EXPERTEC

SERVICIOS Y SOLUCIONES INFORMÁTICAS

Elaboración del plan director de implementación del SGSI basado en la ISO/IEC27001 para una empresa de Servicios y Soluciones Informáticas.

Nombre Estudiante: William Alexander Ortiz Jiménez

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: Mayo de 2021

Dedicatoria

Este trabajo final es dedicado primeramente a Dios por brindarme la salud, vida y protección para poder finalizar este gran triunfo.

A mi familia y mis seres queridos que me han apoyado en todo momento para poder culminar con éxito este gran proyecto.

Quiero dedicar de forma muy especial a mi gran amor Alejandra quien me acompaño en todo este proceso con su comprensión, cariño y apoyo incondicional. Eres una mujer muy luchadora y que logra alcanzar lo que sueña. Para ti mi gran respeto y admiración.

A mi mami Doris, quien me ha inspirado para seguir adelante y alcanzar todas mis metas y en espera de muchas más.

A mi angelito Chispita que me acompaña en el cielo y quien me acompaño durante todos los días y las noches brindándome su cariño y ternura.

Igualmente a mi príncipe Tobías que también me acompaño y me brindo su amor y su ternura para poder realizar este gran logro.

Y a todas las personas que de una u otra forma permitieron que este proyecto se volviera realidad mis más sinceros agradecimientos.

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Elaboración del plan director de implementación del SGSI basado en la ISO/IEC27001 para una empresa de Servicios y Soluciones Informáticas.*
Nombre del autor:	*William Alexander Ortiz Jiménez*
Nombre del consultor/a:	*Antonio Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	Mayo/2021
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave:	*Plan, ISO/IEC27001, ISO/IEC27002, SGSI, CMM, DAFO, MAGERIT, análisis, riesgos, impacto, mitigar.*

Resumen del Trabajo:

El presente Trabajo Final de Master tiene como propósito presentar la implementación del Sistema de Gestión de la Seguridad de la Información de la empresa de servicios y soluciones informáticas EXPERTEC ubicada en Colombia en el Departamento del Cauca en la ciudad de Popayán, basado en la norma ISO/IEC 27001 y los controles del estándar ISO/IEC 27002 referente a las buenas prácticas.

Para la implementación del SGSI se estableció diferentes etapas iniciando con un análisis DAFO para contextualizar y comprender la situación actual de la empresa en referencia al ámbito de la seguridad de la información, posterior se realizó un análisis diferencial de la empresa para evaluar la norma ISO/IEC 27001 y los controles de la norma ISO/IEC 27002 en su estado inicial; así mismo, se establecieron los documentos para el cumplimiento normativo de la implementación del SGSI. Por otra parte, se utilizó la metodología de análisis y gestión de riesgos MAGERIT para orientar a la empresa en la gestión de riesgos a los que está expuesta la empresa. Una vez definido el análisis y gestión de riesgos se establecieron propuestas de proyectos para implementar mejoras y medidas de control adecuadas que permitan mitigar los riesgos encontrados. Finalizando las etapas, se estableció un proceso de auditoría para analizar el nivel de capacidad de madurez en la que avanzo el SGSI después de implementar las propuestas de proyectos planteados junto con los

resultados obtenidos.

Abstract:

The purpose of this Master's Final Project is to present the implementation of the Information Security Management System of the IT services and solutions company EXPERTEC located in Colombia in the Department of Cauca in the city of Popayán, based on the ISO/IEC 27001 standard and the controls of the ISO/IEC 27002 standard referring to good practices.

For the implementation of the ISMS, different stages were established, starting with a SWOT analysis to contextualize and understand the current situation of the company in reference to the field of information security, followed by a differential analysis of the company to evaluate the ISO/IEC 27001 standard and the controls of the ISO/IEC 27002 standard in its initial state; likewise, the documents for the regulatory compliance of the implementation of the ISMS were established. On the other hand, the MAGERIT risk analysis and management methodology was used to guide the company in managing the risks to which the company is exposed. Once the risk analysis and management was defined, project proposals were established to implement improvements and adequate control measures to mitigate the risks found. At the end of the stages, an audit process was established to analyze the level of maturity of the ISMS after implementing the project proposals and the results obtained.

Índice

Lista de Ilustraciones

Lista de Tablas

1. Introducción

1.1 Conociendo la norma ISO/IEC 27001 y la norma ISO/IEC 27002

La norma ISO/IEC 27001 fue publicada en el 2005 siendo una adaptación de la norma BS 7799-2 [1]. Esta norma proporciona los requisitos o disposiciones para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Su utilización permite a las organizaciones o entidades gestionar la seguridad de los activos, la evaluación de los riesgos y la aplicación de los controles necesarios para mitigar y eliminar los riesgos.

La norma cuenta con una estructura [2] para cumplir con los requisitos o disposiciones establecidos de la siguiente manera:

1) Objeto y campo de aplicación: orientaciones sobre la aplicabilidad y uso de la norma.
2) Referencias normativas: referencia de documentos normativos para la aplicación de la norma y la metodología PDCA.
3) Términos y definiciones: establecimiento de términos y definiciones referentes a la seguridad de la información y a la aplicación de la norma.
4) Contexto de la organización: conocimiento de la organización y el contexto como punto de referencia en la aplicación del SGSI.
5) Liderazgo: compromisos adquiridos por la dirección de la organización para la implantación y cumplimiento del SGSI.
6) Planificación: planeación para definir los activos a proteger y las acciones a realizar para mitigar y prevenir los riesgos.
7) Soporte: disponer con los recursos para implementar la planificación
8) Operación: seguimiento, control y ejecución de los planes de tratamiento de riesgos.
9) Evaluación del desempeño: auditorias y revisión para evaluar el desempeño de las acciones realizadas.
10) Mejora: actualización permanente del sistema de gestión para definir oportunidades de mejora.

La norma ISO/IEC 27002 fue publicada en 2007 y renombra la norma ISO 17799:2005 [1]. Esta norma es una guía de buenas prácticas para la seguridad de la información mediante la implementación de controles de seguridad. La norma no es certificable.

Esta norma contiene 114 controles, 35 objetivos de control y 14 dominios o capítulos organizados en la siguiente tabla:

Tabla 1 – Dominios, objetivos de control y controles norma ISO/IEC 27002

Dominios	Objetivos de control/Controles
A.5 Políticas de seguridad de la información	1/2
A.6 Organización de la seguridad de la información	2/7

A.7 Seguridad de los recursos humanos	3/6
A.8 Gestión de activos	3/10
A.9 Control de acceso	4/14
A.10 Criptografía	1/2
A.11 Seguridad física y del entorno	2/15
A.12 Seguridad de las operaciones	7/14
A.13 Seguridad de las comunicaciones	2/7
A.14 Adquisición, desarrollo y mantenimientos de sistemas	3/13
A.15 Relación con los proveedores	2/5
A.16 Gestión de incidentes de seguridad de la información	1/7
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	2/4
A.18 Cumplimiento	2/8

1.2 Contexto y Justificación

Para la realización del TFM se ha escogido una empresa pequeña clasificada según la ley de Colombia 590 del 2000 como MiPyme ubicada en el Departamento de Cauca en la ciudad de Popayán. Esta empresa ofrece servicios y soluciones de implementación y configuración de redes estructuradas, implementación y configuración de servidores con múltiples plataformas y servicios, desarrollo de software y aplicaciones móviles, soporte técnico a empresas y organizaciones tanto en software como en hardware de los distintos dispositivos de cómputo.

La empresa dispone de 9 empleados y dentro de su organigrama está conformada por las siguientes áreas, personas y relaciones entre las partes:

- Director Ejecutivo (CEO): Representante legal de la empresa.
- Director de Finanzas (CFO): Encargado de la planificación financiera, revisar el estado financiero de la empresa, realizar presupuestos, proyecciones e inversiones y colabora en la toma de decisiones junto con el Director Ejecutivo.
- Director de Tecnología o jefe de tecnología (CTO): Encargado de establecer estrategias de alineación de las Tecnologías de la Información con las diferentes áreas y partes de la empresa. Además supervisa y controla las áreas relacionadas con los servicios que ofrece la empresa. Cada área tiene asignado un jefe o responsable:
    - Jefe de Redes Estructuradas y Servidores: Responsable de los servicios de instalación, implementación y gestión de redes estructuradas y administración de servidores.
    - Jefe de desarrollo de software: Responsable de gestionar y supervisar proyectos y servicios relacionados con el desarrollo de software.

    - Jefe de soporte técnico: Responsable de supervisar y monitorear servicios y procesos relacionados con el soporte técnico.
- Director de Marketing (CMO): Encargado de desarrollar y administrar, gestionar y supervisar los procesos de marketing y publicidad de la empresa.
- Auxiliar o asistente administrativo: Encargada de ser la intermediaria entre la dirección general y las demás áreas.
- Auxiliar de oficina: encargado de la correspondencia y trámites generales de la empresa.

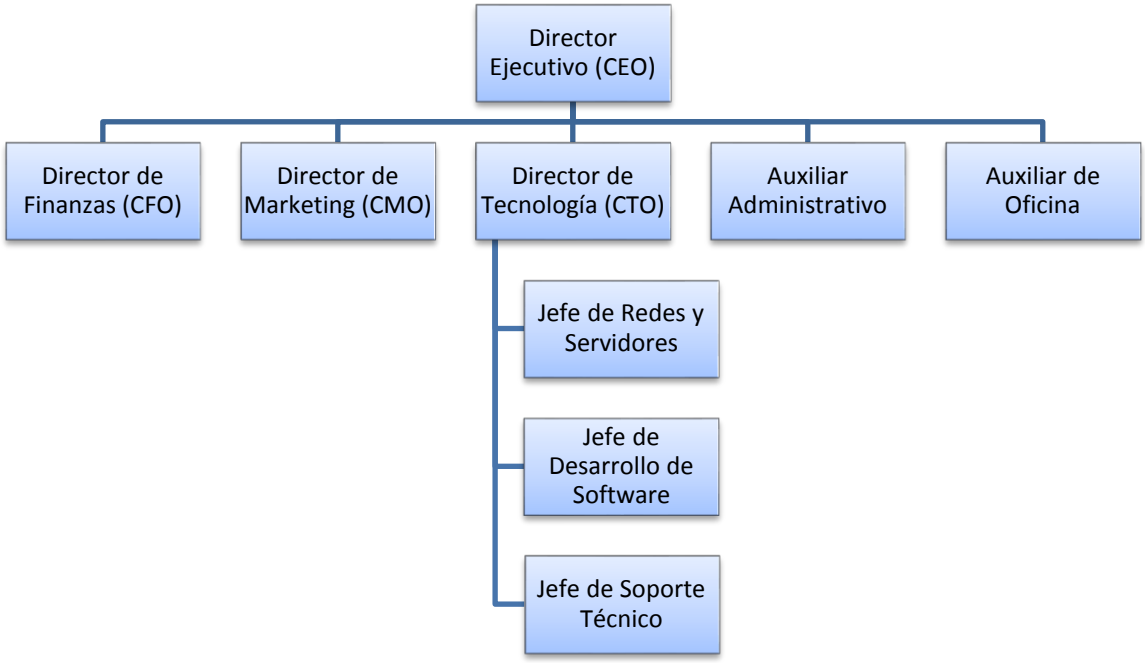

Ilustración 1 - Organigrama empresarial

La empresa fue constituida hace 5 años con un presupuesto mínimo y con recursos humanos y tecnológicos limitados; pero actualmente estos recursos se han incrementado según las necesidades del mercado tecnológico e informático vigente y la inversión que la empresa ha realizado para su innovación; por ende, la situación actual de la empresa en relación a la protección de los activos y la seguridad informática se la puede determinar realizando una análisis DAFO el cual es una herramienta de diagnóstico y gestión que permite establecer el estado actual de la empresa facilitando el proceso de planeación estratégica con el objetivo de implementar acciones y medidas correctivas [3]. Para el análisis se emplean 4 componentes debilidades, amenazas, fortalezas y oportunidades:

<u>Debilidades:</u>

- Los recursos de la red estructurada y servidores no están protegidos por elementos de bloqueo ante amenazas y ataques de redes externas como el Internet.

- La infraestructura de red y servidores no poseen elementos o sistemas de protección ante amenazas como firewalls o cortaguegos.
- El centro de cableado (Paneles de conexión, switches, routers, servidores) presenta deficiencias en cuanto a la falta de elementos redundantes tales como UPS (sistemas de alimentación ininterrumpida SAI).
- El equipo de cómputo utilizado para el proceso de realización de copias de seguridad de los computadores de las empresas para las cuales ofrece el servicio no posee la seguridad básica de almacenamiento de información puesto que no tiene un sistema de protección de antivirus y antimalware que proteja la información.
- Las copias de seguridad de la información de los computadores son almacenadas en un solo dispositivo de almacenamiento.
- Los sistemas de identificación y autenticación para los equipos de cómputo en el área de desarrollo son deficientes, ya que no se poseen políticas de acceso y las autorizaciones a los sistemas las manejan varios usuarios.
- Falta y desconocimiento de políticas de seguridad bien definidas para los diferentes procesos de la empresa.
- Uso indebido de los dispositivos tecnológicos (smartphones, tablets, computadores, etc) y de la red wifi.

Amenazas:

- Fallas en el servicio de internet, alojamiento y cloud suministrado por terceros.
- Insatisfacción en el servicio de soporte técnico que se ofrece a las empresas por falencias en oportunidad de respuesta.
- Ataques y explotación de vulnerabilidades realizados por entes externos a la infraestructura tecnológica y al personal de la empresa.
- Robo, pérdida y secuestro de información por ataques informáticos realizados por entes externos.
- Perdida de activos de información por motivos de desastres naturales y accidentales.

Fortalezas:

- Experiencia y amplio conocimiento por parte del personal en las funciones asignadas en las diferentes áreas.
- Posicionamiento de la empresa en relación a los servicios que presta a las empresas en la región.
- Inversión constante en tecnología y en capacitación de personal.
- Actualización periódica de equipos, dispositivos y software logrando estar a la vanguardia tecnológica.
- Gran capacidad de repositorio de elementos de hardware y software para la prestación del servicio técnico.
- El trabajo en equipo y el ambiente laboral es bueno.
- La seguridad física de los elementos, dispositivos y herramientas es buena.

Oportunidades:

- Definir las políticas de seguridad de la información.

- Obtener la certificación ISO/IEC 27001
- Alinear los procedimientos y políticas con el modelo del negocio de la empresa para un mejoramiento en la calidad de los servicios.
- Concientizar al personal en la importancia de la implementación y ejecución del SGSI.

Para lograr establecer un análisis completo de la situación actual de la empresa en relación a la seguridad de activos se utiliza una estrategia CAME que pretende definir un plan estratégico. En la matriz se identifican 4 factores: corregir, afrontar, mantener y explotar; las cuales, en vinculación con los componentes de la DAFO permitirán establecer las estrategias.

Tabla 2 – Matriz DAFO en estrategia CAME

DAFO/CAME	Análisis Interno	Análisis Externo
Factores Negativos	Estrategias para **Corregir Debilidades** *- Generar sistemas de protección ante ataques de redes externas.* *- Implementar elementos redundantes de sistemas de alimentación UPS necesarios para el continuó funcionamiento de servidores y sistemas de información.* *- Implementar sistemas de protección de antivirus y antimalware en los dispositivos de almacenamiento donde se realizan los backups.* *- Generar métodos de identificación y autenticación a los equipos de cómputo del área de desarrollo.* *- Plan de concientización y capacitación sobre las políticas de seguridad a los funcionarios de la empresa.* *- Formación a los funcionarios sobre buenas prácticas y uso de los dispositivos tecnológicos y el Internet.*	Estrategias para **Afrontar Amenazas** *- Plan de soporte ante fallas de Internet, servicio de alojamiento y cloud.* *- Estrategias de asistencia efectiva y oportuna a las empresas que requieren el servicio de soporte técnico.* *- Monitoreo y protección constante de la infraestructura de red y servidores que contienen información crítica y sensible.* *- Actualización de sistemas operativos, antivirus y sistemas de información.* *- Emplear estrategias para la protección de los vectores de ataque identificados en el monitoreo.* *- Realización periódica de copias de seguridad de la información crítica y sensible.*
Factores Positivos	Estrategias para **Mantener Fortalezas** *- Capacitación y*	Estrategias para **Explotar Oportunidades** *- Establecer los controles y*

	actualización en tendencias tecnológicas al personal de la empresa. *- Certificación permanente de la empresa y el personal de acuerdo a los objetivos y modelo de negocio.* *- Estrategias para la continua inversión en tecnología.* *- Mejoramiento y actualización de equipos, dispositivos y software requerido en la empresa.* *- Generación de espacios y actividades para el fortalecimiento del trabajo colaborativo entre los funcionarios o personal.*	*parámetros para el tratamiento de la seguridad de la información.* *- Obtener la certificación ISO/IEC 27001 mediante la implementación del SGSI.* *- Aplicar los procedimientos y controles para lograr los objetivos planteados en el SGSI y el mejoramiento continuo del negocio.* *- Evaluar las capacitaciones sobre la implementación y ejecución del SGSI al personal para retroalimentar y obtener una constante mejoría en la realización de los procesos.*

Además, la empresa contiene dentro de su infraestructura tecnológica elementos tales como:

- Servidores
- Computadores y portátiles
- Centro de Cableado
- Switchs
- Routers
- Impresoras
- Teléfonos

La ilustración 2 muestra los elementos en la infraestructura tecnológica de la empresa de Servicios y Soluciones Informáticas mediante el siguiente diagrama de red

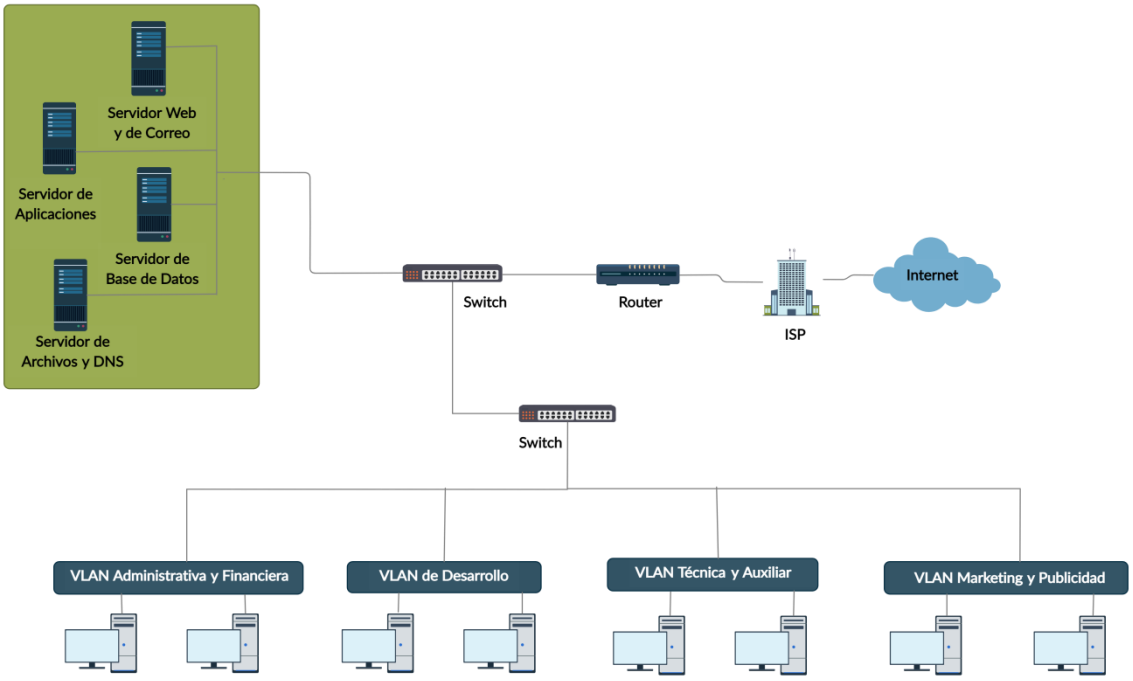

Ilustración 2 – Diagrama de red

En general, se puede determinar que la empresa no posee políticas, lineamientos y medidas de seguridad que permitan llevar una organización y control de los diferentes activos y recursos que posee; por lo cual, se hace necesario implementar un plan director del SGSI que conlleve a la búsqueda del fortalecimiento de la confidencialidad, integridad y disponibilidad de los activos y recursos logrando minimizar los riesgos que se puedan presentar.

1.3 Alcance del SGSI

Para la realización del SGSI de la empresa de servicios y soluciones informáticas se define un alcance que logre abarcar los aspectos que deben tenerse en cuenta para lograr los objetivos del proyecto, por consiguiente la implementación del SGSI comprenderá los sistemas de información y usuarios relacionados con los procesos de la empresa.

Básicamente se aplicará a las áreas y sistemas que ejecutan los procesos más importantes de la empresa como son los activos y recursos de la estructura de redes y servidores, el área de soporte técnico y el área de desarrollo de software y aplicaciones.

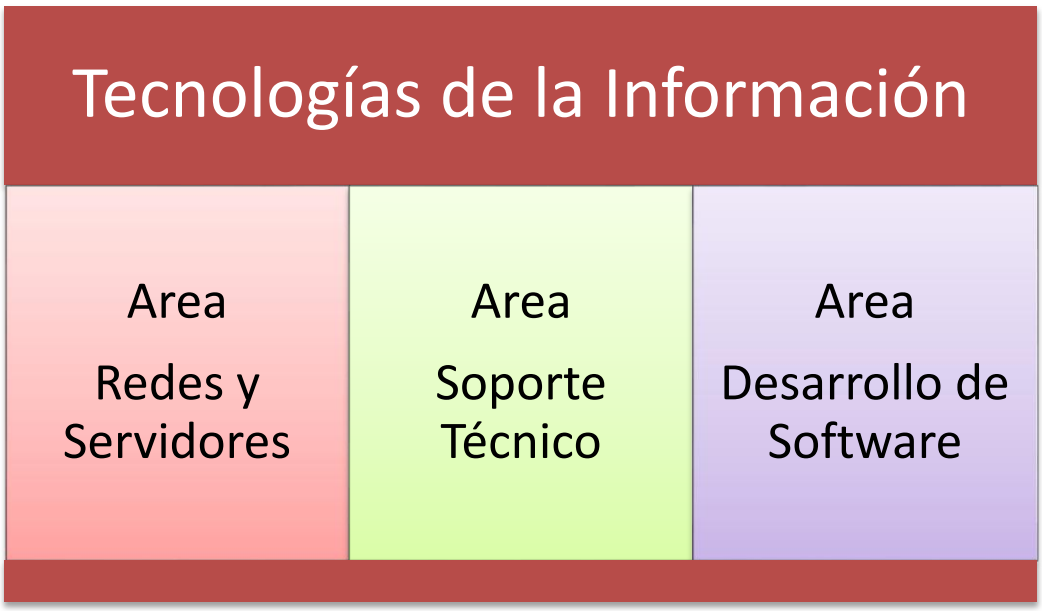

Ilustración 3 - Alcance del SGSI

1.4 Objetivos del Plan Director del SGSI

Para la realización de este proyecto, se tiene en cuenta los siguientes objetivos del Plan Director del SGSI:

- Identificar los activos y recursos que se requieren proteger teniendo en cuenta su nivel de importancia y necesidad para el funcionamiento de los procesos de la empresa.
- Analizar la situación actual de la empresa teniendo en cuenta los factores críticos de seguridad, riesgos potenciales e impactos generados.
- Identificar y analizar amenazas y vulnerabilidades que incidan en los activos y recursos tanto en la infraestructura de redes, servidores, equipos de cómputo y elementos del soporte técnico tanto a nivel físico como lógico.
- Determinar lineamientos, estrategias y parámetros que permitan mitigar las amenazas y vulnerabilidades con el propósito de mitigar los riesgos presentes.
- Elaborar el plan director del sistema de gestión de seguridad de la información SGSI, abarcando las normativas y requerimientos de seguridad; funciones, roles y responsabilidades de los usuarios para el control y administración del SGSI; guías de buenas prácticas y planes de continuidad de negocio acorde a los procesos de la empresa; lo anterior, garantizando la confidencialidad, integridad y disponibilidad de la seguridad de la información en la empresa.

1.5 Análisis Diferencial de la empresa con respecto a la ISO/IEC 27001 + ISO/IEC 27002

La empresa de Servicios y Soluciones Informáticas en la actualidad no presenta experiencia en la implantación de un SGSI; siendo una de las causas el poco tiempo de creación y funcionamiento de la empresa, la falta de normas o directrices de seguridad y la no concientización por parte de los funcionarios y directivos en relación a la seguridad; por tal motivo, para la planeación e implementación del SGSI se requiere realizar un análisis diferencial que permita determinar el estado actual de la seguridad en la empresa.

Para la realización del análisis diferencial de la empresa se debe tener en cuenta los siguientes aspectos:

- Establecer el modelo de capacidad de madurez para el análisis con los diferentes controles.
- Establecer las disposiciones o cláusulas de la ISO/IEC 27001 con el Modelo de Capacidad de Madurez CMM.
- Establecer los controles existentes descritos en la norma ISO/IEC 27002 con el Modelo de Capacidad de Madurez CMM.
- Elaborar un informe de resultados del análisis diferencial de los controles y cláusulas de cada norma con respecto al CMM

A continuación se presenta el Modelo de Capacidad de Madurez que se va a utilizar para valorar en porcentajes el nivel de desempeño actual de la empresa:

Tabla 3 – Modelo de Capacidad de Madurez (CMM)

Nivel	Estado	Valoración en porcentajes	Definición
L0	**Inexistente**	**0%**	Carencia total de procesos reconocibles. No existe gestión en la seguridad.
L1	**Inicial**	**25%**	No existen procesos concretos y tampoco plantillas o guías definidas. Este nivel es preliminar, el cual establece pautas y directivas para asegurar la seguridad de la información.
L2	**Repetible**	**50%**	Se siguen procedimientos similares en las mismas actividades o tareas que realizan las personas. No existe comunicación de procedimientos generales. Las responsabilidades asignadas recaen en cada persona. Existe un alto grado de confianza en el conocimiento de las personas.
L3	**Establecido**	**75%**	Se implementan, comunican y documentan procesos de forma más

			permanente y estable. La entidad tiene más participación en el desarrollo de los procesos por medio de un control y monitoreo establecido.
L4	**Administrado**	**95%**	Se mide el cumplimiento y evolución de los procesos mediante indicadores. Los procesos facilitan mejores prácticas. Se determinan medidas cuando los procesos no funcionan de manera efectiva.
L5	**Mejorado**	**100%**	Teniendo en cuenta los resultados obtenidos de los controles implantados se hace una revisión de los procesos que han tenido una mejora continua. Se dispone de herramientas para garantizar y mejorar la calidad y eficiencia.

