidad**)

Adicionalmente, una vez que se ha determinado los controles a implementarse para poder disminuir el riesgo que afecte a la organización, se debe elaborar documentos que complementaran el plan de gestión de seguridad de la información, estos documentos son parte de los entregables de este proyecto y son los siguientes:

- ANEXO P3- Política Uso aceptable de los activos
- ANEXO P4 - Procedimiento para la recuperación de desastres
- ANEXO P5 - Política de seguridad de la estación de trabajo
- ANEXO P6- Política de seguridad de aplicaciones web
- ANEXO P7 -Política de seguridad del servidor
- ANEXO P8- Política de cifrado aceptable

3.4. Guía de Implementación

Después de tener elaborados todos los entregables del proyecto, se va a realizar la guía de implementación del plan del Sistema de Gestión de la Seguridad de la información (SGSI), esta guía tendrá una secuencia de actividades que se tendrán que realizar en el caso que se disponga a la implementación del SGSI.

Tabla 3.2: Guía del SGSI

Actividad	Descripción	Entregable
Aprobación de la empresa para comenzar el proyecto SGSI.	Obtener aprobación de la Dirección de la empresa para comenzar el proyecto de SGSI.	Documento - Aprobación por parte de la empresa.
Definición del Alcance y los Límites del proyecto SGSI.	Definir el alcance y los límites del SGSI que se realizará.	Sección 3.2 Alcance y límites de SGSI.
Análisis de la situación actual de la seguridad de la información en la empresa.	Conocer el estado actual en el que se encuentra la empresa con respecto a la seguridad de la información.	Sección 1.6 Situación actual de la seguridad de la información.

Identificación de activos críticos de la empresa.	Selección de activos críticos.	Documento – Activos Críticos
Análisis y evaluación de riesgos	Selección y aplicación de la metodología de análisis y evaluación de riesgos (Magerit)	Sección 2.3 Evaluación de riesgos según la metodología MAGERIT
Documentos	<p>Elaboración de documentos necesarios para el tratamiento de riesgo:</p> <ul style="list-style-type: none"> • Guía de control de documentos. • Políticas. • Declaración de aplicabilidad. 	<p>ANEXO P1 – Guía para control de documentos.</p> <p>ANEXO P2 - Política de SGSI.</p> <p>ANEXO P3- Política Uso aceptable de los activos.</p> <p>ANEXO P4 - Procedimiento para la recuperación de desastres.</p> <p>ANEXO P5 - Política de seguridad de la estación de trabajo.</p> <p>ANEXO P6- Política de seguridad de aplicaciones web.</p> <p>ANEXO P7 -Política de seguridad del servidor.</p> <p>ANEXO P8- Política de cifrado aceptable.</p> <p>ANEXO VIII - Declaración de Aplicabilidad.</p> <p>ANEXO IX - Valoración del riesgo</p> <p>ANEXO XI - Análisis del Estado de Cumplimiento Esperado</p>
Implementación de políticas	Implementación de los controles seleccionados.	No aplica
Capacitación de los empleados	Capacitación a todos los empleados para realizar una correcta ejecución de los controles seleccionados que serán implementados.	No aplica

Fuente: Elaborado por los autores en base a la ISO/IEC 27003.

3.5. Aplicabilidad de la propuesta

Para tener evidencia sobre la mejora que se presentaría en cuanto a la seguridad de la información en relación a la ISO 27001 en la empresa Alpha Technologies CIA.LTDA, después que se implementen las políticas y/o controles seleccionados de acuerdo a la evaluación de riesgos vista en la sección 2.3 Evaluación de riesgos según la metodología MAGERIT, se calcula el porcentaje para el nivel de cumplimiento esperado, presentando a continuación como resultado la Tabla 0.1 (ver **ANEXO XI - Estado de Cumplimiento Esperado** presenta los resultados para cada dominio):

Tabla 0.1: Estado de Cumplimiento Esperado

Dominio	% Cumple	% Cumple Parcialmente	% No Cumple
A.5 Políticas de Seguridad	100%	0%	0%
A.6 Aspectos organizativos de la Seguridad de la Información	64%	36%	0%
A.7 Gestión de activos	60%	40%	0%
A.8 Seguridad ligada a los Recursos Humanos	22%	67%	11%
A.9 Seguridad Física y Ambiental	54%	23%	23%
A.10 Gestión de Comunicaciones y Operaciones	37%	22%	41%
A.11 Control de acceso	76%	20%	4%
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	56%	38%	6%
A.13 Gestión de incidentes en la Seguridad de la Información	60%	0%	40%
A.14 Gestión de la Continuidad del Negocio	100%	0%	0%
A.15 Cumplimiento	40%	20%	40%

Fuente: Elaborado por los autores

A continuación, en la Tabla 3.4 se mostrará el cambio entre el porcentaje del estado de cumplimiento actual y el porcentaje del estado de cumplimiento actual como el del nivel de cumplimiento esperado.