La *Tabla 4 – Evaluación de cláusulas de la ISO/IEC 27001 vs CMM* indica las disposiciones actuales de la empresa en relación con la ISO/IEC 27001 con respecto al Modelo de Capacidad de Madurez CMM

Tabla 4 – Evaluación de cláusulas de la ISO/IEC 27001 vs CMM

Disposiciones o cláusulas	Nivel CMM	Valoración %
4. Contexto de la organización.	**L0**	**12,5**
4.1 Comprensión de la organización y su contexto.		25
4.2 Comprensión de las necesidades y expectativas de las partes interesadas.		25
4.3 Determinación del alcance del sistema de gestión de continuidad de negocios.		0
4.4 Sistema de Gestión de Continuidad de Negocios.		0
5. Liderazgo	**L0**	**18,75**
5.1 Liderazgo y compromiso.		25
5.2 Compromiso gerencial.		25
5.3 Política.		0
5.4 Roles, responsabilidades y autoridades de la organización.		25
6. Planificación.	**L0**	**12,5**
6.1 Acciones para atender los riesgos y las oportunidades.		25
6.2 Objetivos de continuidad de negocios y planes para lograrlos.		0

7. Soporte.	**L0**	**10**
7.1 Recursos.		25
7.2 Competencia.		25
7.3 Concientización.		0
7.4 Comunicación.		0
7.5 Información a documentar		0
8. Operación.	**L0**	**5**
8.1 Planificación y control operacional.		25
8.2 Análisis de impactos en los negocios y valuación de riesgos.		0
8.3 Estrategia de continuidad de negocios.		0
8.4 Establecimiento e implementación de los procedimientos de continuidad de negocios.		0
8.5 Ejercicios y pruebas.		0
9. Evaluación del desempeño.	**L0**	**0**
9.1 Monitoreo, medición, análisis y evaluación.		0
9.2 Auditoría interna.		0
9.3 Revisión gerencial.		0
10. Mejoramiento.	**L0**	**0**
10.1 No conformidades y acciones correctivas.		0
10.2 Mejoramiento continuo.		0

La *Tabla 5 – Evaluación de controles de la ISO/IEC 27002 vs Modelo CMM* presenta los controles (114) de seguridad de la norma ISO/IEC 27002 con el que se cumplen los objetivos (34) en base al análisis referenciado con el Modelo CMM

Tabla 5 – Evaluación de controles de la ISO/IEC 27002 vs Modelo CMM

CONTROL			Nivel CMM	Valoración %
A.5 Políticas de seguridad de la información			**L0**	**0**
5.1 Directrices de gestión de la seguridad de la información				0
	A.5.1.1	Políticas para la seguridad de la información		0
	A.5.1.2	Revisión de las políticas para la seguridad de la información		0
A.6 Organización de la seguridad de la información			**L0**	**17,5**
A.6.1 Organización interna				10
	A.6.1.1	Roles y responsabilidades para la seguridad de la información		0
	A.6.1.2	Separación de deberes		25
	A.6.1.3	Contacto con las autoridades		25

	A.6.1.4	Contacto con grupos de interés especial		0
	A.6.1.5	Seguridad de la información en la gestión de proyectos.		0
A.6.2 Dispositivos móviles y teletrabajo				25
	A.6.2.1	Política para dispositivos móviles		0
	A.6.2.2	Teletrabajo		50
A.7 Seguridad de los recursos humanos			**L0**	**19,44**
A.7.1 Antes de asumir el empleo				50
	A.7.1.1	Selección		75
	A.7.1.2	Términos y condiciones del empleo		25
A.7.2 Durante la ejecución del empleo				8,33
	A.7.2.1	Responsabilidades de la dirección		25
	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.		0
	A.7.2.3	Proceso disciplinario		0
A.7.3 Terminación y cambio de empleo				0
	A.7.3.1	Terminación o cambio de responsabilidades de empleo		0
A.8 Gestión de activos			**L1**	**29,16**
A.8.1 Responsabilidad por los activos				37,5
	A.8.1.1	Inventario de activos		50
	A.8.1.2	Propiedad de los activos		50
	A.8.1.3	Uso aceptable de los activos		25
	A.8.1.4	Devolución de activos		25
A.8.2 Clasificación de la información				25
	A.8.2.1	Clasificación de la información		25
	A.8.2.2	Etiquetado de la información		25
	A.8.2.3	Manejo de activos		25
A.8.3 Manejo de medios				25
	A.8.3.1	Gestión de medio removibles		25
	A.8.3.2	Disposición de los medios		25
	A.8.3.3	Transferencia de medios físicos		25
A.9 Control de acceso			**L0**	**16,87**
A.9.1 Requisitos del negocio para el control de acceso				25
	A.9.1.1	Política de control de acceso		25
	A.9.1.2	Acceso a redes y a servicios en red		25
A.9.2 Gestión de acceso de usuarios				12,5
	A.9.2.1	Registro y cancelación del registro de usuarios		25
	A.9.2.2	Suministro de acceso de usuarios		25
	A.9.2.3	Gestión de derechos de acceso		0

		privilegiado		
	A.9.2.4	Gestión de información de autenticación secreta de usuarios		0
	A.9.2.5	Revisión de los derechos de acceso de usuarios		0
	A.9.2.6	Retiro o ajuste de los derechos de acceso		25
A.9.3 Responsabilidades de los usuarios				25
	A.9.3.1	Uso de información de autenticación secreta		25
A.9.4 Control de acceso a sistemas y aplicaciones				5
	A.9.4.1	Restricción de acceso a la información		25
	A.9.4.2	Procedimiento de ingreso seguro		0
	A.9.4.3	Sistema de gestión de contraseñas		0
	A.9.4.4	Uso de programas utilitarios privilegiados		0
	A.9.4.5	Control de acceso a códigos fuente de programas		0
A.10 Criptografía			**L0**	**0**
A.10.1 Controles criptográficos				0
	A.10.1.1	Política sobre el uso de controles criptográficos		0
	A.10.1.2	Gestión de llaves		0
A.11 Seguridad física y del entorno			**L1**	**31,25**
A.11.1 Áreas seguras				37,5
	A.11.1.1	Perímetro de seguridad física		50
	A.11.1.2	Controles de acceso físicos		25
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones		25
	A.11.1.4	Protección contra amenazas externas y ambientales		25
	A.11.1.5	Trabajo en áreas seguras		50
	A.11.1.6	Áreas de carga, despacho y acceso público		50
A.11.2 Equipos				25
	A.11.2.1	Ubicación y protección de los equipos		25
	A.11.2.2	Servicios de suministro		0
	A.11.2.3	Seguridad en el cableado		50

	A.11.2.4	Mantenimiento de los equipos		25
	A.11.2.5	Retiro de activos		25
	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		50
	A.11.2.7	Disposición segura o reutilización de equipos		25
	A.11.2.8	Equipos de usuario desatendido		25
	A.11.2.9	Política de escritorio limpio y pantalla limpia		0
A.12 Seguridad de las operaciones			**L1**	**27,97**
A.12.1 Procedimientos operacionales y responsabilidades				33,33
	A.12.1.1	Procedimientos de operación documentados		25
	A.12.1.2	Gestión de cambios		0
	A.12.1.3	Gestión de capacidad		25
	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		50
A.12.2 Protección contra códigos maliciosos				50
	A.12.2.1	Controles contra códigos maliciosos		50
A.12.3 Copias de seguridad				25
	A.12.3.1	Respaldo de la información		25
A.12.4 Registro y seguimiento				12,5
	A.12.4.1	Registro de eventos		25
	A.12.4.2	Protección de la información de registro		25
	A.12.4.3	Registros del administrador y del operador		0
	A.12.4.4	Sincronización de relojes		0
A.12.5 Control de software operacional				50
	A.12.5.1	Instalación de software en sistemas operativos		50
A.12.6 Gestión de la vulnerabilidad técnica				37,5
	A.12.6.1	Gestión de las vulnerabilidades técnicas		25
	A.12.6.2	Restricciones sobre la instalación de software		50
A.12.7 Consideraciones sobre auditorias de sistemas de información				0

	A.12.7.1	Controles de auditorías de sistemas de información		0
A.13 Seguridad de las comunicaciones			**L0**	**21,87**
A.13.1 Gestión de la seguridad de las redes				25
	A.13.1.1	Controles de redes		25
	A.13.1.2	Seguridad de los servicios de red		25
	A.13.1.3	Separación en las redes		25
A.13.2 Transferencia de información				18,75
	A.13.2.1	Políticas y procedimientos de transferencia de información		25
	A.13.2.2	Acuerdos sobre transferencia de información		25
	A.13.2.3	Mensajería Electrónica		0
	A.13.2.4	Acuerdos de confidencialidad o de no divulgación		25
A.14 Adquisición, desarrollo y mantenimientos de sistemas			**L0**	**22,22**
A.14.1 Requisitos de seguridad de los sistemas de información				33,33
	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		25
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		50
	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		25
A.14.2 Seguridad en los procesos de Desarrollo y de Soporte				33,33
	A.14.2.1	Política de desarrollo seguro		25
	A.14.2.2	Procedimientos de control de cambios en sistemas		25
	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		50
	A.14.2.4	Restricciones en los cambios a los paquetes de software		25
	A.14.2.5	Principio de Construcción de los Sistemas Seguros		25
	A.14.2.6	Ambiente de desarrollo seguro		25
	A.14.2.7	Desarrollo contratado externamente		50
	A.14.2.8	Pruebas de seguridad de sistemas		25

	A.14.2.9	Prueba de aceptación de sistemas		50
A.14.3 Datos de prueba				0
	A.14.3.1	Protección de datos de prueba		0
A.15 Relación con los proveedores			**L2**	**54,16**
A.15.1 Seguridad de la información en las relaciones con los proveedores				58,33
	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		75
	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		50
	A.15.1.3	Cadena de suministro de tecnología de información y comunicación		50
A.15.2 Gestión de la prestación de servicios de proveedores				50
	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		50
	A.15.2.2	Gestión del cambio en los servicios de los proveedores		50
A.16 Gestión de incidentes de seguridad de la información			**L0**	**14,28**
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información				14,28
	A.16.1.1	Responsabilidades y procedimientos		25
	A.16.1.2	Reporte de eventos de seguridad de la información		25
	A.16.1.3	Reporte de debilidades de seguridad de la información		0
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		0
	A.16.1.5	Respuesta a incidentes de seguridad de la información		25
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		0
	A.16.1.7	Recolección de evidencia		25
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			**L0**	**0**
A.17.1 Continuidad de Seguridad de la información				0
	A.17.1.1	Planificación de la continuidad de la seguridad de la información		0
	A.17.1.	Implementación de la continuidad		0

	2	de la seguridad de la información		
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		0
A.17.2 Redundancias				0
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información		0
A.18 Cumplimiento			**L0**	**12,5**
A.18.1 Cumplimiento de requisitos legales y contractuales				25
	A.18.1.1	Identificación de la legislación aplicable		25
	A.18.1.2	Derechos propiedad intelectual		25
	A.18.1.3	Protección de registros		50
	A.18.1.4	Privacidad y protección de información de datos personales		25
	A.18.1.5	Reglamentación de controles criptográficos.		0
A.18.2 Revisiones de seguridad de la información				0
	A.18.2.1	Revisión independiente de la seguridad de la información		0
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad		0
	A.18.2.3	Revisión del cumplimiento técnico		0

1.6 Resultados

Con base en los resultados obtenidos se puede concluir que los requisitos y/o cláusulas de la norma ISO/IEC 27001 para un Sistema de Gestión de Seguridad de la información de la empresa de Servicios y soluciones Informáticas se encuentran por debajo del 20% de cumplimiento en la valoración realizada. Lo anterior indica que el nivel de la capacidad de madurez está por debajo del nivel L1(Inicial) mostrando en las cláusulas de Evaluación de desempeño y Mejoramiento una valoración baja del 0% y la cláusula de Liderazgo la más alta con una valoración de 18,75%.

Presenta un bajo cumplimiento del 10% en el requisito del soporte; expuesto en la gestión de recursos y activos principales, en la competencia y concienciación de los empleados, comunicación en las distintas áreas tanto de nivel administrativo como las de nivel técnico y auxiliar; y en la documentación generada para el cumplimiento de los requisitos (manuales, guías, etc).

Los resultados se pueden observar y determinar en el siguiente gráfico de los resultados de análisis de las cláusulas de la ISO/IEC 27001 vs Modelo CMM

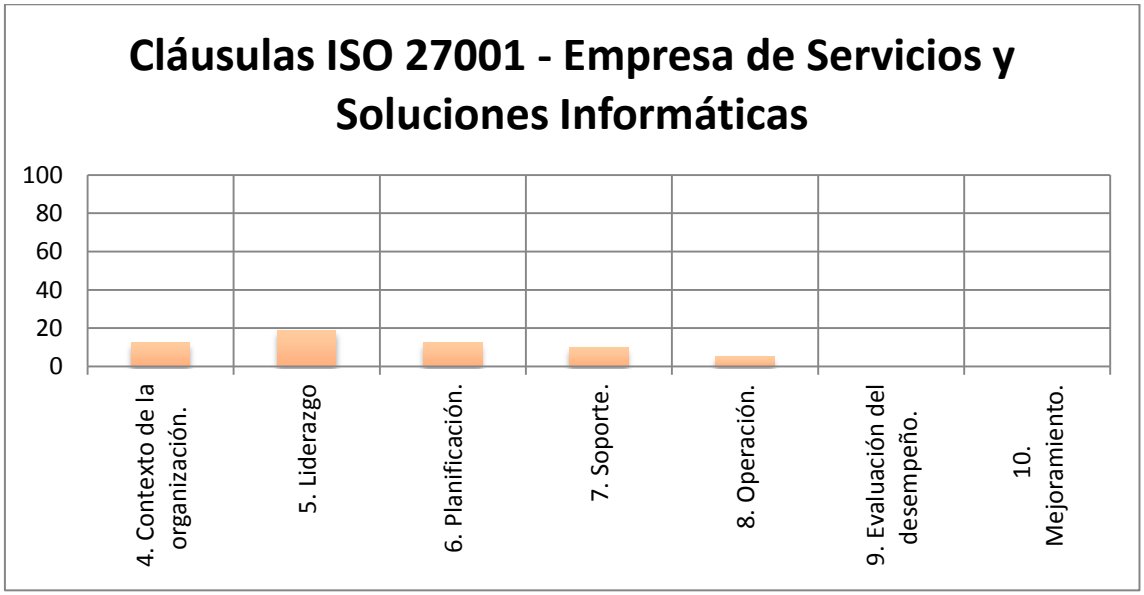

Ilustración 4 – Gráfico de resultados de análisis de las cláusulas de la ISO/IEC 27001 vs Modelo CMM

Con respecto al análisis realizado de los controles de la norma ISO 27002 con base al CMM se puede establecer los siguientes resultados:

- La mayoría de los controles se encuentran en un nivel de madurez inexistente e inicial, lo que indica que no existe procesos fuertemente establecidos que permitan abordar los problemas o peligros de la seguridad de la información en las diferentes áreas de la empresa.
- El control de Relación con los proveedores presenta un nivel de madurez repetible L2 siendo el único que contiene procedimientos más asertivos en relación a la seguridad y gestión de políticas, tratamientos y seguimientos de las relaciones y servicios prestados por los proveedores.

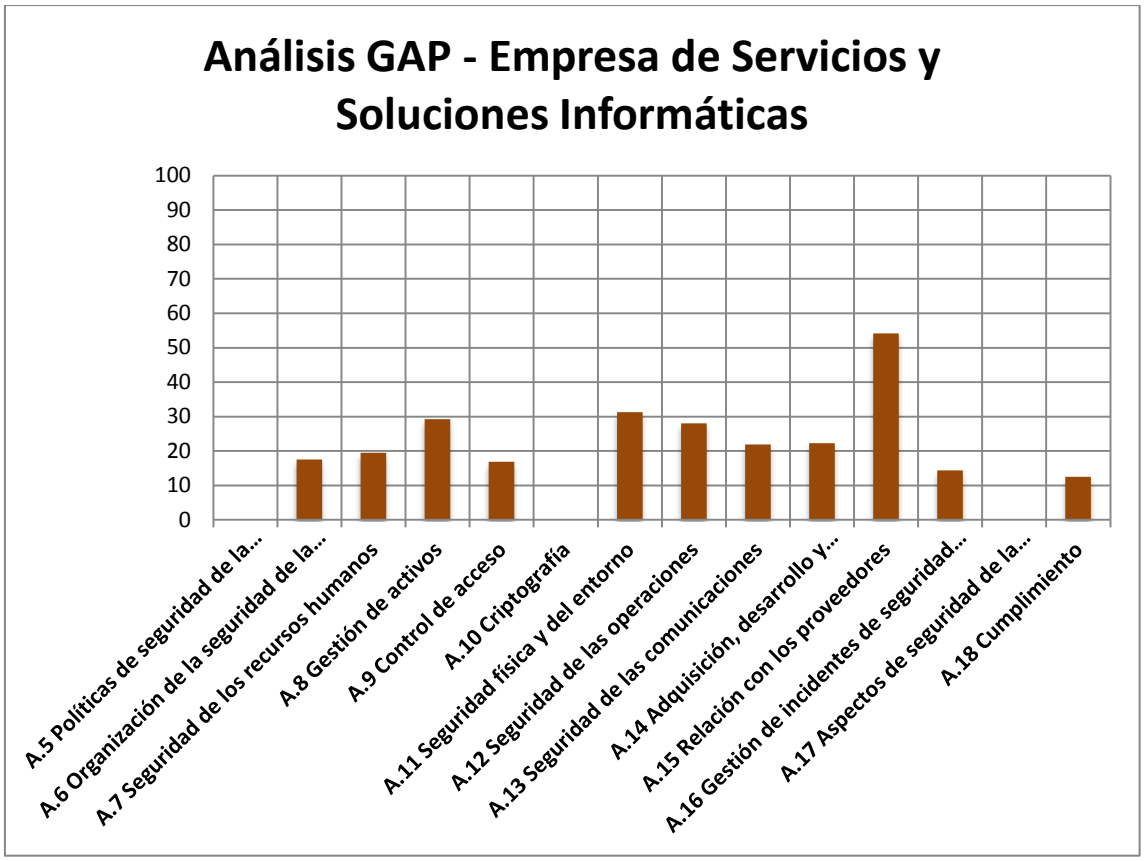

Ilustración 5 – Gráfico de resultados de análisis de los controles de la ISO/IEC 27002 vs Modelo CMM

Teniendo en cuenta el análisis GAP de la ISO/IEC 27002, a continuación, se describirá brevemente el estado actual de cumplimiento de la empresa de Servicios y Soluciones Informáticas con respecto a los dominios y controles que presentan un porcentaje mayor al 0%.

A.6 Organización de la seguridad de la información

A.6.1 Organización interna

- 6.1.2 Separación de funciones: existe una separación de funciones con respecto a los perfiles y roles de cada funcionario de la empresa.
- 6.1.3 Contacto con autoridades: se mantiene un contacto con las empresas proveedoras de servicios de Internet y cloud en caso de fallas y caídas de sistema.

A.6.2 Dispositivos móviles y teletrabajo

- 6.2.2 Teletrabajo: existe un procedimiento mínimo en relación a las restricciones de acceso y niveles de confianza a los activos permitidos para ciertos funcionarios.

A.7 Seguridad de los recursos humanos

A.7.1 Antes de asumir el empleo

- 7.1.1 Selección: existe procedimientos establecidos para la contratación, experiencia, estudios y en general hoja de vida del personal contratado soportándose en los documentos requeridos.
- 7.1.2 Términos y condiciones de empleo: a pesar que existe el control de selección y contratación, existe un nivel inicial en responsabilidades y obligaciones de los empleados en relación a la seguridad y privacidad de la información.

A.7.2 Durante la ejecución del empleo

- 7.2.1 Responsabilidades de la dirección: la dirección de la empresa comunica las políticas, normas y procedimientos de forma verbal sin existir documentación e información textual que soporte el cumplimiento de las normas.

A.8 Gestión de activos

A.8.1 Responsabilidad por los activos

- 8.1.1 Inventario de activos: existe un proceso de registro de los activos pero no se tiene una organización en la información detallada de cada activo. El proceso se realiza en un archivo de una hoja de cálculo pero no se ha sistematizado y organizado de forma completa.
- 8.1.2 Propiedad de los activos: en algunos casos no existe el propietario del activo y no se realiza una constante actualización del propietario del activo.
- 8.1.3 Uso aceptable de los activos: existe una pauta sencilla de comunicar el uso apropiado de los activos pero aún no se ha documentado completamente el uso, la descripción de los requisitos de seguridad, instalación, precauciones y advertencias, etc.
- 8.1.4 Devolución de activos: El proceso de devolución de activos se realiza de forma sencilla y no existe una planilla de registro digital ni física.

A.8.2 Clasificación de la información

- 8.2.1 Clasificación de la información: existe una directiva para la clasificación de los activos y la información solo por el valor y la asignación a las áreas de la empresa.
- 8.2.2 Etiquetado de la información: existe pautas de etiquetado físico de los activos pero no se ha sistematizado el proceso y además la información es básica referente al activo (propietario, área y fecha de ingreso)
- 8.2.3 Manejo de los activos: se establece un manejo de acuerdo a la asignación de los activos al área y personal pero no hay procedimientos de restricciones, autorizaciones, registro de almacenamiento y copias de seguridad de los activos.

A.8.3 Manejo de medios

- 8.3.1 Gestión de soportes extraíbles: no existe documentación para la administración, acceso y registro de los soportes extraíbles; además, no existe planillas para registrar la gestión de estos soportes.
- 8.3.2 Eliminación de soportes: Los soportes extraíbles se desechan de forma personal por cada funcionario sin existir procedimientos para la

eliminación segura del soporte una vez finalice su uso o se deseche por daño físico o lógico del soporte.

- 8.3.3 Traslado de soportes físicos: se dispone de una empresa para el traslado de los soportes físicos pero no se lleva un control sobre el proceso de envío y recepción y sobre el seguimiento del soporte.

A.9 Control de acceso

A.9.1 Requisitos del negocio para el control de acceso

- 9.1.1 Política de control de acceso: no existe una documentación definida sobre políticas de control de acceso a la información (sistemas de información, acceso a áreas con autorización, acceso a dispositivos, acceso a información reservada)
- 9.1.2 Acceso a las redes y a los servicios de red: no existe documentación definida sobre políticas y controles a los servicios de red, elementos de red, medios de conexión y servidores en relación a los accesos y autorizaciones.

A.9.2 Gestión de acceso de usuarios

- 9.2.1 Registro de usuarios y cancelación del registro: aunque los usuarios se registran en los sistemas y servicios dentro de la empresa no hay documentación que permita definir políticas para el registro y bajas o eliminaciones de usuarios.
- 9.2.2 Gestión de acceso a los usuarios: la directriz de acceso a los usuarios lo realiza el administrador de servicios de red y servidores aprobado por los jefes de cada área. Por lo tanto, no existe políticas y planillas que evidencien el debido proceso de acceso a los usuarios.
- 9.2.6 Remoción o ajuste de los derechos de acceso: solo se remueve o ajusta los derechos de acceso cuando el empleado es ubicado en otro cargo o área y cuando se finaliza la contratación del empleado; y se lo realiza por orden del jefe inmediato sin el diligenciamiento de formatos o planillas.

A.9.3 Responsabilidades de los usuarios

- 9.3.1 Uso de la información de autenticación secreta: solo el administrador de servicios, redes y servidores realiza la creación, modificación y eliminación de contraseñas, pero no existe protocolos establecidos para este proceso. Se hace de forma personal por cada funcionario con el administrador.

A.9.4 Control de acceso a sistemas y aplicaciones

- 9.4.1 Restricción de acceso a la información: Hay un proceso sencillo sobre restricción de acceso a información clasificada pero no hay lineamientos específicos para estas restricciones.

A.11 Seguridad física y del entorno

A.11.1 Áreas seguras

- 11.1.1 Perímetro de seguridad física: existe procesos de protección de acceso y autorizaciones a las instalaciones físicas, seguridad perimetral, medidas de seguridad y alrededores; los cuales, las funciones de seguridad física solo son realizadas por el personal específico y no existe protocolos más definidos y documentados.

- 11.1.2 Controles de acceso físico: existe un control de acceso a áreas clasificadas pero no se determina protocolos para el ingreso, autorización, registro, monitoreo por parte del personal interno y externo a los diferentes lugares con restricción (centro de cableado, servidores, área de desarrollo, área directiva, etc.)
- 11.1.3 Seguridad de oficinas, despachos e instalaciones: existe ciertos elementos para la seguridad de oficinas pero no se ha establecido parámetros más concretos para obtener una máxima seguridad.
- 11.1.4 Protección contra amenazas externas y del ambiente: existe unos lineamientos para protección física contra factores externos y del ambiente pero no se ha establecido medidas más concretas y definidas.
- 11.1.5 El trabajo en las áreas seguras: se estipulan procedimientos para el trabajo en áreas seguros (restricción de dispositivos móviles y cámaras en el área de redes y servidores, protección de inserción de dispositivos externos en áreas seguras, etc.)
- 11.1.6 Áreas de entrega y de carga: se hace revisión de los productos recibidos y enviados, revisión de los equipos y dispositivos del área de soporte técnico, control del personal para la entrega de los productos y dispositivos; pero, no existe medidas más concretas y documentación que evidencie la entrega y recepción de carga.

A.11.2 Equipos

- 11.2.1 Ubicación y protección del equipamiento: los equipos y dispositivos se protegen pero no se encuentran medidas de protección contra daños eléctricos como por ejemplo UPS para el continuo funcionamiento temporal de los servicios y servidores.
- 11.2.3 Seguridad en el cableado: existe protección contra daño ambiental y provocado en el cableado estructurado con materiales y elementos tales como canaletas, tomas, racks, closets, patch panels, etc.
- 11.2.4 Mantenimiento del equipamiento: solo existe el control de mantenimiento de equipos el cual se trata de la limpieza externa de los equipos por parte del personal de limpieza.
- 11.2.5 Retiro de activos: el control que se lleva del retiro de equipos es la desvinculación del activo con el personal o funcionario que estaba asignado, pero no existen más controles y registros del activo retirado.
- 11.2.6 Seguridad del equipamiento y de los activos fuera de las instalaciones: existe una planilla de registro de los equipos que salen de las instalaciones de la empresa y se lleva un control y seguimiento de los equipos.
- 11.2.7 Disposición segura o reutilización de equipos: no se realiza una adecuada eliminación de archivos de los equipos para su reutilización y el formateo de estos se lo realiza de forma básica y solo al sistema operativos sin tener en cuenta las demás particiones.
- 11.2.8 Equipos de usuario desatendido: no existe hábitos adecuados para el cierre de sesión, bloqueos de pantalla y cierres de aplicaciones web por parte de los funcionarios, solos algunos pero en poca cantidad lo realizan.

A.12 Seguridad de las operaciones

A.12.1 Procedimientos operacionales y responsabilidades

- 12.1.1 Procedimientos documentados de operación: se realiza procesos de instalación, configuración y administración de software, también gestión de copias de seguridad, pero de manera operativa sin tener en cuenta lineamientos y documentación específica para estas operaciones.
- 12.1.3 Gestión de la capacidad: no existen procesos definidos para gestionar la capacidad en los servidores de base de datos, web correo, archivos y DNS.
- 12.1.4 Separación de los ambientes para desarrollo, prueba y operación: existe separación de ambientes de prueba con los de producción en el área de desarrollo, pero no se establecen políticas en cuestión a la parte de código seguro.

A.12.2 Protección contra códigos maliciosos

- 12.2.1 Controles ante software malicioso: existen sistemas de detección de código malicioso y malware en los equipos personales como en los servidores.

A.12.3 Copias de seguridad

- 12.3.1 Respaldo de la información: existe unos lineamientos de respaldo de la información pero no existe definido las políticas que establezcan la periodicidad, formas, tipos y demás con las que se realizan los respaldos.

A.12.4 Registro y seguimiento

- 12.4.1 Registro de eventos: se hace un almacenamiento de eventos para determinar los incidentes y fallas de los sistemas pero no se hace un registro y seguimiento de los eventos.
- 12.4.2 Protección de la información de registros: se realiza una protección mínima de los registros por medio de copias pero no se establecen directrices más concretas para su protección.

A.12.5 Control de software operacional

- 12.5.1 Instalación de software en los sistemas operativos: existen procedimientos para la instalación, pruebas, configuración, monitoreo de software instalado en los equipos y servidores.

A.12.6 Gestión de la vulnerabilidad técnica

- 12.6.1 Gestión de vulnerabilidades técnicas: no se realiza pruebas de ataques y escaneo de vulnerabilidades en los sistemas de información de la empresa.
- 12.6.2 Restricciones en la instalación de software: la instalación de software la realiza el personal capacitado y autorizado y además se utiliza un sistema de bloqueo de instalación en los computadores personales de las diferentes dependencias y oficinas de la empresa.

A.13 Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes

- 13.1.1 Controles de Red: hay una administración de bajo nivel en los elementos físicos de la red y en la correcta transmisión de los datos.
- 13.1.2 Seguridad de los servicios de red: no se brinda una alta calidad en la seguridad de los servicios de red puesto que no hay auditorias y evaluación permanente de estos servicios.

- 13.1.3 Separación en redes: existe una leve segmentación correcta de las subredes dentro de la empresa tanto lógica como física.

A.13.2 Transferencia de información

- 13.2.1 Políticas y procedimientos de intercambio de información: solo algunas áreas de la empresa manejan lineamientos y procedimientos para el envio, recepción y manejo de información.
- 13.2.2 Acuerdos de intercambio de información: las partes solo cubren los controles de acceso a la información entre las empresas pero no hay requisitos de cifrado, responsabilidades, acuerdos de protección y custodia.
- 13.2.4 Acuerdos de confidencialidad y de no divulgación: Los acuerdos de confidencialidad entre las áreas o dependencias y entre terceras partes se realizan de forma verbal y no se realiza de forma textual o digital y firmada.

A.14 Adquisición, desarrollo y mantenimientos de sistemas

A.14.1 Requisitos de seguridad de los sistemas de información

- 14.1.1 Análisis y especificación de los requisitos de seguridad: el área de desarrollo no especifica un análisis minucioso en la parte de seguridad en el desarrollo de las aplicaciones.
- 14.1.2 Aseguramiento de los servicios de aplicación en las redes públicas: se utiliza conexiones seguras para la transmisión de información a través de Internet, utilización de VPN y SSH.
- 14.1.3 Protección de transacciones de los servicios de las aplicaciones: solo se tiene aplicado la utilización de protocolos seguros para las transacciones entre las aplicaciones.

A.14.2 Seguridad en los procesos de Desarrollo y de Soporte

- 14.2.1 Política de desarrollo seguro: se determinan pautas para el desarrollo seguro en el área de desarrollo de aplicaciones y software de la empresa pero no hay reglas y políticas para este control.
- 14.2.2 Procedimiento de control de cambio del sistema: existen actualizaciones de software y sistemas operativos pero no se definen documentos y políticas que permitan gestionar los cambios y actualizaciones de forma más precisa.
- 14.2.3 Revisión técnica de aplicaciones después de cambios de las plataformas operativas: existe una revisión de los cambios en los sistemas operativos y el software después de realizar las actualizaciones de los equipos de las diferentes áreas de la empresa.
- 14.2.4 Restricciones a los cambios en los paquetes de software: las actualizaciones del software y los sistemas operativos son generales y no hay restricciones con criterios antes de realizarlas.
- 14.2.5 Principios de construcción de los Sistemas Seguros: existe algunos documentos en los procedimientos y técnicas de desarrollo seguro.
- 14.2.6 Ambiente de desarrollo seguro: hay un cierto grado en la confiabilidad del personal y en los procesos para los entornos de desarrollo.

- 14.2.7 Desarrollo contratado externamente: existe un control y gestión en lo relacionado con licencias y propiedades de código fuente de desarrollo de terceras partes.
- 14.2.8 Pruebas de seguridad del sistema: se ejecutan pruebas del sistema pero no hay un plan de pruebas documentado correctamente.
- 14.2.9 Pruebas de aceptación del sistema: existen validaciones funcionales y de seguridad del sistema a implementar aunque falta establecer planificación y mayor control en las pruebas.

A.15 Relación con los proveedores

A.15.1 Seguridad de la información en las relaciones con los proveedores

- 15.1.1 Política de seguridad de la información para las relaciones con los proveedores: existe establecido los acuerdos de políticas de seguridad de la información con los proveedores mediante la estipulación de documentos y firma de contratos en acuerdo mutuo con cláusulas definidas.
- 15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores: se estipulan acuerdos para el tratamiento de la seguridad dentro de los documentos y contratos acordados por las partes.
- 15.1.3 Cadena de suministro de tecnologías de la información y las comunicaciones: se estipula en los documentos la lista de proveedores de confianza y el control de seguridad a los proveedores subcontratados o aliados.

A.15.2 Gestión de la prestación de servicios de proveedores

- 15.2.1 Seguimiento y revisión de los servicios de proveedores: hay registros o informes sobre el estado y nivel de los servicios prestados por los proveedores pero no se hace un seguimiento periódico sobre la monitorización de los servicios.
- 15.2.2 Gestión de cambios en los servicios de los proveedores: se realiza un análisis de los cambios de servicios para minimizar riesgos.

A.16 Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

- 16.1.1 Responsabilidades y procedimientos: se tiene unas actividades muy básicas sobre quiénes son los responsables en caso de incidentes de seguridad y que acciones se deben realizar.
- 16.1.2 Reporte de eventos de seguridad de la información: no existe mecanismos de notificación de eventos e incidentes y solo hay un canal de comunicación para reportar estos incidentes (teléfonos) en las dependencias y con el personal de la empresa.
- 16.1.5 Respuesta a incidentes de seguridad de la información: solo existe una comunicación para informar los eventos e incidentes presentados pero no se registra las acciones y se hace un análisis para determinar las causas del incidente.
- 16.1.7 Recolección de evidencia: se determina sanciones a los involucrados en las situaciones o incidentes, se recolecta la evidencia pero no se documenta y se establecen criterios para posteriores incidentes similares.

A.18 Cumplimiento

A.18.1 Cumplimiento de requisitos legales y contractuales

- 18.1.1 Identificación de la legislación aplicable: se procede a dar cumplimiento de los requisitos legales para la seguridad de la información pero se desconocen los procedimientos de identificar la legislación dependiendo de la situación presente y su permanente actualización legislativa.
- 18.1.2 Derechos de propiedad intelectual: algunos funcionarios aplican la utilización legal de software pero no hay políticas que controlen este uso.
- 18.1.3 Protección de los registros: se define lineamientos sobre protección de registros contables, bases de datos, procedimientos operativos, registros documentales y de algunos archivos cifrados.
- 18.1.4 Privacidad y protección de información de datos personales: se tiene conocimiento sobre la ley de protección de datos (ley 1581 de 2012) pero no hay controles para verificar su cumplimiento en la empresa.

2. Documentación del SGSI

La norma ISO/IEC 27001 dispone de una serie de documentos obligatorios para el cumplimiento normativo de la implementación correcta de un Sistema de Gestión de Seguridad de la Información y la certificación del sistema.

A continuación se enumera la documentación a la que se refiere la norma y en los apartes siguientes se hace una breve descripción de cada una de ellas y el contenido requerido para la misma dentro del proyecto:

- **Política de Seguridad.**
- **Procedimiento de Auditorías Internas.**
- **Gestión de Indicadores.**
- **Procedimiento Revisión por Dirección.**
- **Gestión de Roles y Responsabilidades.**
- **Metodología de Análisis de Riesgos.**
- **Declaración de Aplicabilidad.**

Para establecer la documentación del SGSI se empleará un formato que permitirá organizar los documentos mencionados anteriormente de forma más sistémica, teniendo en cuenta los siguientes parámetros:

Tabla 6 – Formato de esquema de Documentación del SGSI

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**POLITICA, DOCUMENTO, PROCEDIMIENTO, ETC**	Código: Versión: Fecha de aprobación: Página:

ESQUEMA
1. Introducción: definición de la pauta que se va a realizar
2. Objetivo: fin o propósito del documento
3. Alcance: a quien o quienes está dirigido el documento
4. Marco normativo y regulatorio: se indican las normas de guía o modelo en la construcción del documento.
5. Descripción: descripción del documento, política, metodología, procedimiento, etc.
6. Medios de divulgación: medios de comunicación por el cual se va a divulgar el documento

	Nombres y Apellidos	**Cargo**	**Fecha**	**Firma**
Elaborado				
Revisado				
Aprobado				

El anterior formato se adapta según la documentación, procedimiento, metodología o gestión que se desarrolle y teniendo en cuenta algunos otros

parámetros que se utilicen para la gestión de la seguridad de la información en la empresa.

2.1 Política de Seguridad

Definición de política de la seguridad de la información de la empresa, la cual deben conocer y cumplir todos los funcionarios involucrados. El propósito de la política es preservar la información y los sistemas de la empresa, garantizando la integridad, confidencialidad y disponibilidad de la información y de los activos.

Para definir la política de la seguridad se ha empleado el Anexo – **10.1 Anexo Política de Seguridad**, en donde se estipula el esquema o contenido del documento establecido para la empresa.

2.2 Procedimientos de Auditorías Internas

Documento que define la planeación de las auditorías que se realizarán durante el periodo de certificación una vez obtenida, requisitos establecidos por los auditores internos y la plantilla de informe o reporte de auditoría.

El documento se puede establecer en el Anexo - **10.2 Anexo - 2.2 Procedimientos de Auditorías Internas**

2.3 Gestión de Indicadores

Parámetros que sirven para medir y guiar el proceso de evaluación de eficiencia y eficacia de los controles de seguridad implementados.

Los indicadores se pueden verificar en el Anexo - **10.3 Anexo - 2.3 Gestión de Indicadores**

2.4 Procedimiento Revisión por Dirección

Definición de procedimientos para la revisión del Sistema de Gestión de Seguridad de la Información por parte del área Directiva de la empresa con el objetivo de determinar el cumplimiento de los requisitos de la norma ISO/IEC 2700.
La revisión de la Alta dirección se puede verificar en el Anexo - **10.4 Anexo - 2.4 Procedimiento Revisión por Dirección**

2.5 Gestión de Roles y Responsabilidades

Conformación de un equipo denominado Comité de Seguridad, encargado de construir, proteger, monitorear y mejorar el sistema; y en donde, se establecen roles funciones y responsabilidades.

Los roles y responsabilidades están determinadas en el Anexo - **10.5 Anexo - 2.5 Gestión de Roles y Responsabilidades**

2.6 Metodología de Análisis de Riesgos

Metodología empleada para identificar y valorar los activos, amenazas y vulnerabilidades con el objetivo de visualizar un panorama de los riesgos que afronta la empresa.

El análisis de riesgos dispuesto en la empresa se lo puede verificar en el Anexo - **10.6 Anexo - 2.6 Metodología de Análisis de Riesgos**

2.7 Declaración de Aplicabilidad

Documento que describe los controles de seguridad establecidos en la empresa teniendo en cuenta su aplicabilidad, el estado y la documentación anexa.

La declaración de la aplicabilidad está determinada en el Anexo - **10.7 Anexo - 2.7 Declaración de Aplicabilidad**

3. Análisis de Riesgos

El marco de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT versión 3.0 busca orientar a la empresas u organizaciones en la gestión de los riesgos de seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) integrando la presente metodología a los diferentes casos que se puedan presentar y vinculando la identificación y el análisis de riesgos a las entidades u organizaciones. Esta metodología será aplicada al caso expuesto sobre la empresa dedicada al campo o sector de las Tecnologías de Información y las comunicaciones TIC.

3.1 Inventario de Activos

Teniendo en cuenta la norma ISO/IEC 27000:2013 un activo se define como todo aquello que tiene valor para una empresa u organización; y que por consiguiente requiere ser protegido.

Los activos se pueden agrupar en los siguientes tipos: instalaciones, datos, personal, componentes hardware, componentes software, servicios, red, equipamiento auxiliar.

Cada activo posee algunas características que permiten su identificación tales como: propietario del activo, ubicación física del activo, factor de criticidad, entre otros. Para el inventario de activos de la empresa se plantea la siguiente tabla, en donde, se tienen en cuenta el tipo de activo y las características más relevantes:

Tabla 7 – Inventario de activos de la empresa

Activo	Tipo de activo	Características	Factor de criticidad *
Servidores	**Componente hardware**	**Cantidad:** 4 **Propietario:** Jefe de redes estructuradas y servidores **Ubicación física:** CDP	**Alto**
Equipo de sobremesa	**Componente hardware**	**Cantidad:** 1 **Propietario:** Director de Finanzas **Ubicación física:** Oficina del área de Finanzas	**Alto**
Equipo de sobremesa	**Componente hardware**	**Cantidad:** 1 **Propietario:** Director de Marketing **Ubicación física:** Oficina del área de Marketing	**Alto**
Equipo de sobremesa	**Componente hardware**	**Cantidad:** 1 **Propietario:** Auxiliar o asistente administrativo	**Alto**

		Ubicación física: Oficina del área de secretaria	
Equipo de sobremesa	**Componente hardware**	**Cantidad:** 1 **Propietario:** Director de Tecnología **Ubicación física:** Oficina del área de Tecnologías de la Información	**Alto**
Equipo de sobremesa	**Componente hardware**	**Cantidad:** 1 **Propietario:** Jefe de Desarrollo de software **Ubicación física:** Oficina del área de desarrollo de software	**Alto**
Laptop	**Componente hardware**	**Cantidad:** 1 **Propietario:** Director Ejecutivo **Ubicación física:** Oficina del área de Dirección	**Alto**
Laptop	**Componente hardware**	**Cantidad:** 1 **Propietario:** Jefe de redes estructuradas y servidores **Ubicación física:** Oficina del área de redes y servidores	**Alto**
Laptop	**Componente hardware**	**Cantidad:** 1 **Propietario:** Director de Tecnología **Ubicación física:** Oficina del área de Tecnologías de la Información	**Alto**
Laptop	**Componente hardware**	**Cantidad:** 1 **Propietario:** Jefe de soporte técnico **Ubicación física:** Oficina del área de soporte técnico	**Alto**
Smartphones	**Componente hardware**	**Cantidad:** 9 **Propietario:** Cada uno de los empleados de la empresa	**Medio**
Impresora	**Componente hardware**	**Cantidad:** 1 **Propietario:** Director de Marketing **Ubicación física:** Oficina del área de Marketing	**Bajo**
Impresora	**Componente hardware**	**Cantidad:** 1 **Propietario:** Auxiliar o asistente administrativo **Ubicación física:** Oficina del área de secretaria	**Bajo**
VLANs	**Red**	**Cantidad:** 4 **Propietario:** jefe de redes y servidores	**Alto**

		Ubicación física: redes locales de cada área	
Puntos de acceso wifi	**Red**	**Cantidad:** 1 **Propietario:** jefe de redes y servidores **Ubicación física:** Oficina del área de redes y servidores	**Medio**
Puntos de acceso wifi	**Red**	**Cantidad:** 1 **Propietario:** Jefe de soporte técnico **Ubicación física:** Oficina del área soporte técnico	**Medio**
Switch	**Red**	**Cantidad:** 2 **Propietario:** jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Router	**Red**	**Cantidad:** 2 **Propietario:** jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Director Ejecutivo (CEO)	**Personal**	**Cantidad:** 1	**Medio**
Director de Finanzas (CFO)	**Personal**	**Cantidad:** 1	**Medio**
Director de Tecnología (CTO)	**Personal**	**Cantidad:** 1	**Medio**
Jefe de Redes Estructuradas y Servidores	**Personal**	**Cantidad:** 1	**Medio**
Jefe de desarrollo de software	**Personal**	**Cantidad:** 1	**Medio**
Jefe de soporte técnico	**Personal**	**Cantidad:** 1	**Medio**
Director de Marketing (CMO)	**Personal**	**Cantidad:** 1	**Medio**
Auxiliar o asistente administrativo	**Personal**	**Cantidad:** 1	**Medio**
Auxiliar de oficina	**Personal**	**Cantidad:** 1	**Medio**
Entornos de producción	**Componente Software**	**Propietario:** Director de tecnología **Ubicación física:** Servicio Cloud contratado y repositorio local.	**Alto**
Sistema	**Componente**	**Cantidad:** 9	**Medio**

Operativo Windows	**Software**	**Propietario:** Empresa con licencia respectiva **Ubicación física:** Equipos de sobremesa y laptops	
Software de servicio de correo	**Servicio**	**Cantidad:** 1 **Propietario:** Jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Software de servicio web	**Servicio**	**Cantidad:** 1 **Propietario:** Jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Software de servicio de aplicaciones	**Servicio**	**Cantidad:** 1 **Propietario:** Jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Software de servicio de base de datos	**Servicio**	**Cantidad:** 1 **Propietario:** Jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Software de servicio de archivos	**Servicio**	**Cantidad:** 1 **Propietario:** Jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Software de servicio de DNS	**Servicio**	**Cantidad:** 1 **Propietario:** Jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Software de entorno de desarrollo IDE	**Componente Software**	**Cantidad:** 1 **Propietario:** Jefe de desarrollo de software **Ubicación física:** área de desarrollo de software	**Alto**
Software de entorno marketing digital	**Componente Software**	**Cantidad:** 1 **Propietario:** Director de Marketing **Ubicación física:** área de marketing y publicidad	**Bajo**
Antivirus	**Componente Software**	**Cantidad:** 9 **Propietario:** Empresa con licencia respectiva **Ubicación física:** Equipos de sobremesa y laptops	**Medio**
Herramientas Ofimáticas	**Componente Software**	**Cantidad:** 9 **Propietario:** Empresa con licencia respectiva **Ubicación física:** Equipos de sobremesa y laptops	**Bajo**
Información	**Datos**	**Cantidad:** 13	**Alto**

empresarial		**Propietario:** Cada uno de los funcionarios o empleados de la empresa, jefes de área. **Ubicación física:** Equipos de sobremesa, laptops y smartphones, servidores.	
Información personal	**Datos**	**Cantidad:** 9 **Propietario:** Cada uno de los funcionarios o empleados de la empresa **Ubicación física:** Equipos de sobremesa, laptops y smartphones	**Medio**
Contactos de clientes y proveedores	**Datos**	**Propietario:** Director de Finanzas **Ubicación física:** Equipo de empleado que gestiona la parte administrativa de la empresa.	**Alto**
Fibra óptica	**Equipamiento auxiliar**	**Cantidad:** 1 **Propietario:** jefe de redes y servidores **Ubicación física:** CDP	**Alto**
Sistema eléctrico	**Equipamiento auxiliar**	**Cantidad:** 1 **Propietario:** jefe de redes y servidores **Ubicación física:** En todo el edificio de la empresas	**Alto**
Dispositivos de almacenamiento externos	**Media**	**Cantidad:** 1 **Propietario:** Jefe de soporte técnico **Ubicación física:** Oficina del área soporte técnico	**Medio**

* El Factor de criticidad se lo mide en la siguiente escala:

Tabla 8 – Tabla factor de criticidad de activos

Alto	El activo es altamente relevante para los procesos esenciales de la empresa y es indispensablemente disponible. La continuidad de la empresa se pone en peligro.
Medio	El activo es medianamente importante para los proceso de la empresa y su ausente disponibilidad retrasa algunos procesos. La continuidad de la empresa no se ve afectada
Bajo	El activo interviene en algunos procesos de la empresa que no están directamente relacionados con la empresa y su ausente disponibilidad causa algún contratiempo. La continuidad en ningún caso se ve afectada.

3.2 Valoración de Activos

Para la valoración de activos de la empresa se propone el análisis que realiza la metodología MAGERIT en el Libro III – Guía de Técnicas (Punto 2.1. Análisis mediante tablas) [4]. El cual permite realizar una valoración de activos utilizando una escala de calificación y una valoración cuantitativa de costos, de acuerdo a las siguientes categorías:

- **MB:** muy bajo
- **B:** bajo
- **M:** medio
- **A:** alto
- **MA:** muy alto

La Tabla 9 – Escalafón de valoración de activos, contiene la categoría de valoración de activos y su correspondiente rango de cuantificación de costos.

Tabla 9 – Escalafón de valoración de activos

Categoría	Valoración	Rango de costos ($USD)
MB	Muy bajo	< $USD 500
B	Bajo	> $USD 500, <= $USD 3.000
M	Medio	> $USD 3.000, <= $USD 10.000
A	Alto	> $USD 10.000, <= $USD 55.000
MA	Muy alto	> $USD 55.000

La valoración de activos se complementa con la definición de las dependencias de los activos de nivel superior con los activos de nivel inferior. Para ello, en la siguiente ilustración se ha establecido las dependencias de activos, según el código asignado a los activos de la empresa definido en la Tabla 18 – Asignación de código a los activos según su ámbito

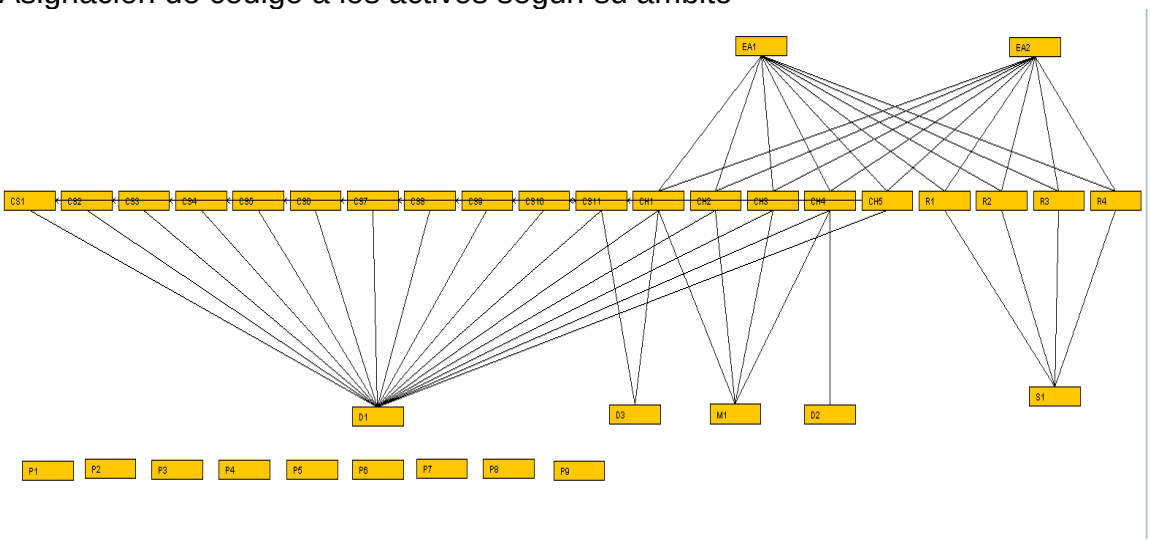

Ilustración 6 – Diagrama de dependencias de activos

Establecido el escalafón de valoración de activos y las dependencias se procede a definir la valoración de activos.

Tabla 10 – Valoración de activos según categoría de escalafón de costos y dependencias de activos

Activo	Cantidad	Categoría de escalafón de valoración	Categoría de dependencias de activos
Servidores	**4**	**M**	**R, S**
Equipos de sobremesa	**5**	**M**	**CH, CS**
Laptops	**4**	**M**	**CH, CS**
Smartphones	**9**	**B**	**CS, D, P**
Impresoras	**2**	**B**	**CH, CS, I**
VLANs	**4**	**M**	**R, EA**
Puntos de acceso wifi	**2**	**MB**	**R**
Switch	**2**	**MB**	**R**
Router	**1**	**MB**	**R**
Director Ejecutivo (CEO)	**1**	**M**	**P**
Director de Finanzas (CFO)	**1**	**B**	**P**
Director de Tecnología (CTO)	**1**	**B**	**P**
Jefe de Redes Estructuradas y Servidores	**1**	**B**	**P**
Jefe de desarrollo de software	**1**	**B**	**P**
Jefe de soporte técnico	**1**	**B**	**P**
Director de Marketing (CMO)	**1**	**B**	**P**
Auxiliar o asistente administrativo	**1**	**MB**	**P**
Auxiliar de oficina	**1**	**MB**	**P**
Entornos de producción	**1**	**MB**	**S**
Sistema Operativo Windows	**9**	**B**	**CS**
Software de servicio de correo	**1**	**B**	**CS**
Software de servicio web	**1**	**B**	**CS**
Software de servicio de aplicaciones	**1**	**B**	**CS**
Software de servicio de base de datos	**1**	**B**	**CS**
Software de servicio de archivos	**1**	**B**	**CS**
Software de servicio de DNS	**1**	**B**	**CS**
Software de entorno de desarrollo IDE	**1**	**M**	**CS**
Software de entorno marketing digital	**1**	**M**	**CS**

Antivirus	**9**	**MB**	**CS**
Herramientas Ofimáticas	**9**	**B**	**CS**
Información empresarial	**13**	**A**	**D**
Información personal	**9**	**M**	**D**
Contactos de clientes y proveedores	**1**	**M**	**D**
Fibra óptica	**1**	**B**	**R, EA**
Sistema eléctrico	**1**	**B**	**EA**
Dispositivos de almacenamiento externos	**1**	**MB**	**MEDIA**

La siguiente tabla indica los resultados de la valoración de activos según el escalafón por rango de costos y la asignación del tipo de activos.

Tabla 11 – Resultados de valoración de rangos de costos vs categoría de tipos de activos

Valoración	Categoría del tipo de activo
MB: Muy bajo	**R, S, CS, MEDIA**
B: Bajo	**I, CH, CS, P, D, R, EA**
M: Medio	**CH, CS, R, S, D**
A: Alto	**P, D**
MA: Muy alto	

Como resultado se puede concluir que las valoraciones donde se encuentran la mayoría de tipos de activos están en los rangos de Muy bajo, Bajo y Medio, perteneciente a los tipos de activos de componentes Hardware y Software, Red, Servicios y Datos. También, se puede determinar que los tipos de activos Personal y Datos se encuentran en el rango de Alto y que no existe un tipo de activo el cual tenga costos en la categoría Muy alto.

3.3 Dimensiones de Seguridad

Después de realizarse la valoración de activos, se procede a realizar la valoración ACIDT (valoración de las 5 dimensiones de la Seguridad de la Información), el cual permite medir el grado de criticidad de las dimensiones con respecto al impacto o consecuencia que tendrá la ejecución de una amenaza sobre un activo expuesto. En otras palabras, se determina la valoración del activo en la medida del perjuicio para la empresa si el activo es dañado en cierta dimensión.

Las 5 dimensiones de la seguridad de la información que se tienen en cuenta para la valoración se presentan en el siguiente esquema:

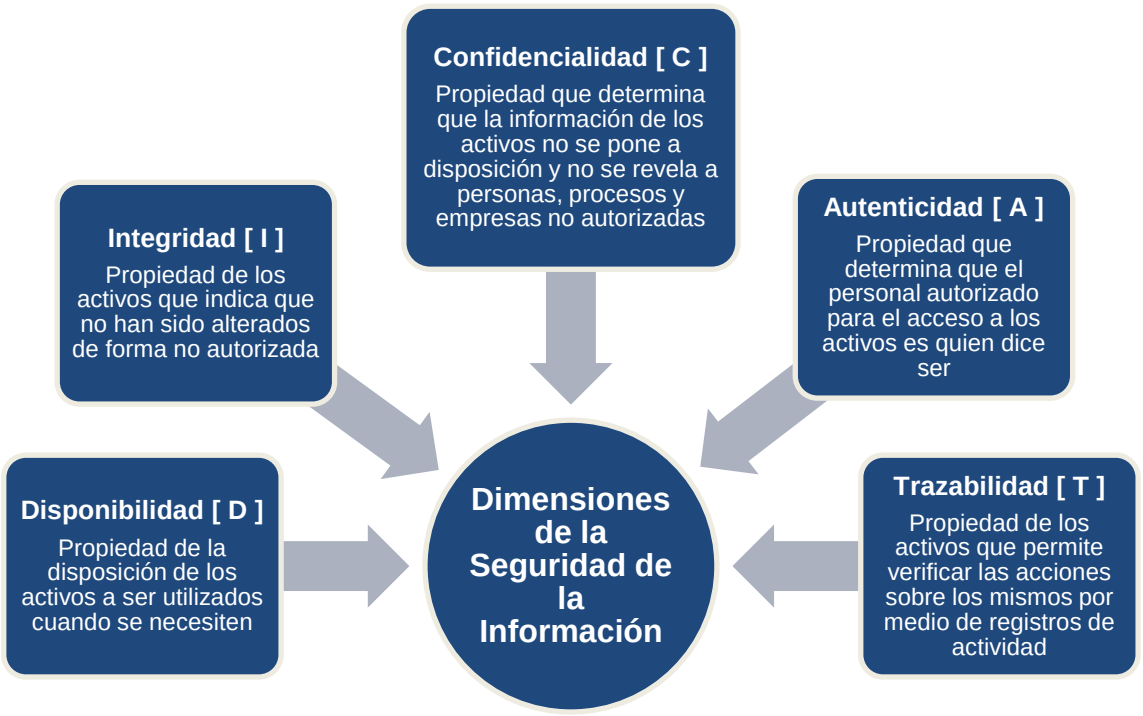

Ilustración 7 – Esquema de las dimensiones de la seguridad de la información en los activos

Teniendo en cuenta las cinco dimensiones se establece una escala para realizar las valoraciones de criticidad teniendo en cuenta los siguientes criterios

Tabla 12 – Valoraciones de criticidad de las dimensiones de seguridad

Valoración	Criterio
10	Daño muy grave a la empresa
7-9	Daño grave a la empresa
4-6	Daño importante a la empresa
1-3	Daño menor a la empresa
0	Irrelevante para la empresa

Los activos se valoran de acuerdo a su grado de importancia según los siguientes criterios:

Tabla 13 – Valoraciones según grado de importancia del activo

Valoración de grado de Importancia	Criterio
MA	Muy alta
A	Alta
M	Media
B	Baja
D	Despreciable

3.4 Tabla Resumen de Valoración

La siguiente tabla refleja la valoración de los activos según el grado de importancia de los mismos (Tabla 14) como las valoraciones de los aspectos críticos de las dimensiones de la seguridad que afectaría a los activos de la empresa (Tabla 13). Este resumen de valoración permitirá generar acciones sobre los activos que tengan un valor alto y muy alto puesto que generan un daño grave y muy grave en el funcionamiento de la empresa.