Tabla 0.4: Comparación del cumplimiento actual y el cumplimiento esperado

Dominio	Estado de cumplimiento actual	Estado de Cumplimiento Esperado
A.5 Políticas de Seguridad	0%	100%
A.6 Aspectos organizativos de la Seguridad de la Información	46%	64%
A.7 Gestión de activos	0%	60%
A.8 Seguridad ligada a los Recursos Humanos	22%	22%
A.9 Seguridad Física y Ambiental	23%	56%
A.10 Gestión de Comunicaciones y Operaciones	19%	37%
A.11 Control de acceso	40%	76%
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información	44%	56%
A.13 Gestión de incidentes en la Seguridad de la Información	0%	60%
A.14 Gestión de la Continuidad del Negocio	0%	100%
A.15 Cumplimiento	20%	40%

Fuente: Elaborado por los autores

Como se puede observar en la tabla 3.4, la mayoría de los dominios incrementaron su nivel de cumplimiento considerablemente, esto se debe a que los objetivos de control y sus controles están directamente relacionados con los resultados del análisis de riesgo de los activos críticos de empresa; mientras que otros dominios presentan poco incremento ya que no están relacionados de manera directa con el análisis.

De esta manera se puede observar que la implementación de los controles seleccionados ayudó al estado de cumplimiento de la empresa, el cual en un principio la mayoría tenía un porcentaje bajo de cumplimiento.

Cabe recalcar que este plan de Gestión de la Seguridad de la Información tiene un tiempo de validez de un año, ya que pasado ese tiempo pueden existir más vulnerabilidades y amenazas o las ya existentes pueden cambiar y llegar a tener un nivel de riesgo alto. De esta manera se recomienda realizar un nuevo análisis de riesgo cada año dentro de la empresa AlphaTechnologies CIA.LTDA.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Con base al análisis realizado se pudo determinar que la empresa Alphatechnologies CIA. LTDA. posee controles de seguridad que ayudan a la gestión de la seguridad de la información, sin embargo, la gran mayoría de estos no se encontraban siguiendo un proceso y/o política formal. Estos controles fueron tomados en cuenta en el estado del cumplimiento actual respecto a la norma ISO/IEC 27001 tomándolos como “cumple parcialmente”.
- Alphatechnologies CIA. LTDA. al ser una empresa de seguridad informática posee software que ayudan a la mitigación de amenazas a la seguridad de la información, los mismos que son los principales productos ofrecidos a sus clientes por lo que el análisis de estos softwares fueron de gran importancia para poder tomar medidas correctivas sobre los mismos.
- En el análisis de riesgo se pudo apreciar que algunas de las vulnerabilidades presentadas se debían a que la empresa a pesar de tener varios mecanismos de seguridad de la información como por ejemplo registros tanto en proxy como en firewall, estos no eran usados correctamente y no daban un seguimiento adecuado. Por lo que en gran parte la asignación y concientización de roles y responsabilidades debería ser una prioridad para que luego se realice una correcta implementación de las mejoras propuestas en este SGSI.
- El estado de cumplimiento esperado respecto al estado de cumplimiento actual de la empresa presenta una mejora significativa para la misma, una vez sean implementados los controles puestos en este SGSI. Esto implicara para la empresa un nivel nuevo de prestigio en seguridad de la información complementaria a la seguridad informática que ya posee.
- Al término de este documento elaborado por los autores la empresa Alphatechnologies CIA. LTDA se encontraba en un proceso de reestructuración organizacional por lo que los resultados de este documento serán de gran ayuda para el nuevo personal que esté a cargo.

4.2. Recomendaciones

- Ya que la empresa Alphatechnologies CIA. LTDA. se encuentra en un proceso de reestructuración organizacional, se recomendaría realizar como parte de este proceso la implementación de los controles y políticas propuestos en este plan de Gestión de la Seguridad de la Información y junto con esto definir

responsables de seguridad de la información, así como también establecer el compromiso de la gerencia para dar seguimiento a esta implementación.

- Realizar un levantamiento formal de los controles actuales que se tienen en la organización de manera que se definan procedimientos, responsables, alcance, etc. Para que estos controles no se realicen de forma empírica o por una sola necesidad, sino que sean algo constante y de conocimiento de todo el personal.
- Ya que las políticas y controles propuestos como parte del SGSI se encuentran establecidos en base al análisis realizado a los activos críticos, se recomienda realizar un análisis en donde se pueda establecer un mayor nivel de vulnerabilidades para levantar nuevas políticas que ayuden a mejorar la seguridad de la información
- Realizar periódicamente una revisión de los controles y políticas implementadas y propuestas para determinar si están cumplimiento según lo acordado. Además, también poder definir mejoras que puedan ser modificadas tanto en los procedimientos, así como en los documentos guías que se tengan habilitados.
- Establecer planes calendarizados de concientización dirigidos a todo el personal de la empresa, en donde se cuente con la participación de la gerencia como ejemplo y apoyo del cumplimiento de la seguridad de la información, correcto uso de los recursos, compromiso y divulgación de lo acordado en el SGSI.