Tabla 14 – Valoración de activos

Ámbito	Activo	Valor	Aspectos críticos				
			A	C	I	D	T
CH	Servidores	A	9	8	10	10	8
CH	Equipos de sobremesa	A	8	8	7	8	7
CH	Laptops	A	8	8	7	8	7
CH	Smartphones	M	6	5	5	6	5
CH	Impresoras	D	0	0	0	1	0
R	VLANs	MA	10	10	9	10	5
R	Puntos de acceso wifi	A	7	8	7	8	3
R	Switch	A	7	7	8	8	3
R	Router	A	9	9	9	10	3
P	Director Ejecutivo (CEO)	MA	10	10	9	7	3
P	Director de Finanzas (CFO)	MA	10	10	9	8	5
P	Director de Tecnología (CTO)	MA	10	10	9	10	5
P	Jefe de Redes Estructuradas y Servidores	A	9	9	9	9	6
P	Jefe de desarrollo de software	A	8	8	8	7	5
P	Jefe de soporte técnico	M	7	6	7	7	4
P	Director de Marketing (CMO)	M	6	7	5	5	2
P	Auxiliar o asistente administrativo	M	5	6	5	7	3
P	Auxiliar de oficina	B	4	4	3	4	1
S	Entornos de producción	A	7	7	8	8	4
CS	Sistema Operativo Windows	M	4	6	5	5	0
CS	Software de servicio de correo	A	7	7	8	8	5
CS	Software de servicio web	A	7	7	9	10	6
CS	Software de servicio de aplicaciones	A	7	8	9	9	7

CS	**Software de servicio de base de datos**	**A**	**7**	**9**	**9**	**9**	**6**
CS	**Software de servicio de archivos**	**M**	**7**	**6**	**7**	**7**	**4**
CS	**Software de servicio de DNS**	**M**	**5**	**4**	**5**	**6**	**2**
CS	**Software de entorno de desarrollo IDE**	**M**	**6**	**7**	**7**	**6**	**5**
CS	**Software de entorno marketing digital**	**B**	**4**	**3**	**3**	**4**	**3**
CS	**Antivirus**	**M**	**4**	**6**	**7**	**8**	**1**
CS	**Herramientas Ofimáticas**	**D**	**0**	**0**	**0**	**2**	**0**
D	**Información empresarial**	**MA**	**9**	**10**	**10**	**10**	**6**
D	**Información personal**	**B**	**0**	**2**	**0**	**0**	**0**
D	**Contactos de clientes y proveedores**	**M**	**6**	**9**	**9**	**8**	**3**
EA	**Fibra óptica**	**A**	**8**	**6**	**7**	**9**	**4**
EA	**Sistema eléctrico**	**MA**	**3**	**4**	**8**	**10**	**4**
MEDIA	**Dispositivos de almacenamiento externos**	**A**	**7**	**8**	**9**	**9**	**4**

3.5 Análisis de Amenazas

Para realizar el análisis de amenazas a las que están expuestos los activos de la empresa, se empleará una tabla definida en la metodología MAGERIT (Libro II – Catálogo de Elementos) donde se establece los tipos de amenaza que podemos clasificar y organizar en referencia a los activos afectados.

Tabla 15 – Tipos de amenazas

Tipo de amenaza	Código
Desastres naturales	**N**
De origen industrial	**I**
Errores y fallos no intencionados	**E**
Ataques intencionados	**A**

También, se tendrá en cuenta la siguiente tabla para realizar un análisis en cuanto a la frecuencia o periodicidad con la que se produce una amenaza asignando un valor y una escala a dicha frecuencia.

Tabla 16 – Frecuencia con la que se produce una amenaza

Valor	Escala de Frecuencia
1	**MB:** Muy Bajo
2	**B:** Bajo
3	**M:** Medio

4	**A:** Alto
5	**MA:** Muy Alto

Para realizar un análisis estructurado de las amenazas que afectarían a los activos de la empresa, se empleará la siguiente tabla donde se establece un rango de valores porcentuales en relación a la escala de impacto que produce la amenaza en las dimensiones de la seguridad de la información.

Tabla 17 – Impacto que produce la amenaza en las dimensiones de seguridad

Rango de valor en porcentajes	Escala de Impacto
<= 20%	**MB:** Muy Bajo
>20%, <=40%	**B:** Bajo
>40%, <=60%	**M:** Medio
>60%, <=80%	**A:** Alto
>80%, <=100%	**MA:** Muy Alto

Completando el análisis de las amenazas, se presenta la siguiente tabla que pretende codificar los activos valorados en la empresa con el objetivo de presentar de forma más organizada la información de dichos activos teniendo en cuenta el ámbito o el tipo de activo.

Tabla 18 – Asignación de código a los activos según su ámbito

Ámbito	Activo	Código
CH	**Servidores**	**CH1**
	Equipos de sobremesa	**CH2**
	Laptops	**CH3**
	Smartphones	**CH4**
	Impresoras	**CH5**
R	**VLANs**	**R1**
	Puntos de acceso wifi	**R2**
	Switch	**R3**
	Router	**R4**
P	**Director Ejecutivo (CEO)**	**P1**
	Director de Finanzas (CFO)	**P2**
	Director de Tecnología (CTO)	**P3**
	Jefe de Redes Estructuradas y Servidores	**P4**
	Jefe de desarrollo de software	**P5**
	Jefe de soporte técnico	**P6**
	Director de Marketing (CMO)	**P7**
	Auxiliar o asistente administrativo	**P8**
	Auxiliar de oficina	**P9**
S	**Entornos de producción**	**S1**
CS	**Sistema Operativo Windows**	**CS1**
	Software de servicio de correo	**CS2**
	Software de servicio web	**CS3**
	Software de servicio de aplicaciones	**CS4**

	Software de servicio de base de datos	**CS5**
	Software de servicio de archivos	**CS6**
	Software de servicio de DNS	**CS7**
	Software de entorno de desarrollo IDE	**CS8**
	Software de entorno marketing digital	**CS9**
	Antivirus	**CS10**
	Herramientas Ofimáticas	**CS11**
D	**Información empresarial**	**D1**
	Información personal	**D2**
	Contactos de clientes y proveedores	**D3**
EA	**Fibra óptica**	**EA1**
	Sistema eléctrico	**EA2**
MEDIA	**Dispositivos de almacenamiento externos**	**M1**

Como resultado del análisis de las amenazas que pueden afectar a los activos de la empresa se presenta la siguiente tabla resumen, en donde, se establece los diferentes amenazas de acuerdo al tipo acordado en la metodología MAGERIT (Libro II – Catálogo de Elementos), el código de los activos de la empresa que podrían verse afectados, el valor asignado de la frecuencia con la que se produce la amenaza, y el impacto definido en porcentajes que produce la amenaza en las dimensiones (ACIDT) de la seguridad.

Tabla 19 – Amenazas en los activos y las dimensiones de la seguridad

Tipo de Amenaza: N – Desastres Naturales							
Amenaza	**Activos afectados**	**F***	**Impacto de la amenaza (%)**				
			A	**C**	**I**	**D**	**T**
[N.1] Fuego	CH1-CH5, R1-R4, M1, EA1,EA2					70%	
[N.2] Daños por agua	CH1-CH5, R1-R4, M1, EA1,EA2					70%	
[N.*] Desastres naturales	CH1-CH5, R1-R4, M1, EA1,EA2					70%	
Tipo de Amenaza: I – Origen Industrial							
Amenaza	**Activos afectados**	**F***	**Impacto de la amenaza (%)**				
			A	**C**	**I**	**D**	**T**
[I.1] Fuego	CH1-CH5, R1-R4, M1, EA1,EA2	2				70%	
[I.2] Daños por agua	CH1-CH5, R1-R4, M1, EA1,EA2	2				70%	
[I.*] Desastres industriales	CH1-CH5, R1-R4, M1, EA1,EA2	1				70%	
[I.3] Contaminación mecánica	CH1-CH5, R1-R4, M1, EA1,EA2	3				80%	
[I.4] Contaminación electromagnética	CH1-CH5, R1-R4, M1, EA1,EA2	1				70%	
[I.5] Avería de origen físico o lógico	CH1-CH5, CS1-CS11, M1, EA1	4			60%	70%	
[I.6] Corte del suministro eléctrico	CH1-CH5, R1-R4, M1, EA1,EA2	2				80%	

[I.7] Condiciones inadecuadas de temperatura o humedad	CH1-CH5, R1-R4, M1, EA1,EA2	3				80%	
[I.8] Fallo de servicios de comunicaciones	R1-R4	3				50%	
[I.9] Interrupción de otros servicios y suministros esenciales	CH5	3				10%	
[I.10] Degradación de los soportes de almacenamiento de la información	M1	4				50%	
Tipo de Amenaza: E – Errores y fallos no intencionados							
Amenaza	**Activos afectados**	**F***	**Impacto de la amenaza (%)**				
			A	**C**	**I**	**D**	**T**
[E.1] Errores de los usuarios	D1-D3, S1, CS1-CS11, M1	5		60%	60%	60%	
[E.2] Errores del administrador	CH1-CH5, CS1-CS11, D1-D3, R1-R4, S1, M1	3		70%	70%	70%	
[E.3] Errores de monitorización (log)	D1	2			40%		40%
[E.4] Errores de configuración	D1	3			70%		
[E.7] Deficiencias en la organización	P1-P9	3				70%	
[E.8] Difusión de software dañino	CS1-CS11	4		80%	80%	80%	
[E.9] Errores de [re-]encaminamiento	CS2-CS7, S1, R1-R4	1		50%			
[E.10] Errores de secuencia	CS2-CS7, S1, R1-R4				60%		
[E.15] Alteración accidental de la información	D1-D3, S1, CS1-CS11, M1, R1	2			90%		
[E.18] Destrucción de información	D1-D3, S1, CS1-CS11, M1, R1	2			80%	80%	
[E.19] Fugas de información	D1-D3, S1, CS1-CS11, M1, R1	3		60%			
[E.20] Vulnerabilidades de los programas (software)	CS1-CS11	4		40%	60%	80%	
[E.21] Errores de mantenimiento / actualización de programas (software)	CS1-CS11	5			60%	80%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	CH1-CH5, M1, EA1-EA2, R1-R4	3				80%	

[E.24] Caída del sistema por agotamiento de recursos	CH1-CH5, M1, EA1-EA2, R1-R4	3				60%	
[E.25] Pérdida de equipos	CH1-CH5, M1, EA1-EA2, R1-R4	3		40%		80%	
[E.28] Indisponibilidad del personal	P1-P9	3				40%	
Tipo de Amenaza: A – Ataques intencionados							
Amenaza	**Activos afectados**	**F***	**Impacto de la amenaza (%)**				
			A	**C**	**I**	**D**	**T**
[A.3] Manipulación de los registros de actividad (log)	D1	3			50%		60%
[A.4] Manipulación de la configuración	D1	3		50%	60%	60%	
[A.5] Suplantación de la identidad del usuario	D1-D3, S1, CS1-CS11, R1-R4	4	100 %	100 %	100 %		
[A.6] Abuso de privilegios de acceso	D1-D3, S1, CS1-CS11, R1-R4	2		60%	70%	70%	
[A.7] Uso no previsto	CH1-CH5, CS1-CS11, EA1-EA2, R1-R4, S1, M1	2		40%	60%	60%	
[A.8] Difusión de software dañino	CS1-CS11	3		60%	80%	80%	
[A.9] [Re-]encaminamiento de mensajes	S1, CS1-CS11, R1-R4	2		40%			
[A.10] Alteración de secuencia	S1, CS1-CS11, R1-R4	3			50%		
[A.11] Acceso no autorizado	CH1-CH5, CS1-CS11, D1-D3, EA1-EA2, R1-R4, S1, M1	3		80%	90%		
[A.12] Análisis de tráfico	R1-R4	4		90%			
[A.13] Repudio	S1, D1	2			40%		50%
[A.14] Interceptación de información (escucha)	R1-R4	3		80%			
[A.15] Modificación deliberada de la información	CS1-CS11, D1-D3, R1-R4, S1, M1	3			100 %		
[A.18] Destrucción de información	CS1-CS11, D1-D3, S1, M1	5				100 %	
[A.19] Divulgación de información	CS1-CS11, D1-D3, R1-R4, S1, M1	3		70%			
[A.22] Manipulación de programas	CS1-CS11	2		40%	80%	80%	

[A.23] Manipulación de los equipos	CH1-CH5, M1, EA1-EA2	2		50%		90%	
[A.24] Denegación de servicio	CH1-CH5, R1-R4, S1	4				100 %	
[A.25] Robo	CH1-CH5, M1, EA1-EA2	2		60%		80%	
[A.26] Ataque destructivo	CH1-CH5, M1, EA1-EA2	2				80%	
[A.28] Indisponibilidad del personal	P1-P9	4				70%	
[A.29] Extorsión	P1, P2, P3, P4, P7	2		70%	70%	70%	
[A.30] Ingeniería social (picaresca)	P1-P9	2		60%	70%	60%	

***F** – define la escala de frecuencia con la que se produce una amenaza

3.6 Impacto Potencial

El impacto potencial es la medida del daño sobre el activo derivado de la materialización de una amenaza [5]. Con los análisis realizados en las tablas anteriores se puede calcular el impacto potencial, con el propósito de tomar las medidas respectivas para reducir los riesgos y tomar las decisiones de acuerdo al grado de aceptación.

La tabla que se presenta a continuación permite establecer la valoración de los niveles de impacto que se puede determinar teniendo en cuenta el rango del impacto en porcentajes, el rango del impacto en valores decimales, el rango del impacto en valores enteros y su valor asignado definitivo.

Tabla 20- Escala de niveles de impacto

Impacto	Rango del Impacto en %	Rango del Impacto en decimal	Rango del Impacto en valores	Valor
N: Nulo	0%	0	0	**0**
MB: Muy Bajo	>0%,<=10%	>0,<=0,1	>0,<=1	**1**
B: Bajo	>10%,<=20%	>0,1,<=0,2	>1,<=2	**2**
M: Medio	>20%,<=50%	>0,2,<=0,5	>2,<=5	**3**
A: Alto	>50%,<=80%	>0,5,<=0,8	>5,<=8	**4**
MA: Muy alto	>80%,<=100%	>0,8,<=1,0	>8,<=10	**5**

Para obtener el impacto potencial se utiliza la siguiente formula en donde se calcula el valor del activo por el porcentaje del impacto de amenaza:

Impacto potencial = Valoración de activos X Porcentaje de impacto de amenaza

La siguiente tabla indica los registros de los impactos potenciales calculados en la empresa según las dimensiones de la seguridad ACIDT establecidas en las

valoraciones de los activos, el impacto de amenazas y el valor del impacto potencial según la formula presentada.

Tabla 21 – Cálculo y registro del Impacto Potencial

Activo	Valoración de activos					Impacto de amenaza* (% / 100)					Impacto Potencial en valores				
	A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
Servidores	9	8	10	10	8	0	1,0	1,0	1,0	0	0	8	10	10	0
Equipos de sobremesa	8	8	7	8	7	0	0,8	0,8	0,8	0	0	6,4	5,6	6,4	0
Laptops	8	8	7	8	7	0	0,8	0,8	0,8	0	0	6,4	5,6	6,4	0
Smartphones	6	5	5	6	5	0	0,8	0,8	0,8	0	0	4	4	4,8	0
Impresoras	0	0	0	1	0	0	0,5	0,5	0,5	0	0	0	0	0,5	0
VLANs	10	10	9	10	5	1,0	1,0	1,0	1,0	0	10	10	9	10	0
Puntos de acceso wifi	7	8	7	8	3	0	0,7	0,7	0,7	0	0	5,6	4,9	5,6	0
Switch	7	7	8	8	3	0	0,7	0,7	0,7	0	0	4,9	5,6	5,6	0
Router	9	9	9	10	3	0	0,8	0,8	0,8	0	0	7,2	7,2	8	0
Director Ejecutivo (CEO)	10	10	9	7	3	0	1,0	0,8	0,8	0	0	6,4	7,2	5,6	0
Director de Finanzas (CFO)	10	10	9	8	5	0	0,8	0,8	0,8	0	0	8	7,2	6,4	0
Director de Tecnología (CTO)	10	10	9	10	5	0	0,8	0,8	1,0	0	0	8	7,2	10	0
Jefe de Redes Estructuradas y Servidores	9	9	9	9	6	0	0,7	0,7	0,7	0	0	6,3	6,3	6,3	0
Jefe de desarrollo de software	8	8	8	7	5	0	0,6	0,7	0,7	0	0	4,8	5,6	4,9	0
Jefe de soporte técnico	7	6	7	7	4	0	0,5	0,5	0,5	0	0	3	3,5	3,5	0
Director de Marketing (CMO)	6	7	5	5	2	0	0,5	0,5	0,5	0	0	3,5	2,5	2,5	0
Auxiliar o asistente administrativo	5	6	5	7	3	0	0,4	0,4	0,4	0	0	2,4	2	2,8	0
Auxiliar de oficina	4	4	3	4	1	0	0,2	0,2	0,2	0	0	0,8	0,6	0,8	0
Entornos de producción	7	7	8	8	4	0,7	0,7	0,7	0,7	0	4,9	4,9	5,6	5,6	0
Sistema Operativo Windows	4	6	5	5	0	0,7	0,7	0,7	0,7	0	2,8	4,2	3,5	3,5	0
Software de servicio de correo	7	7	8	8	5	0,8	0,8	0,8	0,8	0	5,6	5,6	6,4	6,4	0
Software de servicio web	7	7	9	10	6	0,8	0,8	0,8	0,8	0	5,6	5,6	7,2	8	0
Software de servicio de aplicaciones	7	8	9	9	7	0,8	0,8	0,8	0,8	0	5,6	6,4	7,2	7,2	0
Software de servicio de base de datos	7	9	9	9	6	0,8	0,8	0,8	0,8	0	5,6	7,2	7,2	7,2	0

Software de servicio de archivos	7	6	7	7	4	0,7	0,7	0,7	0,7	0	4,9	4,2	4,9	4,9	0
Software de servicio de DNS	5	4	5	6	2	0,7	0,7	0,7	0,7	0	3,5	2,8	3,5	4,2	0
Software de entorno de desarrollo IDE	6	7	7	6	5	0,7	0,7	0,7	0,7	0	4,2	4,9	4,9	4,2	0
Software de entorno marketing digital	4	3	3	4	3	0,7	0,7	0,7	0,7	0	2,8	2,1	2,1	2,8	0
Antivirus	4	6	7	8	1	0,8	0,8	0,8	0,8	0	3,2	4,8	5,6	6,4	0
Herramientas Ofimáticas	0	0	0	2	0	0,7	0,7	0,7	0,7	0	0	0	0	1,4	0
Información empresarial	9	10	10	10	6	1,0	1,0	1,0	1,0	1,0	9	10	10	10	6
Información personal	0	2	0	0	0	0,1	0,1	0,1	0,1	0,1	0	2	0	0	0
Contactos de clientes y proveedores	6	9	9	8	3	1,0	1,0	1,0	1,0	1,0	6	9	9	8	3
Fibra óptica	8	6	7	9	4	0,6	0,6	0,6	0,6	0	4,8	3,6	4,2	5,4	0
Sistema eléctrico	3	4	8	10	4	0,7	0,7	0,7	0,7	0	2,1	2,8	5,6	7	0
Dispositivos de almacenamiento externos	7	8	9	9	4	0,7	0,7	0,7	0,7	0	4,9	5,6	6,3	6,3	0

Impacto de amenaza* - El impacto de amenaza se calcula teniendo en cuenta el valor en porcentaje sobre cien (%/100) el cual da un valor decimal.

3.7 Nivel de Riesgo Aceptable y Riesgo Residual

Para establecer el nivel de riesgo aceptable el cual permite definir el límite al que la empresa decide asumir el riesgo y aplicar controles, se propone realizar el análisis teniendo en cuenta la frecuencia de ocurrencia y sus niveles en cada uno de los activos con el objetivo de realizar la valoración del riesgo.

A continuación se indica la tabla de frecuencia de ocurrencia para establecer el valor teniendo en cuenta la misma:

Tabla 22 – Frecuencia de ocurrencia

Valor	frecuencia de ocurrencia	Niveles de frecuencia de ocurrencia
0,01	Varios años	**MB:** Muy Bajo
0,1	Más de 2 años	**B:** Bajo
1	Anual	**N:** Normal
10	Mensual	**A:** Alto
100	Diaria	**MA:** Muy Alto

Continuando con el análisis de riesgo aceptable y riesgo residual se establece la siguiente tabla de los niveles de riesgo que permite a través del rango de valoración identificar en qué estado se encuentra la valoración con respecto al impacto potencial registrados en la tabla 21.

En el análisis se ha establecido que el umbral de riesgo para los valores mayores a seis (>6) clasificados en los niveles Alto y Muy Alto, se deben

implementar controles o salvaguardas que permitan reducir los niveles de riesgos en los activos identificados en relación al parámetro mencionado. La tabla 23 indica lo establecido marcado con color verde.

Tabla 23 – Niveles de riesgo

Niveles	Rango de valoración de riesgo
MB: Muy Bajo	>0,<=1
B: Bajo	>1,<=3
M: Medio	>3,<=6
A: Alto	>6,<=8
MA: Muy Alto	>8,<=10

Una vez determinado el valor de la frecuencia de ocurrencia y obtenido el valor del impacto potencial, se procede a calcular la valoración del riesgo que permita identificar los activos que requieran implantar medidas o controles para la reducción de los riesgos en cuanto a las amenazas identificadas. Para ello, se utiliza la siguiente formula permitiendo establecer los valores de riesgo:

Valoración de riesgo = Valor de frecuencia de ocurrencia X Valor del Impacto Potencial

La siguiente tabla establece el análisis y cálculo realizado teniendo en cuanta la fórmula para la valoración de riesgos en los activos establecidos en la empresa:

Tabla 24 – Valoración de riesgo según la frecuencia de ocurrencia y el impacto potencial

Activo	Frecuencia de ocurrencia (valor)	Impacto Potencial en valores					Valoración de riesgo				
		A	C	I	D	T	A	C	I	D	T
Servidores	1	0	8	10	10	0	0	8	10	10	0
Equipos de sobremesa	1	0	6,4	5,6	6,4	0	0	6,4	5,6	6,4	0
Laptops	1	0	6,4	5,6	6,4	0	0	6,4	5,6	6,4	0
Smartphones	1	0	4	4	4,8	0	0	4	4	4,8	0
Impresoras	1	0	0	0	0,5	0	0	0	0	0,5	0
VLANs	1	10	10	9	10	0	10	10	9	10	0
Puntos de acceso wifi	1	0	5,6	4,9	5,6	0	0	5,6	4,9	5,6	0
Switch	1	0	4,9	5,6	5,6	0	0	4,9	5,6	5,6	0
Router	1	0	7,2	7,2	8	0	0	7,2	7,2	8	0
Director Ejecutivo (CEO)	1	0	6,4	7,2	5,6	0	0	6,4	7,2	5,6	0

Director de Finanzas (CFO)	1	0	8	7,2	6,4	0	0	8	7,2	6,4	0
Director de Tecnología (CTO)	1	0	8	7,2	10	0	0	8	7,2	10	0
Jefe de Redes Estructuradas y Servidores	1	0	6,3	6,3	6,3	0	0	6,3	6,3	6,3	0
Jefe de desarrollo de software	1	0	4,8	5,6	4,9	0	0	4,8	5,6	4,9	0
Jefe de soporte técnico	1	0	3	3,5	3,5	0	0	3	3,5	3,5	0
Director de Marketing (CMO)	1	0	3,5	2,5	2,5	0	0	3,5	2,5	2,5	0
Auxiliar o asistente administrativo	1	0	2,4	2	2,8	0	0	2,4	2	2,8	0
Auxiliar de oficina	1	0	0,8	0,6	0,8	0	0	0,8	0,6	0,8	0
Entornos de producción	1	4,9	4,9	5,6	5,6	0	4,9	4,9	5,6	5,6	0
Sistema Operativo Windows	1	2,8	4,2	3,5	3,5	0	2,8	4,2	3,5	3,5	0
Software de servicio de correo	1	5,6	5,6	6,4	6,4	0	5,6	5,6	6,4	6,4	0
Software de servicio web	1	5,6	5,6	7,2	8	0	5,6	5,6	7,2	8	0
Software de servicio de aplicaciones	1	5,6	6,4	7,2	7,2	0	5,6	6,4	7,2	7,2	0
Software de servicio de base de datos	1	5,6	7,2	7,2	7,2	0	5,6	7,2	7,2	7,2	0
Software de servicio de archivos	1	4,9	4,2	4,9	4,9	0	4,9	4,2	4,9	4,9	0
Software de servicio de DNS	1	3,5	2,8	3,5	4,2	0	3,5	2,8	3,5	4,2	0
Software de entorno de desarrollo IDE	1	4,2	4,9	4,9	4,2	0	4,2	4,9	4,9	4,2	0
Software de entorno marketing digital	1	2,8	2,1	2,1	2,8	0	2,8	2,1	2,1	2,8	0
Antivirus	1	3,2	4,8	5,6	6,4	0	3,2	4,8	5,6	6,4	0
Herramientas Ofimáticas	1	0	0	0	1,4	0	0	0	0	1,4	0
Información empresarial	1	9	10	10	10	6	9	10	10	10	6
Información personal	1	0	2	0	0	0	0	2	0	0	0
Contactos de clientes y proveedores	1	6	9	9	8	3	6	9	9	8	3
Fibra óptica	1	4,8	3,6	4,2	5,4	0	4,8	3,6	4,2	5,4	0
Sistema eléctrico	1	2,1	2,8	5,6	7	0	2,1	2,8	5,6	7	0
Dispositivos de almacenamiento externos	1	4,9	5,6	6,3	6,3	0	4,9	5,6	6,3	6,3	0

Como resultados según el análisis realizado por la tabla, de los 36 activos establecidos en la empresa, 19 se identificaron en los niveles Alto y Muy Alto

por encima del umbral del riesgo afectando las dimensiones de seguridad (Confidencialidad, Integridad y Disponibilidad) mayormente; 11 se identificaron en el nivel Medio; y 6 se identificaron en los niveles Bajo y Muy Bajo. Cabe resaltar, que en algunos activos se ven afectados algunas dimensiones de la seguridad más que otras, por lo tanto los valores resultantes varían según su análisis.

De igual manera, en esta etapa se define que el propietario del riesgo, persona encargada de tomar estrategias y decisiones conforme al riesgo identificado para el activo a su cargo; será el mismo propietario del activo, teniendo la responsabilidad de establecer los controles de reducción de riesgos junto con el responsable de seguridad (Director de Tecnología CTO) de la empresa.

4. Propuesta de Proyectos

4.1 Evaluación de Propuestas

En esta etapa se identifica los proyectos para implementar en el SGSI en el marco del mejoramiento de los controles de seguridad y a reducir o mitigar los niveles de riesgos encontrados en la etapa de análisis de riesgos. A continuación se enumeran los nombres de los proyectos que se tienen en cuenta para la propuesta:

- P001 - Política de seguridad de la Información.
- P002 - Gestión de redes y comunicaciones.
- P003 - Seguridad y mantenimiento de los equipos y recursos.
- P004 - Organización y formación al personal en seguridad de la información.
- P005 - Implementación de un CPD auxiliar para soporte de servidores y servicios.
- P006 - Organización y clasificación de la información.
- P007 - Mejoramiento en los sistemas de gestión de usuarios.

Se determinará un esquema general para identificar cada proyecto acorde con la siguiente estructura:

- **Nombre del Proyecto:** nombre o título asignado al proyecto.
- **Código:** código asignado al proyecto.
- **Objetivos de mejora:** objetivos que cumplirá el proyecto en su implantación.
- **Justificación:** descripción del proyecto teniendo en cuenta los objetivos de mejoramiento de los controles de seguridad del SGSI.
- **Controles Identificados:** controles identificados en los dominios y subdominios de la norma ISO 27002.
- **Activos afectados:** activos identificados en la empresa que pueden ser afectados en la implantación del proyecto.
- **Puntos de control o medidores:** medidores o controles que permiten verificar el resultado y comprobar la ejecución del proyecto.
- **Responsable de ejecución del proyecto:** persona responsables de la ejecución de las acciones definidas para cada proyecto.
- **Presupuesto:** presupuesto proyectado para la implantación del proyecto.
- **Plazos de consecución y fecha límite de cumplimiento:** tiempo destinado para la ejecución del proyecto planteado.

A continuación se presenta la propuesta de los proyectos estipulados en la tabla.

Tabla 25 – Propuesta de proyectos para la implementación en el SGSI

Nombre del Proyecto:	Política de seguridad de la Información	**Código:**	P001
Objetivos de	• Definir y establecer la política de seguridad de la		

mejora:	información en la empresa.
Justificación:	Como propuesta inicial se debe elaborar la política de seguridad que permita orientar y servir de apoyo en la seguridad de la información de acuerdo con los propósitos de la empresa. Las políticas deben revisarse periódicamente (1 o 2 veces) cada año y se deben establecer en todos los niveles de la empresa.

Controles Identificados:	**Activos afectados:**
A.5.1.1 Políticas para la seguridad de la información A.5.1.2 Revisión de las políticas para la seguridad de la información	CH1-CH5, CS1-CS11, P1-P9, R1-R4, S1, D1-D3, EA1-EA2, M1

Puntos de control o medidores:	• Documentos sobre la política de seguridad de la información aprobada por las directivas y el comité de seguridad. • Revisión de documentación de la política de seguridad. • Comunicación y publicación de la política de seguridad al personal de la empresa.
Responsable de ejecución del proyecto:	Director de Tecnología (CTO)
Presupuesto:	El presupuesto se plantea por jornadas laborales de 8 horas diarias de lunes a viernes. • Horas de trabajo semanal: 40 horas • Total horas por los 2 meses: 320 horas • Costo hora: $USD 8.28 • Costo Total por los 2 meses: $USD 2,649
Plazos de consecución y fecha límite de cumplimiento:	El cumplimiento de los objetivos debe realizarse a corto plazo; por lo tanto, se establece un tiempo de 2 meses para su realización.

Nombre del Proyecto:	Gestión de redes y comunicaciones	**Código:**	P002
Objetivos de mejora:	• Aplicar controles para establecer las reglas de acceso de la información en las redes y servicios de la empresa. • Mejorar el uso y control de las redes de datos para garantizar la confidencialidad, integridad y disponibilidad en los servicios y recursos.		
Justificación:	El asegurar la protección de los recursos y servicios de la infraestructura de red y de comunicaciones de la empresa permite garantizar el intercambio de información interna y externa de forma más confiable y segura. Por lo tanto, se hace necesario establecer controles, monitoreo o seguimientos, asegurar servicios y definir acuerdos y políticas para el intercambio de información en las redes. Así mismo, se requiere realizar actualizaciones en los sistemas de		

	información comprendidos en la red con el objetivo de optimizar los recursos y servicios dependiendo del crecimiento en la misma.

Controles Identificados:	Activos afectados:
A.9.1.2 Acceso a redes y a servicios en red A.13.1 Gestión de la seguridad de las redes A.13.2 Transferencia de información	CH1, CH2, CH3, R1-R4, S1

Puntos de control o medidores:	• Verificación de la aplicación de los controles y de la optimización en el uso y gestión de las redes. • Monitoreo y registro de los estados de las redes, recursos y dispositivos que conforman la infraestructura de la redes dentro de la empresa. • Reportes generados del monitoreo y diagnóstico realizado a la infraestructura de red y los servicios.
Responsable de ejecución del proyecto:	Jefe de Redes y Servidores.
Presupuesto:	Para esta propuesta se tiene un presupuesto de $USD 3.000
Plazos de consecución y fecha límite de cumplimiento:	Para la realización de la propuesta se tiene estipulado un periodo de mediano plazo de 6 meses para su ejecución.

Nombre del Proyecto:	Seguridad y mantenimiento de los equipos y recursos	**Código:**	P003
Objetivos de mejora:	• Garantizar la disponibilidad e integridad de los equipos, recursos, activos y sistemas de información en la empresa.		
Justificación:	Las medidas de seguridad que debe tener la empresa en relación a la seguridad de los equipos y activos permitirán detectar y prevenir incidentes o fallas que alteren los procesos de la empresa en su correcto funcionamiento. De modo similar, el mantenimiento adecuado de los equipos y recursos físicos permitirá brindar un continuo funcionamiento de estos, incluso, con el seguimiento periódico logrará cumplir de forma exitosa este objetivo.		

Controles Identificados:	Activos afectados:
A.8.1 Responsabilidad por los activos A.8.2 Clasificación de la información A.11.2 Equipos A.14.1 Requisitos de seguridad de los sistemas de información	CH1-CH5, R2-R4, EA1-EA2, M1, CS1-CS11

Puntos de control o medidores:	• Sistematización y organización del inventario de activos utilizando herramientas que permiten disponer de la información de forma más efectiva. • Control de responsabilidades y clasificación de activos

	por medio de la utilización de herramientas que se utilizan para tal fin. • Mantenimiento (preventivo y correctivo) realizado a los equipos, dispositivos, equipamiento auxiliar, etc. • Implementación de medidas de protección a los equipos (UPS) y revisión periódica de funcionamiento. • Revisión frecuente de la seguridad en el desarrollo de los sistemas de información con entrega de informes sobre eventualidades y situación actual de la seguridad.
Responsable de ejecución del proyecto:	Jefe de Soporte Técnico.
Presupuesto:	Para el presupuesto de esta propuesta se tiene definido los siguientes aspectos: • Adquisición de software para inventario, clasificación y asignación de equipos y activos: $USD 5.409 • Mantenimiento de equipos y recursos: $USD 8.114 (4 veces al año) • Adquisición de UPS (6): $USD 4.868. • Contratación de personal para realizar seguimiento y revisión de la seguridad en el desarrollo de los sistemas de información: $USD 5.409 Total del presupuesto: $USD 23.800
Plazos de consecución y fecha límite de cumplimiento:	La realización de la propuesta está determinada en un plazo de 1 año con posteriores ejecuciones durante los próximos años (largo plazo)

Nombre del Proyecto:	Organización y formación al personal en seguridad de la información	**Código:**	P004
Objetivos de mejora:	• Establecer y disponer de un plan de formación en temáticas relacionadas a la seguridad de la información enfocado al personal de la empresa con el objetivo de preparar al mismo para enfrentar situaciones e incidentes y mitigar riesgos que afecten los activos de la empresa.		
Justificación:	Elaborar un plan de inducción y formación que permita capacitar al personal de la empresa EXPERTEC en temas relacionados a la seguridad de la información. Para ello se propone realizar cursos orientados a la seguridad tales como: curso básico de seguridad, curso de desarrollo seguro, curso de ciberseguridad, curso de hacking ético, curso de protección y privacidad de la información. Los cursos varían de acuerdo al público objetivo dependiendo de las funciones y responsabilidades de cada empleado de la empresa.		
Controles Identificados:		**Activos afectados:**	

A.6.1 Organización interna A.6.2 Dispositivos móviles y teletrabajo A.7.1 Antes de asumir el empleo A.7.2 Durante la ejecución del empleo A.7.3 Terminación y cambio de empleo	P1-P9

Puntos de control o medidores:	• Documento que especifique la separación de funciones, roles y responsabilidades del personal en las áreas de la empresa. • Documento donde se establezca la política de teletrabajo debido a la situación de pandemia por el COVID19 junto con las evidencias de formación al personal. • Jornadas de inducción y capacitación sobre responsabilidades y obligaciones de los empleados en relación a la seguridad y privacidad de la información evidenciando las capacitaciones por medio de documentos, registros fotográficos y prácticas.
Responsable de ejecución del proyecto:	Jefe de Soporte Técnico
Presupuesto:	El presupuesto planteado para la capacitación o formación del personal es de $USD 2.700
Plazos de consecución y fecha límite de cumplimiento:	El plazo de la consecución de la propuesta está planteada durante 1 año (mediano plazo) con ampliación de los siguientes años ya que se establecen capacitaciones y actualizaciones al personal (largo plazo)

Nombre del Proyecto:	Implementación de un CPD auxiliar para soporte de servidores y servicios	**Código:**	P005
Objetivos de mejora:	• Implementar un centro de procesamiento de datos CPD auxiliar con el fin de brindar apoyo y soporte a los servidores principales en caso de que fallen por cualquier incidente presentado. • Dar continuidad al funcionamiento de los servicios y software instalados en los servidores principales.		
Justificación:	El centro de procesamiento de datos en la empresa se describe como el espacio físico donde se hospeda el equipo tecnológico y permite crear, procesar, almacenar y transferir la información de los servicios que ofrece la empresa; por ende, es de vital importancia generar las medidas de seguridad en el CPD e implementar métodos y técnicas alternativas que permitan salvaguardar la información y darle continuidad a todos los procesos que son indispensables para la empresa.		

Controles Identificados:	Activos afectados:
A.12.3 Copias de seguridad A.12.5.1 Instalación de software en sistemas operativos A.12.6.1 Gestión de las vulnerabilidades técnicas A.13.1.2 Seguridad de los servicios de red A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas A.16.1 Gestión de incidentes y mejoras en la seguridad de la información A.17.1 Continuidad de Seguridad de la información	CH1, CS2-CS7, R1-R4, EA1, EA2

Puntos de control o medidores:	• Instalación del CPD alterno (servidores, redes, infraestructura y software) • Configuraciones y registros del CPD alterno que sirva de respaldo de los servicios que brinda a la empresa y a los clientes. • Registros de las copias de seguridad realizadas a los servidores principales y actualizados en los servidores alternos del CPD. • Documentos donde se establecen los conductos y lineamientos para la gestión y control de redes y servicios de la empresa. • Reportes de eventos e incidentes detectados en los servidores y servicios para su posterior análisis y evaluación.
Responsable de ejecución del proyecto:	Jefe de Redes y Servidores.
Presupuesto:	La implementación de un CPD alterno que de soporte a los servidores y servicios dispone de un presupuesto de $USD 40.544
Plazos de consecución y fecha límite de cumplimiento:	La propuesta para la implementación del CPD alterno está planteada para un periodo de tiempo de 1 año (mediano plazo)

Nombre del Proyecto:	Organización y clasificación de la información	**Código:**	P006
Objetivos de mejora:	• Etiquetar, clasificar y organizar la información según su valor, requisitos legales y nivel de protección, criticidad y sensibilidad.		
Justificación:	Identificar y clasificar el tipo de información existente teniendo en cuenta los activos implícitos, valor económico, nivel de criticidad y sensibilidad es un punto importante dentro de la seguridad de uno de los activos valiosos de la empresa; dado que los		

	servicios y recursos ofrecidos y adquiridos son necesarios dentro los procesos efectuados para la continuidad de la misma. La aplicación de controles se hace necesaria para salvaguardar la información.

Controles Identificados:	**Activos afectados:**
A.8.2 Clasificación de la información A.15.1 Seguridad de la información en las relaciones con los proveedores	D1-D3

Puntos de control o medidores:	• Etiquetado de la información de forma física y utilizando herramientas digitales que registren metadatos. • Consolidado donde se registre la revisión periódica de la clasificación y actualización de la información y activos de la empresa. • Consolidado de las políticas de control de acceso para el esquema de clasificación de la información.
Responsable de ejecución del proyecto:	Director de Tecnología (CTO)
Presupuesto:	El presupuesto asignado para la propuesta será de $USD 1.500
Plazos de consecución y fecha límite de cumplimiento:	Teniendo en cuenta la necesidad de la organización y clasificación de la información de la empresa, esta propuesta está determinada para realizarse en un tiempo de 6 meses (corto plazo)

Nombre del Proyecto:	Mejoramiento en los sistemas de gestión de usuarios	**Código:**	P007
Objetivos de mejora:	• Reestructurar la aplicación de políticas de seguridad en los controles de acceso de los usuarios. • Gestionar de forma correcta los roles, permisos y responsabilidades asignados al personal de la empresa según sus funciones y niveles de acceso asignados.		
Justificación:	Se definen las políticas de seguridad de controles de acceso enfatizadas en los lineamientos y requisitos de la empresa para los diferentes sistemas de información y para los servicios de redes internos y externos. Se estipulara las restricciones, revocaciones y autorizaciones a los usuarios junto con los parámetros de autenticación secreta.		

Controles Identificados:	**Activos afectados:**
A.9.1 Requisitos del negocio para el control de acceso A.9.2 Gestión de acceso de usuarios A.9.3 Responsabilidades de los usuarios	CH1-CH4, D1, D3, CS1-CS9, S1

A.9.4 Control de acceso a sistemas y aplicaciones	
Puntos de control o medidores:	• Documentos estipulados de las políticas de controles de acceso de los usuarios. • Informes de usuarios dados de alta y baja. • Informes de usuarios activos en los diferentes sistemas de información. • Documentos de asignación de responsabilidades y roles de los usuarios junto con la gestión de los controles de acceso a sistemas y aplicaciones.
Responsable de ejecución del proyecto:	Jefe de Desarrollo de Software.
Presupuesto:	El presupuesto asignado para la propuesta es de $USD 2.500
Plazos de consecución y fecha límite de cumplimiento:	Para la realización de las políticas de controles de acceso y la gestión de usuarios se estipula un periodo de 1 mes (corto plazo)

4.2 Cuantificación temporal

Teniendo en cuenta la propuesta de los proyectos se puede establecer a continuación la planificación de cada proyecto en términos de tiempo y/o fechas para la ejecución de cada uno esquematizado en el siguiente diagrama de Gantt:

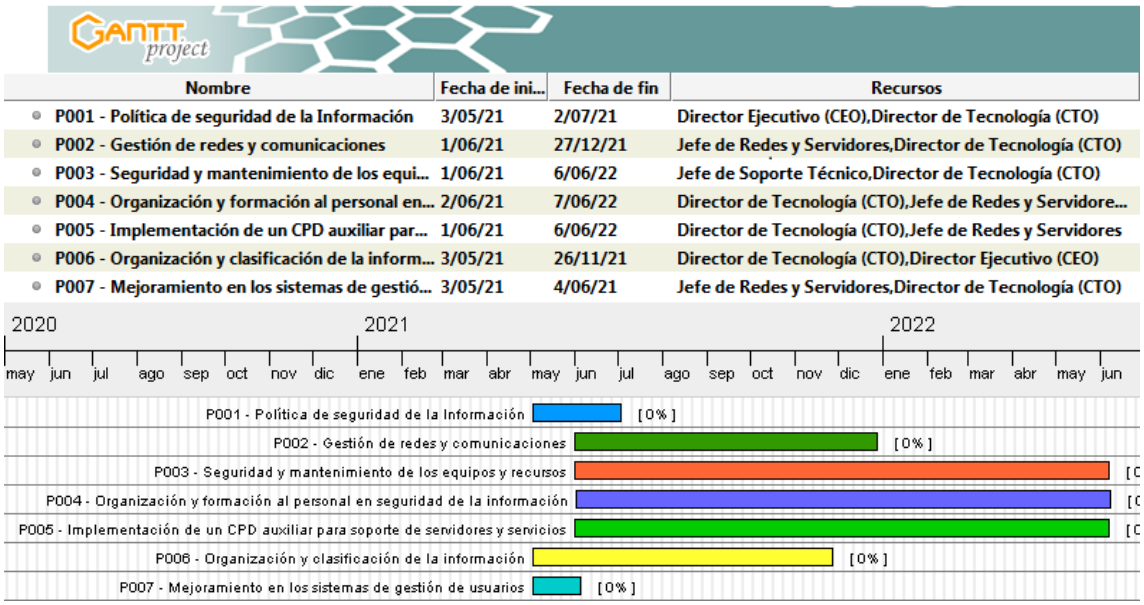

Ilustración 8 – Diagrama de Gantt de la planeación de los proyectos

4.3 Resultados de Propuestas

Considerando que se ha implementado las propuestas de proyectos del SGSI para el mejoramiento de los controles y la reducción o mitigación de riesgos, se realiza el análisis GAP de los controles (dominios y subdominios) de la ISO/IEC

27002 indicando la evolución en los controles identificados en cada proyecto. El siguiente diagrama de radar muestra la evolución que presenta el análisis GAP:

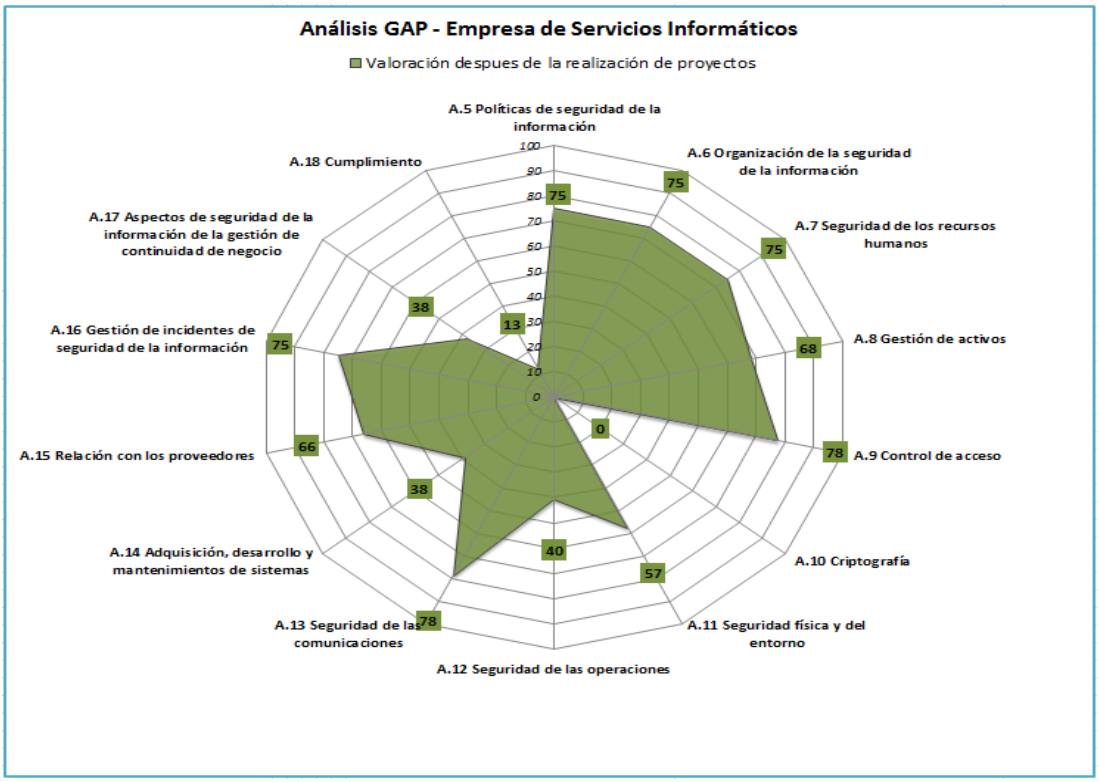

Ilustración 9 – Análisis GAP de la valoración después de la realización de proyectos

En el diagrama de radar se puede notar la evolución y/o crecimiento que han tenido los dominios una vez se implementan cada uno de los proyectos y se conserve un proceso de mejoramiento continuo. El avance se ha presentado en casi la mayoría de dominios o controles reflejando un crecimiento superior en un rango del 78 % aproximadamente con respecto al análisis inicial realizado en el ítem 1.5 del análisis diferencial de la empresa.

Hay que mencionar, además que ciertos dominios mantienen un porcentaje igual al presentado en el análisis inicial, lo que indica que no se han implementado proyectos que mitiguen o reduzca los riesgos y amenazas por motivos de establecer las prioridades detectadas en el análisis de amenazas e impactos de riesgos.

En el siguiente diagrama se puede observar la diferencia que existe al realizar la implementación de los proyectos con respecto al análisis diferencial realizado en la parte inicial del proyecto:

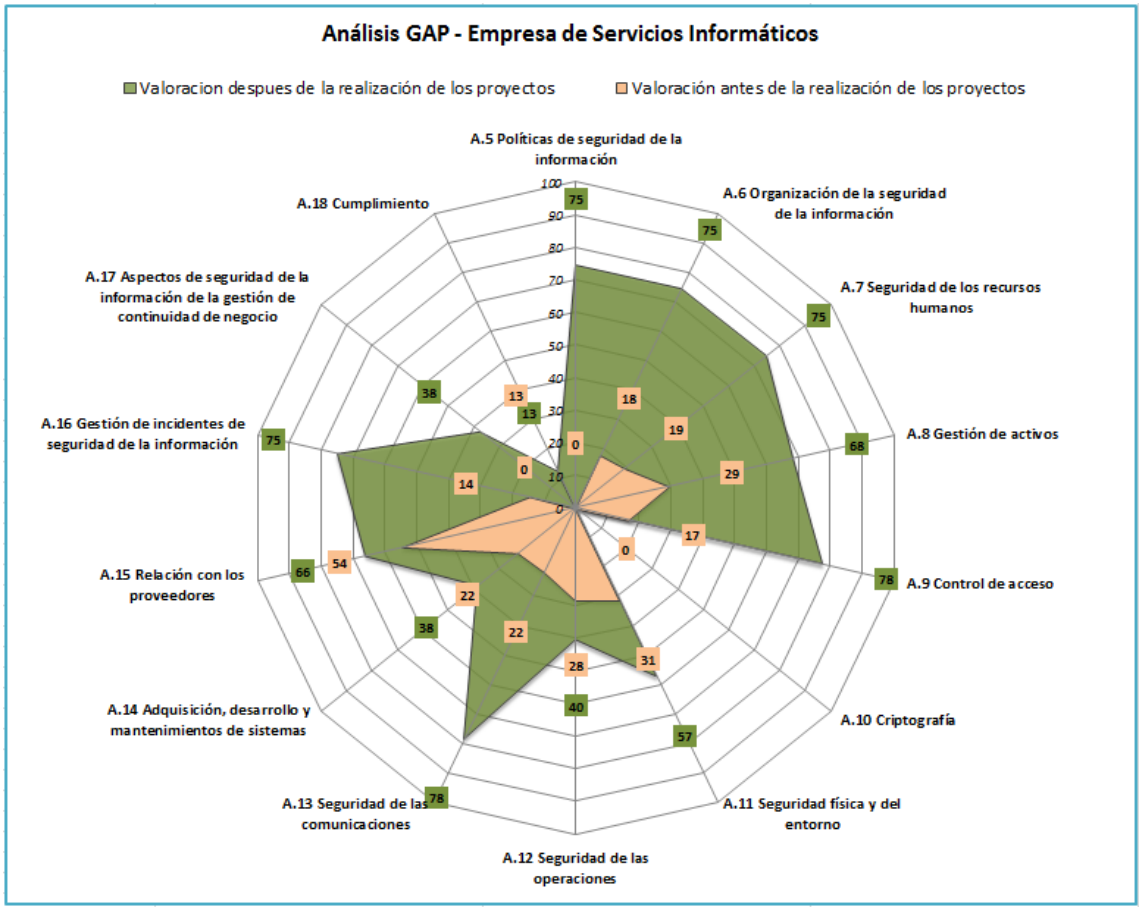

Ilustración 10 – Análisis GAP de la valoración después de la realización de los proyectos vs análisis GAP de la valoración antes de la realización de los proyectos

5. Auditoría de Cumplimiento

5.1 Metodología

Para este proceso antes de realizar la correspondiente metodología se debe tener en cuenta los requisitos para la elección del auditor interno quien será el encargado de verificar y ejecutar los procedimientos de auditoria junto con el equipo auditor seleccionado. Para ello, se debe revisar los requisitos planteados en el anexo 2.2 Procedimientos de Auditorías Internas sección 5.2.

Una vez realizado la selección del auditor interno en el proceso de auditoría de cumplimiento se utiliza el Modelo de Capacidad de Madurez descrito en el Capítulo 1 para revisar y evaluar los 114 controles del estándar ISO/IEC 27002:2013 organizado en 14 dominios y 35 objetivos de control.

Este proceso permitirá determinar y establecer en qué nivel de capacidad de madurez de la seguridad de la información se encuentra el SGSI en la empresa. A continuación, se establecen los controles y los objetivos de control según el dominio que los contiene organizados en un periodo de 3 años determinados en el anexo 2.2 Procedimientos de Auditorías Internas sección 5.1:

Primer año:
- A.5 Políticas de seguridad de la información.
- A.6 Organización de la seguridad de la información.
- A.7 Seguridad de los recursos humanos.
- A.8 Gestión de activos.
- A.9 Control de acceso.

Segundo año:
- A.10 Criptografía.
- A.11 Seguridad física y del entorno.
- A.12 Seguridad de las operaciones.
- A.13 Seguridad de las comunicaciones.
- A.14 Adquisición, desarrollo y mantenimiento de los sistemas.

Tercer año:
- A.15 Relación con los proveedores.
- A.16 Gestión de incidentes de seguridad de la información.
- A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- A.18 Cumplimiento.

El modelo de Capacidad de Madurez CMM se estipuló en la Tabla 3 – Modelo de Capacidad de Madurez (CMM) en el Capítulo 1 – Introducción del proyecto.

Para dar cumplimiento a los procesos de auditoria se establecen las siguientes etapas para su realización:

- Reunión preliminar del equipo auditor.

Etapa en la cual se convoca a reunión al equipo auditor para la asignación de tareas y áreas a auditar. En esta fase se reunió el equipo auditor conformado por el Director de Tecnología (CTO), el Jefe de Redes y Servidores, el Jefe de Desarrollo de Software y el Jefe de Soporte Técnico con el objetivo de determinar las áreas a auditar, por lo cual, se estableció auditar los 114 controles del estándar ISO/IEC 27002:2013 con respecto al Modelo de Capacidad de Madurez CMM de las áreas a auditar en un periodo de 3 años dividiendo los controles por cada año respectivamente.

- Reunión de apertura.

Etapa en la que se establecen los puntos del programa de auditoria a realizar. El programa incluye información como el objetivo de la auditoria, el alcance, el área auditada, el responsable, fecha de inicio y final de auditoria, procedimiento de comunicación, observaciones. Lo anterior, se presenta en la etapa de recolección de información y evidencia.

- Inicio de auditoria interna.

Etapa que se hace recolección de información y evidencia utilizando los debidos procedimientos. Esta información se puede incluir el siguiente formato:

Tabla 26 – Formato de recolección de información y evidencia de auditoria

Formato de recolección de Información y evidencia de auditoria	**Código**	
Objetivo		
Alcance		
Área auditada		
Responsable de área a auditar		
Fecha inicial de auditoria		
Fecha final de auditoria		
Procedimiento de comunicación		
Observaciones		

Además, en esta etapa se realizó la evaluación de la madurez definida en la sección 5.2 Evaluación de la Madurez en la tabla 27 – Análisis del proceso de auditoría de los controles de la ISO/IEC 27002 utilizando el CMM.

- Finalización de la auditoría interna y balance del auditor con el resultado.

Etapa en donde se establece la fecha para realizar el balance del auditor con el resultado obtenido de la tabla 27 - Análisis del proceso de auditoría de los controles de la ISO/IEC 27002 utilizando el CMM.

- Entrega por parte del auditor del informe de auditoría.

Entrega del informe por parte del auditor definido en la sección 5.3 Resultados, donde se presentan los resultados obtenidos de la evaluación de madurez utilizando gráficos (Ilustración 11 y 12) y describiendo los resultados en el informe.

5.2 Evaluación de la Madurez

Para la realización de la evaluación de la Madurez en el proceso de auditoría se emplea la tabla del Modelo de la Capacidad de Madurez mencionado anteriormente. Para ello, se presenta de forma resumida la tabla del CMM

Tabla 27 – Resumen modelo de capacidad de madurez CMM

Nivel	Estado	Valoración en porcentajes
L0	**Inexistente**	**0%**
L1	**Inicial**	**25%**
L2	**Repetible**	**50%**
L3	**Establecido**	**75%**
L4	**Administrado**	**95%**
L5	**Mejorado**	**100%**

A continuación se evalúa cada uno de los 114 controles del estándar ISO/IEC 27002 teniendo en cuenta el modelo de capacidad de madurez planteado en el inicio del proyecto para la realización del análisis diferencial. Posteriormente, se presentarán los resultados obtenidos al realizar la evaluación presentados en gráficas y haciendo una comparación del estado inicial del análisis con el estado posterior una vez realizada la siguiente evaluación. Cabe resaltar, que el valor acogido se hace mediante porcentajes y se asigna el nivel correspondiente según la tabla del CMM.