5. BIBLIOGRAFÍA

- [1] A. F. González, «PublicTIC,» 08 12 2015. [En línea]. Available: deusto.es/master-informatica/la-informacion-en-las-empresas/. [Último acceso: 16 08 2018].
- [2] M. I. CARLOS FERNÁNDEZ APEN, «APEN,» [En línea]. Available: <https://apen.es/2016/06/20/la-seguridad-de-la-informacion-de-una-empresa/>. [Último acceso: 16 08 2018].
- [3] J. d. Proyectos., Interviewee, Primera entrevista- Conociendo la empresa y solicitud de auspicio.. [Entrevista]. 2018.
- [4] INEN, «NTE INEN-ISO/IEC 27001:2011 Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos,» 2012.
- [5] R. S. J. López Neira A., «ISO 27000.es,» 2012. [En línea]. Available: <http://www.iso27000.es/sgsi.html>.
- [6] C. W. L. M. M. C. Bayona Sussy, «Implementación de la NTP ISO/IEC 27001 en las Instituciones Publicas:Caso de Estudio,» Unidad de Posgrado de la Facultad

de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, 2015.

- [7] ISACA, «<http://www.isaca.org/>,» [En línea]. Available: <http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Launches-Risk-IT-Framework-to-Help-Organizations-Balance-Risk-with-Profit-Spanish.aspx>. [Último acceso: 01 01 2020].
- [8] C. R. B. Helena Alemán Novoa, «<http://hemeroteca.unad.edu.co/>,» 2015. [En línea]. Available: <http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874>. [Último acceso: 01 01 2020].
- [9] M. Corporation., Microsoft Security Assessment Tool - User Guide, Microsoft Corporation. All Rights Reserved., 2008.
- [10] Microsoft, «docs.microsoft.com,» 11 10 2017. [En línea]. Available: <https://docs.microsoft.com/es-es/security-updates/security/technetsecurityherramientadeevaluaciondeseguridaddemicrosoftmsat>. [Último acceso: 20 01 2020].
- [11] Consejo Superior de Administración Electrónica, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método,» Madrid, 2012.
- [12] «pmg-ssi,» [En línea]. Available: <https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/>. [Último acceso: 10 02 2020].
- [13] «nanopdf,» NANOPDF Inc., 10 02 2018. [En línea]. Available: https://nanopdf.com/download/seguridad-de-la-informacion-iso-27003-v2_pdf. [Último acceso: 10 02 2020].
- [14] «alphaside,» Alpha Technologies, [En línea]. Available: <https://www.alphaside.com/>. [Último acceso: 08 01 2020].
- [15] Instituto Ecuatoriano de Normalización- INEN, «NTE INEN-ISO/IEC 27001:2011 TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) - REQUISITOS,» Quito.
- [16] Consejo Superior de Administración Electrónica, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos,» Madrid, 2012.

ANEXOS

Documento - Aprobación por parte de la entidad.

Documento – PlanificacionDeActividades.

ANEXO A - ANEXO A - Activos principales de información Alphatechnologies.
Carpeta - Escaneo de Vulnerabilidades con Nessus y Nmap.
ANEXO I -Msat_Alphatechnologies-resumidoANEXO II - Resultado de Medidas de Defensa MSAT.
ANEXO II - Msat_Alphatechnologies-Completo27001-2011 Auditoría Check List.
ANEXO III Auditoria Check List NTE INEN-ISO-IEC 27001-2011 - Manejo de Seguridad de la Información.
ANEXO IV - Análisis del Estado de Cumplimiento Actual.
ANEXO V - Identificación de Amenazas.
ANEXO VI – Escaneo de Vulnerabilidades con las herramientas Nmap y Nessus.
ANEXO VII – Análisis de Vulnerabilidades.
ANEXO VIII - Matriz de riesgos.
ANEXO IX - Valoración del riesgo.
ANEXO X - Declaración de Aplicabilidad.
ANEXO XI - Análisis del Estado de Cumplimiento Esperado
ANEXO P1 - Guía para control de documentos.
ANEXO P2 - Política de SGSI.
ANEXO P3- Política Uso aceptable de los activos.
ANEXO P4 - Procedimiento para la recuperación de desastres.
ANEXO P5 - Política de seguridad de la estación de trabajo
ANEXO P6- Política de seguridad de aplicaciones web.
ANEXO P7 -Política de seguridad del servidor.
ANEXO P8- Política de cifrado aceptable.