Tabla 28 – Análisis del proceso de auditoría de los controles de la ISO/IEC 27002 utilizando el CMM

PRIMER AÑO		
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.5 Políticas de seguridad de la información	**L3**	**75%**
5.1 Directrices de gestión de la seguridad de la información		*75%*
A.5.1.1 Políticas para la seguridad de la información		75%
A.5.1.2 Revisión de las políticas para la seguridad de la información		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.6 Organización de la seguridad de la información	**L3**	**75%**
A.6.1 Organización interna		75%
A.6.1.1 Roles y responsabilidades para la seguridad de la información		75%

A.6.1.2 Separación de deberes		75%
A.6.1.3 Contacto con las autoridades		75%
A.6.1.4 Contacto con grupos de interés especial		75%
A.6.1.5 Seguridad de la información en la gestión de proyectos.		75%
A.6.2 Dispositivos móviles y teletrabajo		*75%*
A.6.2.1 Política para dispositivos móviles		75%
A.6.2.2 Teletrabajo		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.7 Seguridad de los recursos humanos	**L3**	**75%**
A.7.1 Antes de asumir el empleo		*75%*
A.7.1.1 Selección		75%
A.7.1.2 Términos y condiciones del empleo		75%
A.7.2 Durante la ejecución del empleo		*75%*
A.7.2.1 Responsabilidades de la dirección		75%
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.		75%
A.7.2.3 Proceso disciplinario		75%
A.7.3 Terminación y cambio de empleo		*75%*
A.7.3.1 Terminación o cambio de responsabilidades de empleo		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.8 Gestión de activos	**L2**	**68,3%**
A.8.1 Responsabilidad por los activos		*85%*
A.8.1.1 Inventario de activos		95%
A.8.1.2 Propiedad de los activos		95%
A.8.1.3 Uso aceptable de los activos		75%
A.8.1.4 Devolución de activos		75%
A.8.2 Clasificación de la información		*95%*
A.8.2.1 Clasificación de la información		95%
A.8.2.2 Etiquetado de la información		95%
A.8.2.3 Manejo de activos		95%
A.8.3 Manejo de medios		*25%*
A.8.3.1 Gestión de medio removibles		25%
A.8.3.2 Disposición de los medios		25%
A.8.3.3 Transferencia de medios físicos		25%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.9 Control de acceso	**L3**	**77,5%**
A.9.1 Requisitos del negocio para el control de acceso		*85%*
A.9.1.1 Política de control de acceso		75%
A.9.1.2 Acceso a redes y a servicios en red		95%
A.9.2 Gestión de acceso de usuarios		*75%*
A.9.2.1 Registro y cancelación del registro de usuarios		75%
A.9.2.2 Suministro de acceso de usuarios		75%

A.9.2.3 Gestión de derechos de acceso privilegiado		75%
A.9.2.4 Gestión de información de autenticación secreta de usuarios		75%
A.9.2.5 Revisión de los derechos de acceso de usuarios		75%
A.9.2.6 Retiro o ajuste de los derechos de acceso		75%
A.9.3 Responsabilidades de los usuarios		*75%*
A.9.3.1 Uso de información de autenticación secreta		75%
A.9.4 Control de acceso a sistemas y aplicaciones		*75%*
A.9.4.1 Restricción de acceso a la información		75%
A.9.4.2 Procedimiento de ingreso seguro		75%
A.9.4.3 Sistema de gestión de contraseñas		75%
A.9.4.4 Uso de programas utilitarios privilegiados		75%
A.9.4.5 Control de acceso a códigos fuente de programas		75%
SEGUNDO AÑO		
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.10 Criptografía	**L0**	**0%**
A.10.1 Controles criptográficos		*0%*
A.10.1.1 Política sobre el uso de controles criptográficos		0%
A.10.1.2 Gestión de llaves		0%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.11 Seguridad física y del entorno	**L2**	**57,36%**
A.11.1 Áreas seguras		*37,5%*
A.11.1.1 Perímetro de seguridad física		50%
A.11.1.2 Controles de acceso físicos		25%
A.11.1.3 Seguridad de oficinas, recintos e instalaciones		25%
A.11.1.4 Protección contra amenazas externas y ambientales		25%
A.11.1.5 Trabajo en áreas seguras		50%
A.11.1.6 Áreas de carga, despacho y acceso público		50%
A.11.2 Equipos		*77,2%*
A.11.2.1 Ubicación y protección de los equipos		75%
A.11.2.2 Servicios de suministro		75%
A.11.2.3 Seguridad en el cableado		95%
A.11.2.4 Mantenimiento de los equipos		75%
A.11.2.5 Retiro de activos		75%
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones		75%
A.11.2.7 Disposición segura o reutilización de equipos		75%
A.11.2.8 Equipos de usuario desatendido		75%
A.11.2.9 Política de escritorio limpio y pantalla limpia		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.12 Seguridad de las operaciones	**L1**	**40,47%**
A.12.1 Procedimientos operacionales y responsabilidades		*33,3%*
A.12.1.1 Procedimientos de operación documentados		25%

A.12.1.2 Gestión de cambios		0%
A.12.1.3 Gestión de capacidad		25%
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación		50%
A.12.2 Protección contra códigos maliciosos		*50%*
A.12.2.1 Controles contra códigos maliciosos		50%
A.12.3 Copias de seguridad		*75%*
A.12.3.1 Respaldo de la información		75%
A.12.4 Registro y seguimiento		*12,5%*
A.12.4.1 Registro de eventos		25%
A.12.4.2 Protección de la información de registro		25%
A.12.4.3 Registros del administrador y del operador		0%
A.12.4.4 Sincronización de relojes		0%
A.12.5 Control de software operacional		*75%*
A.12.5.1 Instalación de software en sistemas operativos		75%
A.12.6 Gestión de la vulnerabilidad técnica		*50%*
A.12.6.1 Gestión de las vulnerabilidades técnicas		50%
A.12.6.2 Restricciones sobre la instalación de software		50%
A.12.7 Consideraciones sobre auditorias de sistemas de información		*0%*
A.12.7.1 Controles de auditorías de sistemas de información		0%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.13 Seguridad de las comunicaciones	**L3**	**78,3%**
A.13.1 Gestión de la seguridad de las redes		*81,6%*
A.13.1.1 Controles de redes		75%
A.13.1.2 Seguridad de los servicios de red		95%
A.13.1.3 Separación en las redes		75%
A.13.2 Transferencia de información		*75%*
A.13.2.1 Políticas y procedimientos de transferencia de información		75%
A.13.2.2 Acuerdos sobre transferencia de información		75%
A.13.2.3 Mensajería Electrónica		75%
A.13.2.4 Acuerdos de confidencialidad o de no divulgación		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.14 Adquisición, desarrollo y mantenimientos de sistemas	**L1**	**38,3%**
A.14.1 Requisitos de seguridad de los sistemas de información		*81,6%*
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información		75%
A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas		95%
A.14.1.3 Protección de transacciones de los servicios de las aplicaciones		75%
A.14.2 Seguridad en los procesos de Desarrollo y de Soporte		*33,3%*

A.14.2.1 Política de desarrollo seguro		25%
A.14.2.2 Procedimientos de control de cambios en sistemas		25%
A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		50%
A.14.2.4 Restricciones en los cambios a los paquetes de software		25%
A.14.2.5 Principio de Construcción de los Sistemas Seguros		25%
A.14.2.6 Ambiente de desarrollo seguro		25%
A.14.2.7 Desarrollo contratado externamente		50%
A.14.2.8 Pruebas de seguridad de sistemas		25%
A.14.2.9 Prueba de aceptación de sistemas		50%
A.14.3 Datos de prueba		0%
A.14.3.1 Protección de datos de prueba		0%
TERCER AÑO		
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.15 Relación con los proveedores	**L2**	**65,83%**
A.15.1 Seguridad de la información en las relaciones con los proveedores		*81,6%*
A.15.1.1 Política de seguridad de la información para las relaciones con proveedores		95%
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores		75%
A.15.1.3 Cadena de suministro de tecnología de información y comunicación		75%
A.15.2 Gestión de la prestación de servicios de proveedores		*50%*
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores		50%
A.15.2.2 Gestión del cambio en los servicios de los proveedores		50%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.16 Gestión de incidentes de seguridad de la información	**L3**	**75%**
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		*75%*
A.16.1.1 Responsabilidades y procedimientos		75%
A.16.1.2 Reporte de eventos de seguridad de la información		75%
A.16.1.3 Reporte de debilidades de seguridad de la información		75%
A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos		75%
A.16.1.5 Respuesta a incidentes de seguridad de la información		75%
A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información		75%
A.16.1.7 Recolección de evidencia		75%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.17 Aspectos de seguridad de la información	**L1**	**37,5%**

de la gestión de continuidad de negocio		
A.17.1 Continuidad de Seguridad de la información		*75%*
A.17.1.1 Planificación de la continuidad de la seguridad de la información		75%
A.17.1.2 Implementación de la continuidad de la seguridad de la información		75%
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información		75%
A.17.2 Redundancias		*0%*
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información		0%
Dominio y controles	**Nivel CMM**	**Valor CMM**
A.18 Cumplimiento	**L0**	**12,5%**
A.18.1 Cumplimiento de requisitos legales y contractuales		*25%*
A.18.1.1 Identificación de la legislación aplicable		25%
A.18.1.2 Derechos propiedad intelectual		25%
A.18.1.3 Protección de registros		50%
A.18.1.4 Privacidad y protección de información de datos personales		25%
A.18.1.5 Reglamentación de controles criptográficos.		0%
A.18.2 Revisiones de seguridad de la información		*0%*
A.18.2.1 Revisión independiente de la seguridad de la información		0%
A.18.2.2 Cumplimiento con las políticas y normas de seguridad		0%
A.18.2.3 Revisión del cumplimiento técnico		0%

5.3 Resultados

Para apreciar los resultados del proceso de auditoria referente al modelo de capacidad de madurez, se tendrá en cuenta el grafico del análisis inicial del CMM de la empresa con respecto al gráfico de análisis realizado posteriormente.

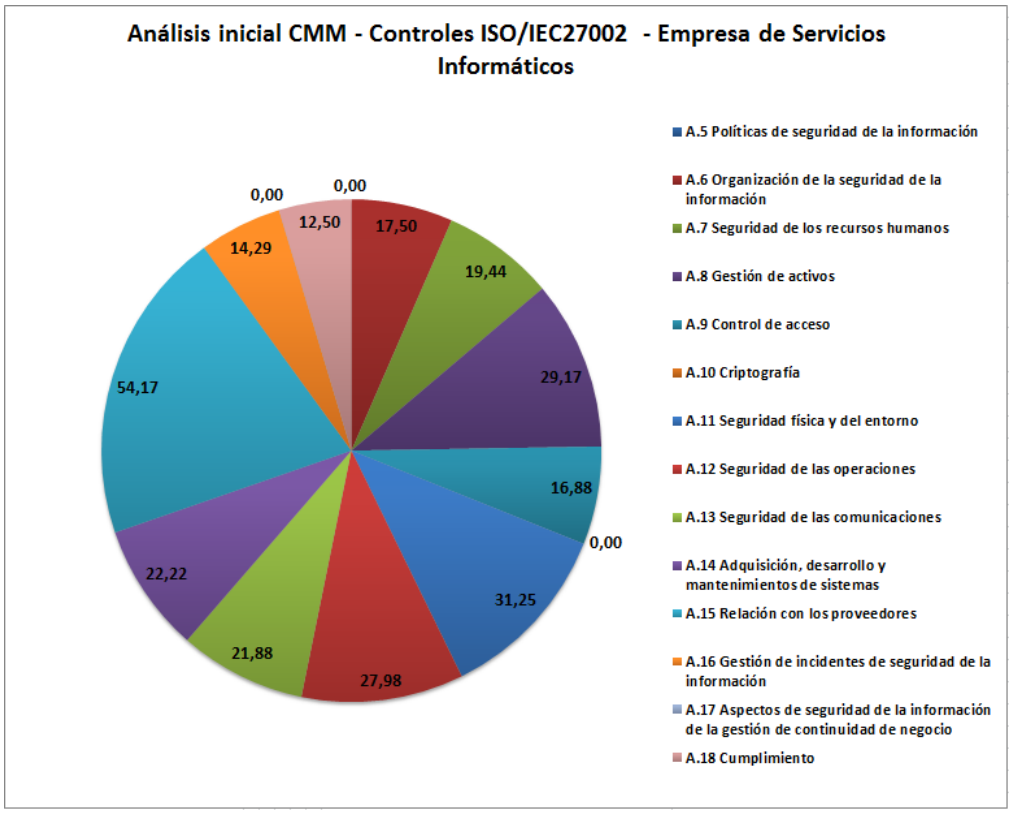

Ilustración 11 – Gráfica de análisis inicial de los controles de la ISO/IEC 27002 utilizando el CMM

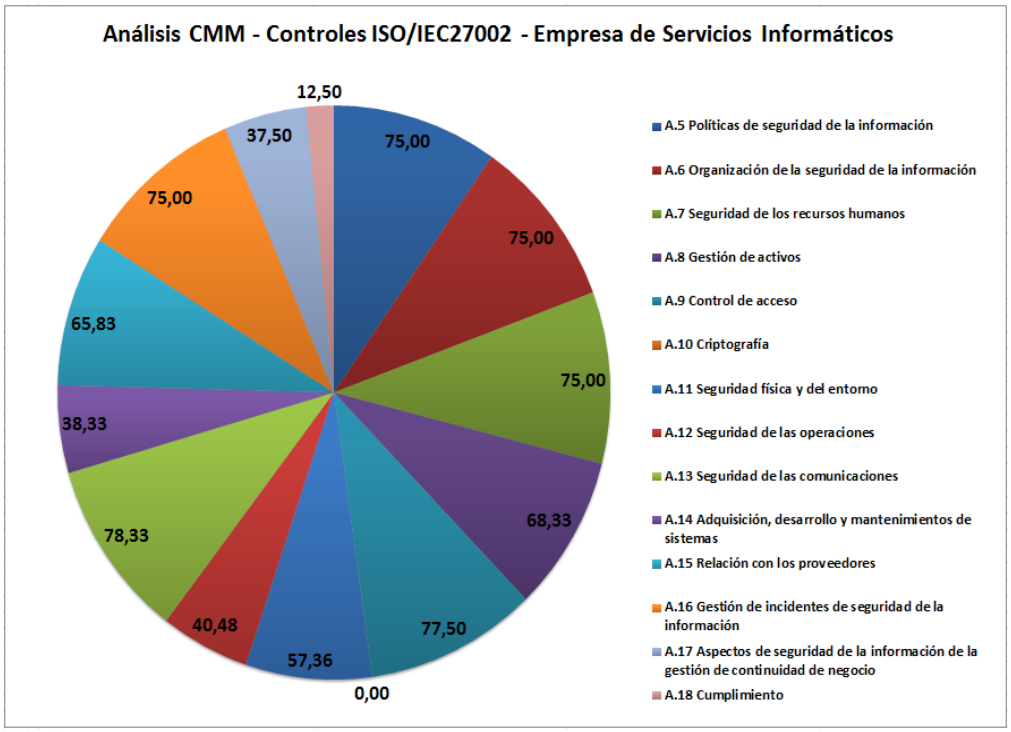

Ilustración 12 – Gráfica de análisis posterior de los controles de la ISO/IEC 27002 utilizando el CMM

Según los gráficos presentados, existe una variación significativa de la mayoría de los controles a su análisis inicial. Los controles A5 Políticas de seguridad de

la información, A6 Organización de la seguridad de la información, A7 Seguridad de los recursos humanos, A9 Control de acceso, A13 Seguridad de las comunicaciones, A16 Gestión de incidentes de seguridad de la información; tuvieron una mejora en 75% teniendo un nivel dentro del CMM del L3.

Igualmente, otros controles mejoraron entre un 25% y un 50%; como es el caso de los controles A8 Gestión de activos, A11 Seguridad física y del entorno, A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. Por último, los controles A10 Criptografía y A18 Cumplimiento, se mantuvieron y no presentaron mejorías.

Aunque los controles han tenido una mejora apreciable, es importante indicar que factores como la evolución de la tecnología y los procesos implementados en la empresa pueden determinar el surgimiento de nuevos inconvenientes que afectarían los resultados tratados, lo cual permitirá realizar nuevos análisis sobre los controles afectados.

Informe de auditoría

Teniendo en cuenta el anexo 10.2 -2.2 Procedimientos de Auditorías Internas, se presenta a continuación el informe de auditoría según lo establecido en la sección 5.3 Procedimiento de la auditoría interna:

a) Fecha de elaboración del informe: 22 de mayo del 2021

b) Área auditada: todas las áreas.

c) Responsable del área auditada: Mario Calderón

d) Cargo del responsable del área auditada: Director de Tecnología (CTO).

e) Email del responsable del área auditada: mario.calderon@expertec.com

f) Objetivo de la auditoría:
Revisar y evaluar los 114 controles del estándar ISO/IEC 27002 teniendo en cuenta el modelo de capacidad de madurez CMM.

g) Alcance de la auditoría:
Todos los procedimientos, documentos y controles que hacen parte del Plan Director del Sistema de Gestión de la Seguridad de la Información de la empresa.

h) Fechas de la auditoria:
Primera fecha: 20 de abril de 2021
Segunda fecha: 20 de Agosto de 2021
Tercera fecha: 20 de Diciembre de 2021.

i) Total, días de duración de la auditoría: 298 días.

j) Integrantes del equipo auditor: Jhony Restrepo, Evelin Castillo, Jesús Martinez.

k) Email de los integrantes del equipo auditor: jhony.restrepo@expertec.com, evelin.castillo@expertec.com, jesus.martinez@expertec.com

l) Actividades realizadas en la auditoria:
   - Criterios para el muestreo: controles implementados, controles faltantes, procedimientos establecidos en la seguridad de la información.
   - Actividades principales: análisis de documentación, verificación de activos, recursos, equipos y dispositivos de la empresa, verificación de procedimientos.
   - Observación de la evaluación: se realiza una observación directa en todos los procesos que incluyen la gestión de controles de seguridad.
   - Observaciones de la evaluación de requisitos de la especificación técnica, proceso o servicio: mediante la utilización de formatos establecidos por el equipo auditor se realizan diferentes observaciones para la evaluación de requisitos.

m) Observaciones:
   - En el proceso de auditoria se pudo observar que los controles A8 Gestión de activos, A11 Seguridad física y del entorno, A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio tuvieron un leve mejoramiento al realizar el análisis.
   - Se puede resaltar que el personal ha tenido una capacitación en relación a los procedimientos y lineamientos sobre la seguridad en los diversos aspectos funcionales de la empresa.
   - La permanente verificación de los controles en los activos y recursos ha posibilitado el avance en los procedimientos y la continuidad del negocio en la empresa.

n) Recomendaciones:
   - Implementar políticas para la utilización de controles criptográficos necesarios en los sistemas y servicios, así mismo, la gestión de contraseñas seguras, en donde, no se obtuvo mejorías en el análisis realizado de los controles de la ISO/IEC 27002 utilizando el CMM.
   - Realizar periódicamente las auditorías internas con el objetivo de evaluar las mejoras en la gestión de los controles de seguridad.
   - Realizar y ejecutar pruebas de simulación de ataques con el objetivo de evaluar la capacidad de respuesta ante incidentes de la empresa y el rendimiento de los controles implementados.
   - Realizar una constante evaluación a los controles que aún están en un nivel L1 y L2 dentro del análisis realizado para su continuo mejoramiento.

o) Nombre del auditor asignado al área auditada, cargo del auditor:
   Mario Calderón. Director de Tecnología (CTO).

6. Presentación de Resultados y Entrega de Informes

La presentación de resultados y entrega de informes se ha realizado de manera continua en cada una de las etapas del Plan Director del Sistema de Gestión de la Seguridad de la Información presentadas en el proyecto y en donde se establecen los análisis y resultados obtenidos.

Además de los resultados e informes se tienen en cuenta los documentos que complementan este Trabajo Final de Master, los cuales, se listan a continuación:

- Presentación de los resultados de análisis de riesgos y las propuestas de proyectos.
- Presentación del proyecto del Trabajo Final de Master con los resultados y las conclusiones obtenidas.
- Video del proyecto del Trabajo Final de Master con los resultados y las conclusiones obtenidas.

7. Conclusiones

El presente trabajo ha permitido a la empresa de servicios y soluciones informáticas EXPERTEC estructurar de manera organizada un Plan director del Sistema de Gestión de la Seguridad de la Información necesario para cumplir los objetivos planteados en el documento y tomar acciones y decisiones para la implementación del Plan con el propósito de brindar un servicio de alta calidad y la continuidad del negocio.

Para lograr cumplir con los objetivos planteados del Plan Director se han determinado las siguientes etapas dentro de la empresa resaltando de forma concluyente los resultados y las acciones realizadas en cada una de ellas:

- Se realizó en primera instancia un análisis DAFO complementado con una estrategia CAME con el propósito de contextualizar y entender la situación actual de la empresa en cuanto al ámbito de seguridad de la información se refiere.
- Posteriormente se realizó un análisis diferencial de la empresa teniendo en cuenta los estándares de la ISO/IEC 27001 y los controles de la norma ISO/IEC 27002 con el objetivo de evaluar las cláusulas de la ISO 27001 y los controles de la ISO 27002 utilizando como referencia y valoraciones el modelo de capacidad de madurez el cual arrojo los resultados de medición de cumplimiento de los estándares en la empresa.
- Además se establecieron los documentos obligatorios para el cumplimiento normativo de la implementación del SGSI, los cuales, se generaron unos formatos para la estructuración y organización de los documentos que permitieron alinear los parámetros y estrategias para la gestión de la seguridad de la información.
- Se aplicó la metodología de Análisis y Riesgos de los Sistemas de Información MAGERIT para direccionar a la empresa en la gestión de riesgos realizando las siguientes actividades: inventario de activos de la empresa, valoración de los activos, valoración de las dimensiones de la seguridad de la información, análisis de amenazas presentes en los activos de la empresa, impacto potencial a materializarse una amenaza en los activos y valoración del nivel de riesgo potencial y residual según la frecuencia de ocurrencia y el impacto potencial. Las anteriores actividades permitieron identificar y analizar los activos que se encuentran en riesgo según los niveles establecidos y que afectan las dimensiones de la seguridad.
- Paso siguiente fue la propuesta de diferentes proyectos que permitieron realizar mejoras en los controles y reducir o mitigar los riesgos identificados en la etapa de análisis y riesgos. En la presentación de los proyectos se utilizó un esquema que abarco los puntos descriptivos de los proyectos con sus características relevantes para su planeación e implementación. De igual manera, se realizó un análisis y comparación GAP en donde se identificó la evolución referente al estado inicial de los controles del estándar ISO/IEC 27002 con respecto a la aplicación de las propuestas de los proyectos.

- Por último, se implementó un proceso de auditoría para estipular el nivel de capacidad de madurez en la que se encuentra el SGSI de la empresa. En este proceso se utilizó el CMM realizado en la primera etapa para realizar un diagnóstico acerca del avance que se obtuvo del análisis realizado inicialmente con respecto al análisis posterior.

Hay que mencionar, también que mediante la implementación del plan director del SGSI se ha logrado establecer niveles de protección de los activos y recursos que se identificaron esenciales y prioritarios en la empresa; tales como la infraestructura de redes, servidores, equipos de cómputo, los elementos de soporte técnico, software utilizado, sistemas de información y servicios implementados.

Por otra parte, se ha logrado mitigar amenazas y vulnerabilidades que afectan los activos, recursos y procesos mediante la implementación del Plan Director del SGSI y los lineamientos, estrategias, documentos y normativas que se han establecido en los análisis y resultados de las etapas mencionadas anteriormente.

En definitiva, la implementación del Plan Director del SGSI ha logrado cumplir con los objetivos planteados para la gestión de riesgos en la empresa EXPERTEC consiguiendo aplicar los controles necesarios para la mitigación y reducción de los riesgos referentes a la seguridad de la información. No obstante, es importante aclarar que se deben mejorar tanto los controles priorizados como los controles que aún no se han logrado superar para obtener de esta forma que la empresa cumpla con los estándares necesarios y darle una calidad en la continuidad del negocio.

8. Glosario

Amenaza: Cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo.
Análisis: Examen detallado de una cosa para conocer sus características o cualidades, o su estado, y extraer conclusiones, que se realiza separando o considerando por separado las partes que la constituyen.
Auditoría: Inspección o verificación de la contabilidad de una empresa o una entidad, realizada por un auditor con el fin de comprobar si sus cuentas reflejan el patrimonio, la situación financiera y los resultados obtenidos por dicha empresa o entidad en un determinado ejercicio.
Cableado: Que está unido o conectado mediante cables.
Capacitación: Acción de capacitar.
Confidencialidad: Cualidad de lo que es confidencial.
Confidencial: Que se hace o se dice en confidencia.
Control: Poder o dominio que una persona o cosa ejerce sobre alguien o algo.
Debilidad: Cualidad de débil.
Directriz: Norma o conjunto de normas e instrucciones que se establecen o se tienen en cuenta al proyectar una acción o un plan.
Disponibilidad: Situación de estar disponible alguien o algo.
Dominio: Parte de una dirección de Internet que identifica un sitio web y que describe el tipo de empresa u organización a la que pertenece o bien el país donde está registrado.
Estrategia: Serie de acciones muy meditadas, encaminadas hacia un fin determinado.
Evaluación: Valoración de conocimientos, actitud y rendimiento de una persona o de un servicio.
Fortaleza: Capacidad de una cosa para sostener, soportar o resistir algo.
Gestión: Acción o trámite que, junto con otros, se lleva a cabo para conseguir o resolver una cosa.
Impacto: Conjunto de los efectos que un suceso o un hecho producen en su entorno físico o social.
Implantación: Acción de implantar.
Implantar: Establecer o instaurar una cosa, especialmente una costumbre, una reforma o una moda.
Incidente: Cosa que se produce en el transcurso de un asunto, un relato, etc., y que repercute en él alterándolo o interrumpiéndolo.
Infraestructura tecnológica: Conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de una actividad o para que un lugar pueda ser utilizado.
Integridad: Calidad de íntegro.
Integro: Que está completo o tiene todas sus partes.
Marketing: Conjunto de técnicas y estudios que tienen como objeto mejorar la comercialización de un producto.
Mejora: Cambio o progreso de una cosa que está en condición precaria hacia un estado mejor.
Mejoramiento: Cambio o progreso de una cosa que está en condición precaria hacia un estado mejor.

Mitigar: Atenuar o suavizar una cosa negativa, especialmente una enfermedad.
Modelo: Cosa que sirve como pauta para ser imitada, reproducida o copiada.
Monitoreo: Controlar el desarrollo de una acción o un suceso a través de uno o varios monitores.
Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad. Regla jurídica.
Oportunidad: Circunstancia, momento o medio oportunos para realizar o conseguir algo.
Organización: Grupo de personas y medios organizados con un fin determinado.
Planeación: Planificación.
Planificación: Elaborar o establecer el plan conforme al que se ha de desarrollar algo, especialmente una actividad.
Política: Orientación o manera de actuar de una persona en un asunto determinado.
Procedimiento: Método o modo de tramitar o ejecutar una cosa.
Proceso: Conjunto de fases sucesivas de un fenómeno o hecho complejo.
Protección: Acción de proteger o impedir que una persona o una cosa reciba daño o que llegue hasta ella algo que lo produzca.
Proveedor: Que se dedica a proveer o abastecer de productos necesarios a una persona o empresa.
Recursos: Conjunto de elementos disponibles para resolver una necesidad o para llevar a cabo una empresa.
Revisión: Prueba o examen a que se somete determinada cosa o persona para hacer las correcciones necesarias.
Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.
Seguridad: Ausencia de peligro o riesgo.
Servicios: Utilidad o función que desempeña una cosa.
Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
Soluciones: Respuesta eficaz a un problema, duda o cuestión.
Usuario: Que usa habitualmente un servicio.
Vulnerabilidad: Cualidad de lo que es vulnerable.
Vulnerable: Que puede ser vulnerado o dañado física o moralmente

9. Bibliografía

[1] Serie “27000” documentación publicada por ISO y relacionada con las normas 27000(27001, 27002, etc), https://www.iso27000.es/iso27000.html, 14/03/2021

[2] Norma ISO 27001, https://normaiso27001.es/, 14/03/2021

[3] El análisis DAFO y los objetivos estratégicos, https://www.eumed.net/ce/2011a/domh.zip , 15/03/2021

Amenazas informáticas y seguridad de la información, https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/, 18/03/2021

[4] MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro III - Guía de Técnicas, https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

[5] MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

10. Anexos

10.1 Anexo – Política de Seguridad

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**POLITICA DE SEGURIDAD**	Código: DGSI-01 Versión:1 Fecha de aprobación: Marzo 2021 Páginas:

ESQUEMA
1. Introducción En harás de mejorar la estrategia de Seguridad de la Información de la empresa EXPERTEC surge la necesidad de establecer una Política de Seguridad de la Información que permita buscar medidas adecuadas de protección de la información, precisando sus lineamientos, para garantizar el correcto control y reducir los riesgos asociados.
2. Objetivo Establecer la normatividad que permita preservar la información y los sistemas de la empresa, garantizando la integridad, confidencialidad y disponibilidad de la información y de los activos.
3. Alcance La política de seguridad está dirigida y aplicada a todas las áreas de la empresa, personal, proveedores y toda persona externa que tenga relación con los activos de la empresa.
4. Marco normativo y regulatorio Norma ISO/IEC 27001
5. Descripción Se han definido las siguiente políticas generales para dar cumplimiento por parte de todo el personal de la empresa: **5.1 Cumplimiento y sanciones** Todo el personal, contratista, colaborador y personal externo deben cumplir y acatar las políticas y procedimientos en cuestión de protección y seguridad de la información. Es deber del comité de seguridad y de la alta dirección velar por el cumplimiento correcto de las políticas. El incumplimiento de una política de seguridad por parte del personal, contratista, colaborador y personal externo es causal para iniciar acciones disciplinarias y dependiendo de su gravedad puede tener efectos de desvinculación o terminación laboral. **5.2 Uso de recursos informáticos** El uso de recursos informáticos debe estar soportado de instrucciones técnicas impartidas por la empresa. El propósito de los recursos informáticos deben ser estrictamente laborales, cualquier otro uso debe estar sujeto a previa autorización de las directivas.

5.3 Identificación y Autorización
Se establecen usuarios y contraseñas para los diferentes equipos de las diferentes áreas de la empresa dependiendo del tipo de usuario, permiso y grupos asignados por el comité de seguridad. Las contraseñas deben ser personales, confidenciales e intransferibles.

Las contraseñas deben ser cambiadas periódicamente con un tiempo estimado de 45 días. Las contraseñas deben tener un formato especifico (Longitud mínima, fortaleza en su cifrado, no ser reutilizadas, almacenadas en un formato especifico y en un lugar específico.)

5.4 Uso del servicio de Internet
La utilización del servicio de Internet es exclusiva para realizar actividades laborales y no personales. El medio a utilizar para las comunicaciones laborales o formales será el correo electrónico y la cuenta de correo de cada funcionario es de carácter personal. Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales y que vulnere los derechos fundamentales de las personas.

Es importante que el funcionario rechace y se abstenga de abrir el correo SPAM y debe informar al área de sistemas. El intercambio de información en Internet debe ser aprobado y utilizando los mecanismos de protección apropiados.

5.5 Gestión de copias y recuperación de información
Se debe realizar una copia de seguridad de forma periódica y completa a toda la información sensible y critica de la empresa y de las empresas a las cuales se brinda el servicio. El tipo de copia de seguridad puede ser total, diferencial o incremental, dependiendo de la planeación realizada por el encargado o responsable. Se requiere realizar pruebas periódicas de las copias para garantizar el buen estado de la información almacenada.

5.6 Políticas para desarrolladores de Software
Las aplicaciones y software deben contar con ambientes de desarrollo, pruebas y producción. Los cambios o actualizaciones que se realicen en el ambiente de producción deben ser probados antes de su lanzamiento en las diferentes versiones; de igual manera deben tener la documentación respectiva. Como punto principal, deben implementarse y probarse medidas de seguridad antes del lanzamiento del software o aplicación.

5.7 Gestión de vulnerabilidades e incidentes de seguridad
Toda infraestructura de red que tenga acceso a Internet debe tener un sistema de detección de intrusos IDS con el propósito de tomar acciones frente a diferentes ataques. Las conexiones externas y hacia Internet deben pasar en primera instancia por un Firewall con el fin de controlar y limitar la entrada y salida de información en la empresa.

Se debe implementar un software de antivirus licenciado y actualizado en los equipos de cómputo de la empresa. Además, se debe implementar a todos los

sistemas conectados a Internet un software de detección de vulnerabilidades y ejecutarlo periódicamente cada 2 meses.

5.8 Políticas de acceso físico
El acceso a las diferentes zonas o áreas de la empresa debe ser con carnet de identificación requerida. En caso de pérdida del carnet de identificación el funcionario debe reportar la pérdida. Todos los activos involucrados en la seguridad de la información que se requieran ser retirados de la empresa deben tener autorización escrita para su salida.

5.9 Políticas para personal externo
Los proveedores, clientes y asociados con la empresa deben tener conocimiento de las responsabilidades y obligaciones relacionadas con la seguridad informática de la empresa y debe estar reflejada en los contratos. De igual manera, los acuerdos relacionados con el tratamiento de la información por parte de terceros deben incluir cláusulas específicas que se involucren la confidencialidad y privacidad de la información.

6. Medios de divulgación:
El medio por el cual se divulgara la política de seguridad ser a través del correo electrónico empresarial del personal de la empresa.

	Nombres y Apellidos	**Cargo**	**Fecha**	**Firma**
Elaborado				
Revisado				
Aprobado				

10.2 Anexo - 2.2 Procedimientos de Auditorías Internas

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**AUDITORIAS INTERNAS**	Código: DGSI-02 Versión:1 Fecha de aprobación: Marzo 2021 Páginas:

ESQUEMA

1. Introducción
Se establecen las auditorías internas con el fin de hacer seguimiento y evaluar el correcto desempeño de los controles de seguridad.
Este procedimiento realizado por personal idóneo, permitirá generar mejoras en los procesos en caso de ser necesario.

2. Objetivo
Verificar que el sistema de seguridad de la empresa es eficaz, la conformidad del proceso según criterios de evaluación, la mantenibilidad y la capacidad de la empresa para asegurar el cumplimiento de los requisitos legales del sistema para la mejora continua.

3. Alcance

Se realizarán auditorías internas a todas las áreas de la empresa.
4. Marco normativo y regulatorio Norma ISO/IEC 27001
5. Descripción Se realizan auditorías internas con el fin de realizar un proceso adecuado de seguimiento, evaluación, medición y análisis.

5.1 Cronograma de la auditoría:

Para la realización de las auditorías internas se desarrolla un programa de auditorías cada 3 años, en donde, se tiene organizado los controles y los objetivos de control según el dominio que los contiene de la siguiente manera:

- El primer año se realizara auditorias de los 5 primeros dominios comprendidos entre el dominio A.5 Políticas de seguridad de la información y el dominio A.9 Control de acceso.
- El segundo año se realizara auditorias de los dominios comprendidos entre el dominio A.10 Criptografía y el dominio A.14 Adquisición, desarrollo y mantenimientos de sistemas.
- El tercer año se realizara auditorias de los dominios comprendidos entre el dominio A.15 Relación con los proveedores y el dominio A.18 Cumplimiento.

En la siguiente tabla se especifican los controles que se van a auditar según el cronograma planteado anteriormente:

Revisión control	Primer año	Segundo año	Tercer año
A.5 Políticas de seguridad de la información			
A.5.1.1 Políticas para la seguridad de la información	X		
A.5.1.2 Revisión de las políticas para la seguridad de la información	X		
A.6 Organización de la seguridad de la información			
A.6.1.1 Roles y responsabilidades para la seguridad de la información	X		
A.6.1.2 Separación de deberes	X		
A.6.1.3 Contacto con las autoridades	X		
A.6.1.4 Contacto con grupos de interés especial	X		
A.6.1.5 Seguridad de la información en la gestión de proyectos.	X		
A.6.2.1 Política para dispositivos móviles	X		

A.6.2.2 Teletrabajo	X		
A.7 Seguridad de los recursos humanos			
A.7.1.1 Selección	X		
A.7.1.2 Términos y condiciones del empleo	X		
A.7.2.1 Responsabilidades de la dirección	X		
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	X		
A.7.2.3 Proceso disciplinario	X		
A.7.3.1 Terminación o cambio de responsabilidades de empleo	X		
A.8 Gestión de activos			
A.8.1.1 Inventario de activos	X		
A.8.1.2 Propiedad de los activos	X		
A.8.1.3 Uso aceptable de los activos	X		
A.8.1.4 Devolución de activos	X		
A.8.2.1 Clasificación de la información	X		
A.8.2.2 Etiquetado de la información	X		
A.8.2.3 Manejo de activos	X		
A.8.3.1 Gestión de medio removibles			
A.8.3.2 Disposición de los medios	X		
A.8.3.3 Transferencia de medios físicos	X		
A.9 Control de acceso			
A.9.1.1 Política de control de acceso	X		
A.9.1.2 Acceso a redes y a servicios en red	X		
A.9.2.1 Registro y cancelación del registro de usuarios	X		
A.9.2.2 Suministro de acceso de usuarios	X		
A.9.2.3 Gestión de derechos de acceso privilegiado	X		
A.9.2.4 Gestión de información de autenticación secreta de usuarios	X		
A.9.2.5 Revisión de los derechos de acceso de usuarios	X		
A.9.2.6 Retiro o ajuste de los derechos de acceso	X		
A.9.3.1 Uso de información de	X		

autenticación secreta			
A.9.4.1 Restricción de acceso a la información	X		
A.9.4.2 Procedimiento de ingreso seguro	X		
A.9.4.3 Sistema de gestión de contraseñas	X		
A.9.4.4 Uso de programas utilitarios privilegiados	X		
A.9.4.5 Control de acceso a códigos fuente de programas	X		
A.10 Criptografía			
A.10.1.1 Política sobre el uso de controles criptográficos		X	
A.10.1.2 Gestión de llaves		X	
A.11 Seguridad física y del entorno			
A.11.1.1 Perímetro de seguridad física		X	
A.11.1.2 Controles de acceso físicos		X	
A.11.1.3 Seguridad de oficinas, recintos e instalaciones		X	
A.11.1.4 Protección contra amenazas externas y ambientales		X	
A.11.1.5 Trabajo en áreas seguras		X	
A.11.1.6 Áreas de carga, despacho y acceso público		X	
A.11.2.1 Ubicación y protección de los equipos		X	
A.11.2.2 Servicios de suministro		X	
A.11.2.3 Seguridad en el cableado		X	
A.11.2.4 Mantenimiento de los equipos		X	
A.11.2.5 Retiro de activos		X	
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones		X	
A.11.2.7 Disposición segura o reutilización de equipos		X	
A.11.2.8 Equipos de usuario desatendido		X	
A.11.2.9 Política de escritorio limpio y pantalla limpia		X	
A.12 Seguridad de las operaciones			
A.12.1.1 Procedimientos de operación documentados		X	
A.12.1.2 Gestión de cambios		X	

A.12.1.3 Gestión de capacidad		X	
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación		X	
A.12.2.1 Controles contra códigos maliciosos		X	
A.12.3.1 Respaldo de la información		X	
A.12.4.1 Registro de eventos		X	
A.12.4.2 Protección de la información de registro		X	
A.12.4.3 Registros del administrador y del operador		X	
A.12.4.4 Sincronización de relojes		X	
A.12.5.1 Instalación de software en sistemas operativos		X	
A.12.6.1 Gestión de las vulnerabilidades técnicas		X	
A.12.6.2 Restricciones sobre la instalación de software		X	
A.12.7.1 Controles de auditorías de sistemas de información		X	
A.13 Seguridad de las comunicaciones			
A.13.1.1 Controles de redes		X	
A.13.1.2 Seguridad de los servicios de red		X	
A.13.1.3 Separación en las redes		X	
A.13.2.1 Políticas y procedimientos de transferencia de información		X	
A.13.2.2 Acuerdos sobre transferencia de información		X	
A.13.2.3 Mensajería Electrónica		X	
A.13.2.4 Acuerdos de confidencialidad o de no divulgación		X	
A.14 Adquisición, desarrollo y mantenimientos de sistemas			
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información		X	
A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas		X	
A.14.1.3 Protección de transacciones de los servicios de las aplicaciones		X	
A.14.2.1 Política de desarrollo		X	

seguro			
A.14.2.2 Procedimientos de control de cambios en sistemas		X	
A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		X	
A.14.2.4 Restricciones en los cambios a los paquetes de software		X	
A.14.2.5 Principio de Construcción de los Sistemas Seguros		X	
A.14.2.6 Ambiente de desarrollo seguro		X	
A.14.2.7 Desarrollo contratado externamente		X	
A.14.2.8 Pruebas de seguridad de sistemas		X	
A.14.2.9 Prueba de aceptación de sistemas		X	
A.14.3.1 Protección de datos de prueba		X	
A.15 Relación con los proveedores			
A.15.1.1 Política de seguridad de la información para las relaciones con proveedores			X
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores			X
A.15.1.3 Cadena de suministro de tecnología de información y comunicación			X
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores			X
A.15.2.2 Gestión del cambio en los servicios de los proveedores			X
A.16 Gestión de incidentes de seguridad de la información			
A.16.1.1 Responsabilidades y procedimientos			X
A.16.1.2 Reporte de eventos de seguridad de la información			X
A.16.1.3 Reporte de debilidades de seguridad de la información			X
A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos			X
A.16.1.5 Respuesta a incidentes			X

de seguridad de la información			
A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información			X
A.16.1.7 Recolección de evidencia			X
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			
A.17.1.1 Planificación de la continuidad de la seguridad de la información			X
A.17.1.2 Implementación de la continuidad de la seguridad de la información			X
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información			X
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información			X
A.18 Cumplimiento			
A.18.1.1 Identificación de la legislación aplicable			X
A.18.1.2 Derechos propiedad intelectual			X
A.18.1.3 Protección de registros			X
A.18.1.4 Privacidad y protección de información de datos personales			X
A.18.1.5 Reglamentación de controles criptográficos.			X
A.18.2.1 Revisión independiente de la seguridad de la información			X
A.18.2.2 Cumplimiento con las políticas y normas de seguridad			X
A.18.2.3 Revisión del cumplimiento técnico			X

5.2 Requisitos para elección de auditor interno:

1. Estar certificado como auditor por entidad competente.
2. No pertenecer al equipo del área auditada.
3. Conocimientos específicos en las actividades de las áreas auditadas.
4. Conocimientos de documentos de referencia para el proceso.
5. Acreditar experiencia profesional en el ámbito de las tecnologías de la información.
6. Acreditar experiencia profesional en el ámbito de seguridad en las tecnologías de la información.
7. Capacidad de trabajo en equipo.

8. Ser observador, tenaz, constante, persistente y orientado a la consecución de los objetivos.
9. Tener poder de decisión.

5.3 El procedimiento de la auditoría interna será el siguiente:

1. Reunión preliminar del equipo auditor.
    a. Carta de citación al equipo auditor.
    b. Asignación de áreas por auditor.

2. Reunión de apertura.
    a. Carta de citación al equipo auditor y líderes de áreas.
    b. Documento de acuerdo de confidencialidad.
    c. Socialización del programa de auditoría: el programa tendrá la siguiente información:
        i. Objetivo
        ii. Alcance
        iii. Área auditada
        iv. Responsable de área a auditar
        v. Calendario de auditoría
        vi. Fecha inicial de auditoría
        vii. Fecha final de auditoría
        viii. Procedimiento de comunicación entre auditor y auditado
        ix. Observaciones
    d. Asignación del auditor por área.

3. Inicio de auditoría interna.
    a. Recolección de información y evidencia según lista de chequeo establecida para el proceso de auditoría. La recolección de la información se hará por medio de los siguientes procedimientos:
        i. Entrevistas
        ii. Recolección de evidencias
        iii. Verificación de documentación en sitio
        iv. Verificación de información digital en línea
        v. Análisis de la información recolectada

4. Finalización de la auditoría interna y balance del auditor con el resultado.

5. Entrega por parte del auditor del informe de auditoría, lista de chequeo, listado de asistencia. El informe de auditoría tendrá la siguiente información:
    a. Fecha de elaboración del informe
    b. Área auditada
    c. Responsable del área auditada
    d. Cargo del responsable del área auditada
    e. Email del responsable del área auditada
    f. Objetivo de la auditoría
    g. Alcance de la auditoría

h. Fechas de la auditoría
i. Total, días de duración de la auditoría
j. Integrantes del equipo auditor
k. Email de los integrantes del equipo auditor
l. Actividades realizadas en la auditoría
    i. Criterios para el muestreo
    ii. Actividades principales
    iii. Observaciones de la evaluación
    iv. Observaciones de la evaluación de requisitos de la especificación técnica, proceso o servicio.
m. Observaciones
n. Recomendaciones
o. Nombre del auditor asignado al área auditada, cargo del auditor, firma del auditor.

6. Reunión de cierre.

Seguimiento a los hallazgos generados en la presente auditoría interna.

6. Medios de divulgación:
Se informará a los interesados por medio de oficios físicos dirigidos y a sus correos electrónicos empresariales.

	Nombres y Apellidos	**Cargo**	**Fecha**	**Firma**
Elaborado				
Revisado				
Aprobado				

10.3 Anexo - 2.3 Gestión de Indicadores

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**GESTIÓN DE INDICADORES**	Código: DGSI-03
		Versión:1
		Fecha de aprobación: Marzo 2021
		Páginas:

ESQUEMA

1. Introducción

Es importante establecer indicadores que ayudan a medir la eficacia de los lineamientos definidos en el sistema de gestión de la seguridad, realizando un control con datos medidos de manera actualizada.

2. Objetivo

Establecer los indicadores necesarios para la supervisión de los controles de seguridad.

3. Alcance

Todas las áreas en las que se implemente por lo menos un control.

4. Marco normativo y regulatorio

5. Descripción

La medición sistemática de los controles de seguridad y su temporalidad, permite tener una visión clara de la efectividad de los mismos.

A continuación, se listan los componentes de cada indicador:

COMPONENTE	DESCRIPCIÓN
ID del indicador	Nomenclatura única definida por la empresa para identificar el indicador.
Nombre del indicador	Representa la medición que se va a realizar.
Descripción	Explicación del objetivo del indicador.
Control del seguridad	Control al cual se le realiza la medición.
Tipo	Efectiva, eficiencia o impacto.
Fórmula	Fórmula para realizar la medición.
Umbral	Límite mínimo para el control.
Unidad de medida	Unidad de medida definida para el cálculo.
Frecuencia de medición	Periodo de tiempo en el cual se realiza cada medición.
Propietario del indicador	Área o persona responsable de la medida.
Responsable del indicador	Responsable de recolectar los datos.
Formato de la información	Tipo de formato para la entrega de la medición.

INDICADORES:

Política de seguridad:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I001
Nombre del indicador	Política de seguridad
Descripción	Indica si la política establecida por la empresa se revisa y actualiza según se crea necesario.
Control del seguridad	Revisión de las políticas para la seguridad de la información.
Tipo	Implementación
Fórmula	Número de revisiones / 1 año
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Número de revisiones
Frecuencia de medición	Anual
Propietario del indicador	Director de tecnología
Responsable del indicador	Auditor interno
Formato de la información	Documento con informe de revisión

Organización de la seguridad de la información:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I002
Nombre del indicador	Contacto con proveedores
Descripción	Medida de la comunicación regular y efectiva con los proveedores de servicios, con el fin de tener una respuesta efectiva ante fallas.
Control del seguridad	6.1.3 Contacto con autoridades
Tipo	Implementación
Fórmula	Número de comunicaciones / 3 meses
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Número de comunicaciones
Frecuencia de medición	Trimestral
Propietario del indicador	Director de tecnología
Responsable del indicador	Auditor interno
Formato de la información	Documento con informe de comunicaciones

Seguridad de los recursos humanos:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I003
Nombre del indicador	Actualización de hoja de vida
Descripción	Medición del control en la actualización de las hojas de vida del personal de la empresa. Cada líder de área certificará que las hojas de vida de los integrantes de sus equipos se encuentran debidamente actualizadas.
Control del seguridad	7.1.1 Selección
Tipo	Implementación
Fórmula	Certificación / semestral
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Certificación
Frecuencia de medición	Semestral
Propietario del indicador	Director ejecutivo
Responsable del indicador	Auditor interno
Formato de la información	Lista de chequeo de entrega

Gestión de activos:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I004
Nombre del indicador	Asignación de activos
Descripción	Actas de entrega debidamente diligenciadas con la asignación de activos a cada empleado de la empresa.
Control del seguridad	8.1.1 Inventario de activos
Tipo	implementación
Fórmula	Número de actas de asignación / número de empleados
Umbral	< 95% no cumplido, >=95% cumplido
Unidad de medida	Porcentaje de empleados con activos asignados
Frecuencia de medición	Trimestral
Propietario del indicador	Auxiliar administrativo
Responsable del indicador	Auditor interno
Formato de la información	Gráfico circular

Control de acceso:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I005
Nombre del indicador	Registro de usuarios
Descripción	Llevar control de los usuarios y los permisos que tengan en relación a la información de cada área
Control del seguridad	9.2.1 Registro de usuarios y cancelación del registro
Tipo	Implementación
Fórmula	Número de empleados activos / Número de formato de asignación de permisos
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Número de empleados
Frecuencia de medición	Mensual
Propietario del indicador	Director de tecnología
Responsable del indicador	Auditor interno
Formato de la información	Documento de informe

Seguridad física y del entorno:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I006
Nombre del indicador	Capacitaciones
Descripción	Se mide la cantidad de empleados activos capacitados con relación con hábitos de seguridad
Control del seguridad	11.2.8 Equipos de usuario desatendido
Tipo	Implementación
Fórmula	Empleados activos capacitados / Total de empleados activos
Umbral	< 80% no cumplido, >= 80% cumplido
Unidad de medida	Porcentaje
Frecuencia de medición	Semestral
Propietario del indicador	Director de tecnología
Responsable del indicador	Auditor interno
Formato de la información	Gráfico circular

Seguridad de las operaciones:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I007
Nombre del indicador	Copias de seguridad
Descripción	Medir la realización periódica de copias de seguridad de la información de la empresa
Control del seguridad	12.3.1 Respaldo de la información
Tipo	Implementación
Fórmula	Copia de seguridad / semana
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Archivo
Frecuencia de medición	Semanal
Propietario del indicador	Director de tecnología
Responsable del indicador	Director de tecnología
Formato de la información	Tabla de seguimiento de copias de seguridad

Seguridad de las comunicaciones:

COMPONENTE	DESCRIPCIÓN
ID del indicador	I008
Nombre del indicador	Acuerdos de confidencialidad
Descripción	Indica la generación de acuerdos de confidencialidad de los empleados de la empresa en relación con la información a la que tienen acceso.
Control del seguridad	13.2.4 Acuerdos de confidencialidad y de no divulgación
Tipo	Implementación
Fórmula	Número de acuerdos / número de empleados
Umbral	< 95% no cumplido, >= 95% cumplido
Unidad de medida	Porcentaje de empleados con acuerdos firmados
Frecuencia de medición	Trimestral
Propietario del indicador	Auxiliar administrativo
Responsable del indicador	Auditor interno
Formato de la información	Gráfico circular

Adquisición, desarrollo y mantenimientos de sistemas

COMPONENTE	DESCRIPCIÓN
ID del indicador	I009
Nombre del indicador	Pruebas de seguridad
Descripción	Mide la realización de pruebas de seguridad del sistema
Control del seguridad	14.2.8 Pruebas de seguridad del sistema
Tipo	Implementación
Fórmula	Total número de pruebas
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Número de prueba
Frecuencia de medición	Trimestral
Propietario del indicador	Director de tecnología
Responsable del indicador	Director de tecnología
Formato de la información	Documento con informe de resultado de pruebas

Gestión de incidentes de seguridad de la información

COMPONENTE	DESCRIPCIÓN
ID del indicador	I010
Nombre del indicador	Incidentes de seguridad
Descripción	Se mide la cantidad de incidentes reportados y solucionados
Control del seguridad	16.1.2 Reporte de eventos de seguridad de la información 16.1.5 Respuesta a incidentes de seguridad de la información
Tipo	Implementación
Fórmula	Número de incidentes solucionados / número de incidentes reportados
Umbral	< 75% no cumplido, >= 75% cumplido
Unidad de medida	Porcentaje de incidentes solucionados
Frecuencia de medición	Mensual
Propietario del indicador	Director de tecnología
Responsable del indicador	Auditor interno
Formato de la información	Gráfico circular

Cumplimiento

COMPONENTE	DESCRIPCIÓN
ID del indicador	I011
Nombre del indicador	Política de privacidad
Descripción	Indica si la política establecida por la empresa se revisa y actualiza según se crea necesario.
Control del seguridad	18.1.4 Privacidad y protección de información de datos personales
Tipo	Implementación
Fórmula	Número de revisiones / 1 año
Umbral	<1 no cumplido, >=1 cumplido
Unidad de medida	Número de revisiones
Frecuencia de medición	Anual
Propietario del indicador	Director de tecnología
Responsable del indicador	Auditor interno
Formato de la información	Documento con informe de revisión

6. Medios de divulgación:
A través de medios físicos y digitales y correo electrónico empresarial.

	Nombres y Apellidos	Cargo	Fecha	Firma
Elaborado				
Revisado				
Aprobado				

10.4 Anexo - 2.4 Procedimiento Revisión por Dirección

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**REVISIÓN POR ALTA DIRECCIÓN**	Código: DGSI-04
		Versión:1
		Fecha de aprobación: Marzo 2021
		Páginas:

ESQUEMA
1. Introducción Parte fundamental de la Alta Dirección está en establecer revisiones periódicas de la implementación y ejecución correcta del Plan Director del SGSI de la empresa para asegurar la eficacia y mejora continua del sistema.
2. Objetivo Inspeccionar y evaluar los documentos, procedimientos y controles que hacen parte del Pan Director del Sistema de Gestión de la Seguridad de la Información de la Empresa.
3. Alcance

Dirigido al área Directiva de la empresa.

4. Marco normativo y regulatorio

Norma ISO/IEC 27001

5. Descripción

El proceso de revisión de la Alta Dirección sobre los documentos, procedimientos y controles del Plan Director del SGSI establece los puntos de entrada y de salida resultantes de las revisiones.

5.1 Puntos de entrada

A continuación se listan los puntos de entrada cuyo propósito son objeto de revisión por la Alta dirección:

a) Resultados del estado de las acciones desde anteriores revisiones por la dirección general.
b) Información sobre cambios realizados en asuntos internos y externos referentes al sistema de gestión de la Seguridad de la Información.
c) Resultados de la información sobre el comportamiento de la seguridad de la información, incluyendo tendencias referentes a:
    1) No conformidades y acciones correctivas.
    2) Seguimiento y resultados de las mediciones.
    3) Resultados de auditoría.
    4) Cumplimiento de los objetivos de seguridad de la información
d) Observaciones realizadas por las partes interesadas.
e) Resultados de la evaluación de los riesgos y la etapa del plan de tratamiento de riesgos.
f) Las oportunidades de mejora.
g) Análisis de la información suministrada en relación al desempeño de los procesos y conformidad de los servicios.
h) Verificación del cumplimiento de los objetivos establecidos en relación a la seguridad.
i) Resultados de los indicadores de gestión y de medición de seguridad de los activos y recursos.

5.2 Puntos de salida

a) El Responsable de Seguridad (CISO) es el encargado de realizar el seguimiento y monitoreo de los planes de acción definidos en base a los resultados del análisis de las revisiones y de informar sobre el estado a la Alta Dirección.
b) El resultado de esto proceso se debe generar un documento donde se indique las oportunidades de mejora o los cambios requeridos identificados en los planes de acción del SGSI, los responsables del proceso y las fechas de realización o ejecución.
c) Se debe realizar actualizaciones de la evaluación de riesgos y del plan de tratamiento de riesgos.
d) Se debe socializar los resultados de las oportunidades de mejora o cambios requeridos con el objetivo de dar a establecer las metas próximas teniendo en cuenta las oportunidades y darle una correcta continuidad del negocio.

6. Medios de divulgación:

A través de medios físicos y digitales y correo electrónico empresarial.

	Nombres y Apellidos	**Cargo**	**Fecha**	**Firma**
Elaborado				
Revisado				
Aprobado				

10.5 Anexo - 2.5 Gestión de Roles y Responsabilidades

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**ROLES Y RESPONSABILIDADES**	Código: DGSI-05 Versión:1 Fecha de aprobación: Marzo 2021 Páginas:

ESQUEMA

1. Introducción

Dentro de la continuidad del negocio para obtener una certificación en la empresa es indispensable asignar y establecer los roles y responsabilidades al personal para poder cumplir con la correcta gestión de la seguridad de la información.

2. Objetivo

Definir y establecer los roles y responsabilidades al personal de la empresa identificando las áreas de trabajo y las funciones asignadas.

3. Alcance

Dirigido a todos los funcionarios de las áreas de la empresa incluyendo proveedores y asociados que intervienen en los procesos de la seguridad de la información y de los activos

4. Marco normativo y regulatorio

Norma ISO/IEC 27001

5. Descripción

A continuación se describen los roles y las responsabilidades de acuerdo al objetivo planteado y el alcance que se desea obtener:

5.1 Responsable de Seguridad

Es el encargado de planear, verificar, ejecutar y darle seguimiento a la implantación del SGSI. El rol es asumido por el responsable o Director de Tecnología o jefe de tecnología (CTO). Las responsabilidades de este rol son:

- Ser parte de la elaboración, revisión y divulgación de las políticas, lineamientos, procedimientos y metodologías de la seguridad de la información de la empresa.
- Gestionar, supervisar y evaluar el cumplimiento de las políticas procedimientos y controles de seguridad de la información.
- Gestionar el comité de seguridad asignando roles, funciones y responsabilidades.
- Analizar, gestionar y hacer seguimiento a las incidencias de seguridad producidas en la empresa.

- Coordinar y supervisar el análisis de riesgos de los procesos y activos más críticos y sensibles.
- Dar respuesta a la reducción de riesgos presentados en el análisis realizado.
- Supervisar la planeación y ejecución de las auditorias.
- Revisar los reportes o informes de auditoría.

5.2 Comité de Seguridad

Conformado por el Responsable de Seguridad (Director de Tecnología o jefe de tecnología CTO), el Director Ejecutivo CEO, el Jefe de Redes Estructuradas y Servidores, el Jefe de desarrollo de software y el Jefe de soporte técnico. Las responsabilidades y funciones son:

- Gestionar y validar el plan director del sistema de gestión de la seguridad de la información.
- Gestionar y promover la implementación de controles y buenas prácticas en la seguridad de la información de la empresa.
- Asignar los roles y responsabilidades a los diferentes funcionarios relacionados con la seguridad de la información.
- Coordinar el análisis de incidentes y el análisis de riesgos y las diferentes acciones para los procesos de mitigación y prevención.
- Supervisar y validar el cumplimiento de las políticas de seguridad implementadas en la empresa.

5.3 Director General

Encargado de coordinar y orientar las directrices y estrategias del plan director del SGSI con los objetivos de la empresa. Es asumido por el Director Ejecutivo CEO, cuyas funciones y responsabilidades son:

- Aprobar las políticas, procedimientos, metodologías y controles de seguridad de la información.
- Impulsar y promover el desarrollo de proyectos e iniciativas de seguridad.
- Participar en el desarrollo y evaluación de planes de acción para la mitigación de riesgos y prevención de incidentes en la empresa.
- Velar por el cumplimiento de las políticas de seguridad de la información en la empresa.

5.4 Auditor interno

Encargado de planear y ejecutar las auditorías internas para determinar el cumplimiento de los requisitos y controles del sistema de gestión de la seguridad de la información en la empresa. Este rol puede ser desempeñado por uno de los jefes de las áreas conformadas por la empresa o por el Director de Tecnología o jefe de tecnología CTO, con capacidades y experiencia en auditorias. Las responsabilidades y funciones que desempeña este rol son:

- Planear y realizar las auditorías internas al SGSI de la empresa.
- Defender la integridad, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría.
- Convocar y gestionar las reuniones para la obtención de la información con el personal involucrado en el proceso de auditoría.

5.5 Dueño o propietario del Activo

Este rol pertenece a cada usuario y personal integrante de la empresa el cual tiene a cargo diferentes activos en la empresa. Las responsabilidades y funciones de este rol son:

- Clasificar y proteger los activos de la información que tiene a su cargo o responsabilidad.
- Verificar que los controles de seguridad se apliquen correctamente dependiendo del nivel de criticidad de cada activo asignado.
- Realizar un seguimiento y reporte del estado y los cambios que se han realizado al activo y de la reasignación de activos a otro usuario o personal dentro de la empresa.

6. Medios de divulgación:
A través de medios físicos y digitales y correo electrónico empresarial.

	Nombres y Apellidos	Cargo	Fecha	Firma
Elaborado				
Revisado				
Aprobado				

10.6 Anexo - 2.6 Metodología de Análisis de Riesgos

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**ANALISIS DE RIESGOS**	Código: DGSI-06
		Versión:1
		Fecha de aprobación: Marzo 2021
		Páginas:

ESQUEMA

1. Introducción
El marco de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT versión 3.0 busca orientar a la empresas u organizaciones en la gestión de los riesgos de seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) integrando la presente metodología a los diferentes casos que se puedan presentar y vinculando la identificación y el análisis de riesgos a las entidades u organizaciones.

2. Objetivos

- Definir la metodología a emplear y adoptar para la gestión de riesgos de la seguridad de la información.
- Guiar a la empresa en el proceso de gestión de riesgos de seguridad de la información integrando la metodología MAGERIT V3.0 como escenario a implementar en el proceso de control y supervisión de la gestión de riesgos.
- Identificar y analizar los riesgos del Sistema de Gestión de Riesgos de la Seguridad de la Información.

3. Alcance
Para definir el alcance y los limites en la gestión de riesgos se debe tener en cuenta aspectos relacionados tales como: Procesos de la empresa, estructura de la empresa, funciones de la empresa y sus integrantes, objetivos y políticas de la empresa, ubicación de la empresa y características geográficas,

estructura legal y reglamentaria de la empresa, enfoque global dirigido a la gestión del riesgo, misión y visión integrada a la gestión de riesgos de la empresa, entre otros.

4. Marco normativo y regulatorio

Norma ISO/IEC 27001
Norma ISO/IEC 27002

5. Descripción

La metodología MAGERIT establece las siguientes etapas para el análisis de riesgos principales para el desarrollo de la misma:

5.1 Identificación de activos

Teniendo en cuenta la norma ISO/IEC 27000:2013 un activo se define como todo aquello que tiene valor para una empresa u organización; y que por consiguiente requiere ser protegido.

Los activos se pueden agrupar en los siguientes tipos:

- Instalaciones
- Datos
- Personal
- Componentes hardware
- Componentes software
- Servicios
- Red
- Equipamiento auxiliar.

Cada activo posee algunas características que permiten su identificación tales como:

- Tipo de activo
- Propietario del activo
- Ubicación física del activo
- Factor de criticidad

El **Factor de criticidad** permite establecer el nivel o estado en que el activo es relevante en los procesos de la empresa y se lo determina en la siguiente tabla:

Estado	Descripción
Alto	El activo es altamente relevante para los procesos esenciales de la empresa y es indispensablemente disponible. La continuidad de la empresa se pone en peligro.
Medio	El activo es medianamente importante para los procesos de la empresa y su ausente disponibilidad retrasa algunos procesos. La continuidad de la empresa no se ve afectada.
Bajo	El activo interviene en algunos procesos de la empresa que no están directamente relacionados con la empresa y su ausente disponibilidad causa algún contratiempo. La continuidad en ningún caso se ve afectada.

5.2 Identificación de amenazas

Las amenazas pueden causar daños a los activos en una empresa u organización. Por lo tanto, para la identificación de amenazas se puede clasificar en 2 grupos, amenazas según su **origen** y amenazas según su **intención.**

Origen: según su origen las amenazas se deben clasificar en:

- **Ambientales** o naturales: eventos ambientales o naturales.
- **Deliberadas** o humanas: intervención humana.
- **Accidentales** o de entorno: causadas por un fallo, deterioro, o accidente de equipos, dispositivos o infraestructuras.

Se debe tener presente que un activo puede ser identificado en varios tipos de amenazas.

Intención: se valora cada amenaza según la intención que alguien realice sobre los activos:

- **Alta:** intención de obtener beneficios económicos o daños a personas
- **Media:** intención de hacer daños a una empresa u organización.
- **Baja:** intención de demostrar conocimiento o solo por juego.
- **N/A:** no aplica.

Teniendo en cuenta los activos de la empresa se puede identificar y clasificar las amenazas según su origen y su intención:

Activo	Amenazas según su origen	Amenazas según su intención
Equipos de sobremesa	Ambientales, Deliberadas y Accidentales	Alta, Media
Laptops	Ambientales, Deliberadas y Accidentales	Alta, Media
Impresora	Ambientales, Deliberadas y Accidentales	Alta, Media
Puntos de acceso wifi	Ambientales, Deliberadas y Accidentales	Alta, Media
Empleados	Deliberadas	N/A
Entornos de producción	Deliberadas y Accidentales	Media, Baja
Sistema Operativo Windows	Deliberadas	Media, Baja
Antivirus	Deliberadas	Media
Contactos de clientes y proveedores	Deliberadas	Media

5.3 Identificación de vulnerabilidades

Una vez definida la relación activos-amenazas, se requiere identificar las vulnerabilidades en donde se hace visible y real las amenazas. Para ello, las vulnerabilidades se pueden clasificar en los siguientes tipos:

- Hardware
- Software
- Red o comunicaciones
- Personal
- Organización
- Documentación

En la empresa se identifican las vulnerabilidades teniendo en cuenta los activos identificados anteriormente.

Activo	Tipo de vulnerabilidades
Equipos de sobremesa	Hardware Organización Documentación
Laptops	Hardware Organización Documentación
Impresora	Hardware Organización Documentación
Puntos de acceso wifi	Hardware Red o comunicaciones Organización Documentación
Empleados	Personal Organización Documentación
Entornos de producción	Software Red o comunicaciones Organización Documentación
Sistema Operativo Windows	Software Personal Organización Documentación
Antivirus	Software Red o comunicaciones Organización Documentación
Contactos de clientes y	Software

proveedores	Personal Organización Documentación

5.4. Establecimiento de la probabilidad y de impacto

La probabilidad es entendida como la posibilidad de ocurrencia de un riesgo, el cual se ha determinado mediante valores de orden inferior a orden superior según la frecuencia en que ocurre; mientras tanto el impacto son las consecuencias que puede ocasionar la ejecución del riesgo. Para el marco **MAGRSI** se tiene en cuenta los siguientes aspectos para la probabilidad, el impacto y el nivel de riesgo.

Para realizar el **análisis de probabilidad** se tiene en cuenta los siguientes aspectos:

- Inviable: asignado con valor → 1
- Poco viable: asignado con valor → 2
- Viable: asignado con valor → 3

Para realizar el **análisis de impacto** se tiene en cuenta los siguientes aspectos:

- Inferior: asignado con valor → 1
- Moderado: asignado con valor → 2
- Superior: asignado con valor → 3

Nivel de riesgo:

- B → Bajo
- M → Medio
- A → Alto

5.5. Identificación de controles

Se debe realizar la identificación de controles que protegen los activos después de que se haya realizado la identificación de amenazas y vulnerabilidades con el objetivo de evitar trabajo ya realizado y costos innecesarios. Los controles los podemos clasificar en:

- **No ejecutado:** se asigna un porcentaje de 0% del control identificado.
- **En proceso de ejecución:** se asigna un porcentaje de 30% del control identificado.
- **Ejecutado Parcialmente:** se asigna un porcentaje de 50% del control identificado.
- **Ejecutado Totalmente:** se asigna un porcentaje de 100% del control identificado.

Según la clasificación del control podemos valora su grado de protección con los siguientes ítems:

- **Alta**
- **Media**
- **Baja**

El grado de protección se establece según el porcentaje asignado a la clasificación del control:

- Si el control es menor o igual del 30% su grado de protección es Baja
- Si el control es mayor al 30% y menor o igual al 50% su grado de protección es Media
- Si el control es mayor al 50% su grado de protección es Alta

La identificación de controles realizado a la empresa se ve reflejado en los siguientes resultados:

Activo que se aplica control	Clasificación de controles	Porcentaje asignado al control	Grado de protección
Equipos de sobremesa	Ejecutado Parcialmente	50%	Media
Laptops	Ejecutado Parcialmente	50%	Media
Impresora	Ejecutado Parcialmente	50%	Media
Puntos de acceso wifi	Ejecutado Parcialmente	50%	Media
Empleados	No ejecutado	0%	Baja
Entornos de producción	Ejecutado Totalmente	100%	Alta
Sistema Operativo Windows	Ejecutado Parcialmente	50%	Media
Antivirus	Ejecutado Totalmente	100%	Alta
Contactos de clientes y proveedores	Ejecutado Parcialmente	50%	Media

5.6. Análisis de riesgos

Para realizar el análisis de riesgos se utiliza la **"Matriz de evaluación de riesgos"**, la cual establece el nivel de probabilidad de ocurrencia del riesgo versus el impacto que ocasiona. Esta matriz se valora según el nivel de riesgo establecido.

Matriz de evaluación de riesgos	Probabilidad		
Impacto	**Inviable (1)**	**Poco viable (2)**	**Viable (3)**
Inferior (1)	**B**	**B**	**M**
Moderado (2)	**B**	**M**	**A**
Superior (3)	**M**	**A**	**A**

Tabla - Matriz de probabilidad e impacto de riesgos

Tomando como referencia la "**Matriz de probabilidad e impacto de riesgos"** podemos aplicarla al caso en estudio de la empresa realizando un análisis a los activos presentados

Análisis de Riesgos			
Activo	**Valoración**		**Nivel de Riesgo**
	Probabilidad	**Impacto**	
Equipos de sobremesa	3	3	Alto
Laptops	3	2	Alto
Impresora	2	2	Medio
Puntos de acceso wifi	3	2	Alto
Empleados	2	2	Medio
Entornos de producción	3	3	Alto
Sistema Operativo Windows	3	1	Medio
Antivirus	2	2	Medio
Contactos de clientes y proveedores	3	3	Alto

5.7 Tratamiento de riesgos

Una vez realizado el análisis de riesgo teniendo en cuenta los activos que se encuentran por encima del nivel de riesgo aceptable.

En el momento de realizar el tratamiento de riesgos se debe decidir el método para su aplicación, definidos en las siguientes opciones:

- **Reducirlos:** se establecen los controles que se aplican para reducir o mitigar los riesgos teniendo un nivel de riesgo con una probabilidad

Poco viable (2) y un impacto **Moderado (2**). El riesgo se puede reducir mas no eliminar completamente.

- **Transferirlos:** se realiza el proceso de transferir los riesgos que están por encima del umbral y la empresa decide contratar terceras partes para que gestionen el riesgo. Este proceso se decide cuando los costos de la contratación son mínimos y se requiere procesos específicos para la gestión.
- **Aceptarlos:** en esta opción se acepta la existencia de un riesgo prioritario, en donde el proceso de implantar controles implica un costo mayor y la empresa decide la implantación. Usualmente, el riesgo se encuentra en un nivel de probabilidad **Viable (3)** y un impacto **Superior (3)**

Se procede a realizar el tratamiento de riesgos en donde se indican los siguientes aspectos:

a) Selección de controles del Anexo A de la norma ISO/IEC 27001
b) Identificación de las acciones que serán necesarias para implementar los controles seleccionados.
c) Determinar los plazos acordados para implementar las acciones.
d) Definir los responsables y recursos.
e) Implantación de controles de seguridad designados.

6. Medios de divulgación:
A través de correos electrónicos empresariales

	Nombres y Apellidos	Cargo	Fecha	Firma
Elaborado				
Revisado				
Aprobado				

10.7 Anexo - 2.7 Declaración de Aplicabilidad

EXPERTEC SERVICIOS Y SOLUCIONES INFORMÁTICAS	**DECLARACIÓN DE APLICABILIDAD**	Código: DGSI-07 Versión:1 Fecha de aprobación: Marzo 2021 Páginas:

ESQUEMA

1. Introducción
Definida y analizada la etapa de análisis de riesgos se establecen los controles de la norma ISO/IEC 27002 que se aplican o no se aplican en la empresa de Servicios y Soluciones Informáticas. Estos controles se sustentan con una justificación y posteriormente deben ser revisados y aprobados por las directivas de la empresa.

2. Objetivo

Determinar qué controles de la norma ISO/IEC 27002 se aplican o no en los procesos de la empresa.
3. Alcance El alcance está orientado a todas las áreas o dependencias dela empresa.
4. Marco normativo y regulatorio Norma ISO/IEC 27002
5. Descripción La declaración de la aplicabilidad está sustentada en la siguiente tabla constituida por los controles

CONTROLES	APLICA/ NO APLICA	JUSTIFICACIÓN
A.5 Políticas de seguridad de la información		
5.1 Directrices de gestión de la seguridad de la información		
A.5.1.1 Políticas para la seguridad de la información	Aplica	Es requisito fundamental e indispensable del SGSI de la empresa.
A.5.1.2 Revisión de las políticas para la seguridad de la información	Aplica	Es requisito fundamental e indispensable del SGSI de la empresa.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
A.6.1.1 Roles y responsabilidades para la seguridad de la información	Aplica	Se debe definir roles y responsabilidades de las tareas asignadas.
A.6.1.2 Separación de deberes	Aplica	Se debe identificar que deberes cumple cada personal en los roles asignados.
A.6.1.3 Contacto con las autoridades	Aplica	El permanente contacto con las autoridades involucradas con el SGSI
A.6.1.4 Contacto con grupos de interés especial	Aplica	Permanente actualización a foros, noticias y organismos de interés en la seguridad de la información.
A.6.1.5 Seguridad de la información en la gestión de proyectos.	Aplica	Se debe involucrar la seguridad en los procesos del negocio, procesos del área TI y en los servicios y productos.
A.6.2 Dispositivos móviles y teletrabajo		
A.6.2.1 Política para dispositivos móviles	Aplica	Se debe adoptar medidas para mitigar los riesgos de la mala utilización de dispositivos móviles.
A.6.2.2 Teletrabajo	Aplica	Garantizar la opción de teletrabajo seguro en la empresa dada la situación actual de COVID19 y velar por la

		protección de los activos y recursos utilizados.
A.7 Seguridad de los recursos humanos		
A.7.1 Antes de asumir el empleo		
A.7.1.1 Selección	Aplica	Se debe aplicar controles de verificación de temas de seguridad, experiencia y formación del personal.
A.7.1.2 Términos y condiciones del empleo	Aplica	Se debe aplicar controles en las responsabilidades y obligaciones ligadas a la seguridad de la información en la contratación.
A.7.2 Durante la ejecución del empleo		
A.7.2.1 Responsabilidades de la dirección	Aplica	Aplicar control para que la dirección exija a los funcionarios el cumplimiento de las políticas, normas y procedimientos.
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Aplica	Control que se aplica para que los funcionarios se capaciten en la parte de concientización y formación en seguridad de la información.
A.7.2.3 Proceso disciplinario	Aplica	Se debe implementar un control para procesos disciplinarios en el incumplimiento de las políticas.
A.7.3 Terminación y cambio de empleo		
A.7.3.1 Terminación o cambio de responsabilidades de empleo	Aplica	Después de terminación o cambio de cargo se debe aplicar un control para establecer comunicar las responsabilidades del funcionario.
A.8 Gestión de activos		
A.8.1 Responsabilidad por los activos		

A.8.1.1 Inventario de activos	Aplica	Aplicar un control sobre la forma y método que se hace la identificación y clasificación de los activos
A.8.1.2 Propiedad de los activos	Aplica	Aplicar control para identificar el propietario de los activos
A.8.1.3 Uso aceptable de los activos	Aplica	Aplicar control para verificar que se utilice correctamente el activo.
A.8.1.4 Devolución de activos	Aplica	Requerimiento para devolución de activos.
A.8.2 Clasificación de la información		
A.8.2.1 Clasificación de la información	Aplica	Uso de control para clasificar la información según su valor, requisitos legales y nivel de protección.
A.8.2.2 Etiquetado de la información	Aplica	Uso de control para identificar y clasificar la información
A.8.2.3 Manejo de activos	Aplica	Uso de control para manejo de activos según su clasificación
A.8.3 Manejo de medios		
A.8.3.1 Gestión de medio removibles	Aplica	Manejo de control para administrar el uso de medios extraíbles en las áreas y activos críticos y sensibles de la empresa.
A.8.3.2 Disposición de los medios	Aplica	Manejo de control para disponer y utilizar los medios removibles
A.8.3.3 Transferencia de medios físicos	Aplica	Disposición de control para traslado de medios físicos entre las áreas de la empresa.
A.9 Control de acceso		
A.9.1 Requisitos del negocio para el control de acceso		
A.9.1.1 Política de control de acceso	Aplica	Aplicar controles para establecer las reglas de acceso de la

		información en los diferentes sistemas de la empresa.
A.9.1.2 Acceso a redes y a servicios en red	Aplica	Aplicar controles para establecer las reglas de acceso de la información en las redes y servicios de la empresa.
A.9.2 Gestión de acceso de usuarios		
A.9.2.1 Registro y cancelación del registro de usuarios	Aplica	Aplicar controles para registrar y dar de baja a usuarios en los servicios y sistemas.
A.9.2.2 Suministro de acceso de usuarios	Aplica	Requisitos para administra el acceso a los usuarios en la sistemas y servicios de la empresa
A.9.2.3 Gestión de derechos de acceso privilegiado	Aplica	Requisitos para gestionar los privilegios del personal en el acceso
A.9.2.4 Gestión de información de autenticación secreta de usuarios	Aplica	Aplicación de estandarización de contraseñas en los accesos
A.9.2.5 Revisión de los derechos de acceso de usuarios	Aplica	Aplicar controles de revisión de permisos de los accesos de los usuarios a los sistemas y servicios
A.9.2.6 Retiro o ajuste de los derechos de acceso	Aplica	
A.9.3 Responsabilidades de los usuarios		
A.9.3.1 Uso de información de autenticación secreta	Aplica	Se debe aplicar normas para la utilización de contraseñas según estándares de la empresa.
A.9.4 Control de acceso a sistemas y aplicaciones		
A.9.4.1 Restricción de acceso a la información	Aplica	Aplicar restricciones al acceso de la información según los permisos otorgados a los usuarios
A.9.4.2 Procedimiento de ingreso seguro	Aplica	Aplicar controles de inicio de sesión seguros
A.9.4.3 Sistema de gestión de	Aplica	Gestión de

contraseñas		contraseñas seguras.
A.9.4.4 Uso de programas utilitarios privilegiados	Aplica	Se debe restringir el uso de programas que bloquean el sistema y los servicios.
A.9.4.5 Control de acceso a códigos fuente de programas	Aplica	Se debe restringir el acceso a código fuente de los desarrollos de software y de los sistemas y servicios.
A.10 Criptografía		
A.10.1 Controles criptográficos		
A.10.1.1 Política sobre el uso de controles criptográficos	Aplica	Implementar política para la utilización de controles criptográficos en los servicios y sistemas.
A.10.1.2 Gestión de llaves	Aplica	Tener políticas para la gestión de contraseñas seguras y su validez periódica.
A.11 Seguridad física y del entorno		
A.11.1 Áreas seguras		
A.11.1.1 Perímetro de seguridad física	Aplica	Aplicar controles para la entrada física no autorizada.
A.11.1.2 Controles de acceso físicos	Aplica	Requisitos para la protección de sitios físicos con acceso autorizado.
A.11.1.3 Seguridad de oficinas, recintos e instalaciones	Aplica	Requisitos para la seguridad de acceso a oficinas y lugares restringidos.
A.11.1.4 Protección contra amenazas externas y ambientales	Aplica	Disposición de planes de protección y emergencias ante amenazas externas y ambientales
A.11.1.5 Trabajo en áreas seguras	Aplica	Se debe generar prohibiciones para el acceso y trabajo en áreas seguras y de acceso publico
A.11.1.6 Áreas de carga, despacho y acceso público	Aplica	
A.11.2 Equipos		
A.11.2.1 Ubicación y protección de los equipos	Aplica	Requisitos para proteger los equipos de daños ambientales y accesos no

		autorizados
A.11.2.2 Servicios de suministro	Aplica	Se debe tener medidas de control de suministro para mantener las operaciones de las instalaciones y los equipos disponibles permanentemente.
A.11.2.3 Seguridad en el cableado	Aplica	Se debe tener medidas para la protección de cables eléctricos y de datos
A.11.2.4 Mantenimiento de los equipos	Aplica	Realización de mantenimiento de equipos para garantizar el óptimo funcionamiento de los equipos.
A.11.2.5 Retiro de activos	Aplica	Se debe controlar y gestionar el retiro o baja de activos
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Aplica	Registra los equipos y activos que salen de la empresa.
A.11.2.7 Disposición segura o reutilización de equipos	Aplica	Se debe gestionar los equipos que se van a reutilizar siguiendo ciertos requisitos
A.11.2.8 Equipos de usuario desatendido	Aplica	Aplicar controles de sesiones abiertas de equipos de usuario desatendido
A.11.2.9 Política de escritorio limpio y pantalla limpia	Aplica	Aplicar controles para escritorio limpio y pantalla limpia
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos operacionales y responsabilidades		
A.12.1.1 Procedimientos de operación documentados	Aplica	Requisito de la política de seguridad aplicada a la empresa.
A.12.1.2 Gestión de cambios	Aplica	
A.12.1.3 Gestión de capacidad	Aplica	Aplicar controles para evitar la pérdida de disponibilidad y rendimiento de los sistemas
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Aplica	Requisito necesario en el área de desarrollo para controlar la

		separación de ambiente de producción con los de desarrollo y pruebas
A.12.2 Protección contra códigos maliciosos		
A.12.2.1 Controles contra códigos maliciosos	Aplica	Implementar sistemas de detección de código malicioso
A.12.3 Copias de seguridad		
A.12.3.1 Respaldo de la información	Aplica	Requisito de la política de seguridad para la copia de seguridad teniendo en cuenta la frecuencia de la realización de esta.
A.12.4 Registro y seguimiento		
A.12.4.1 Registro de eventos	Aplica	Control de registro de eventos para determinar sucesos en caso de incidencias y posibles soluciones
A.12.4.2 Protección de la información de registro	Aplica	Se debe proteger los registros de eventos para evitar pérdidas, corrupción o cambios no autorizados en los sistemas y servicios.
A.12.4.3 Registros del administrador y del operador	Aplica	
A.12.4.4 Sincronización de relojes	Aplica	
A.12.5 Control de software operacional		
A.12.5.1 Instalación de software en sistemas operativos	Aplica	Gestionar procesos de instalación de software y S.O. en los equipos
A.12.6 Gestión de la vulnerabilidad técnica		
A.12.6.1 Gestión de las vulnerabilidades técnicas	Aplica	Se debe identificar y gestión las vulnerabilidades existentes en los sistemas y servicios.
A.12.6.2 Restricciones sobre la instalación de software	Aplica	Requisito que determina el tipo de software a instalar y sus restricciones.
A.12.7 Consideraciones sobre auditorias de sistemas de información		
A.12.7.1 Controles de auditorías de sistemas de información	Aplica	Se debe evaluar el funcionamiento y desempeño de los sistemas realizando auditoria de sistemas.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		

A.13.1.1 Controles de redes	Aplica	Disponer de lineamientos para la gestión y control de la red interna y externa de la empresa
A.13.1.2 Seguridad de los servicios de red	Aplica	
A.13.1.3 Separación en las redes	Aplica	
A.13.2 Transferencia de información		
A.13.2.1 Políticas y procedimientos de transferencia de información	Aplica	Requisito de la política de seguridad para la transferencia de a información
A.13.2.2 Acuerdos sobre transferencia de información	Aplica	
A.13.2.3 Mensajería Electrónica	Aplica	
A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Aplica	Aplicar controles para mantener la confidencialidad, integridad y disponibilidad de la información en el envio y recepción de correos electrónicos.
A.14 Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Aplica	Se debe incluir requisitos de seguridad en la especificación de condiciones para los sistemas de información
A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas	Aplica	Requisitos y controles para la utilización de redes públicas para el envio de información y utilización de servicios
A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	Aplica	Se debe proteger las transacciones de los servicios de las aplicaciones.
A.14.2 Seguridad en los procesos de Desarrollo y de Soporte		
A.14.2.1 Política de desarrollo seguro	Aplica	Aplicar políticas para el desarrollo seguro de aplicaciones
A.14.2.2 Procedimientos de control de cambios en sistemas	Aplica	Se debe monitorear y revisar las actualizaciones y cambios realizados en los sistemas y servicios
A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Aplica	
A.14.2.4 Restricciones en los cambios a los paquetes de software	Aplica	
A.14.2.5 Principio de Construcción de	Aplica	Se debe documentar

los Sistemas Seguros		procedimientos de implementar medidas en las técnicas de desarrollo seguro
A.14.2.6 Ambiente de desarrollo seguro	Aplica	
A.14.2.7 Desarrollo contratado externamente	Aplica	Se debe controlar y supervisar el desarrollo contratado por terceros.
A.14.2.8 Pruebas de seguridad de sistemas	Aplica	Requisitos para las pruebas de seguridad y aceptación de sistemas en ambientes de prueba
A.14.2.9 Prueba de aceptación de sistemas	Aplica	
A.14.3 Datos de prueba		
A.14.3.1 Protección de datos de prueba	Aplica	Utilización de datos no reales para pruebas
A.15 Relación con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	Aplica	Aplicar condiciones para el correcto manejo de la información de la empresa con los proveedores
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Aplica	Convenio entre las partes para los acuerdos de seguridad de la información
A.15.1.3 Cadena de suministro de tecnología de información y comunicación	Aplica	Existe cadena de suministro con los proveedores.
A.15.2 Gestión de la prestación de servicios de proveedores		
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	Aplica	Control para aplicar mecanismos de monitoreo de los servicios prestados por los proveedores y las actualizaciones o cambios de los servicios
A.15.2.2 Gestión del cambio en los servicios de los proveedores	Aplica	
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
A.16.1.1 Responsabilidades y procedimientos	Aplica	Requisito de la política de seguridad sobre los procesos de gestión de incidentes de seguridad
A.16.1.2 Reporte de eventos de seguridad de la información	Aplica	Control de aplicación de canales de

		comunicación para el reporte de eventos e incidentes
A.16.1.3 Reporte de debilidades de seguridad de la información	Aplica	Los reportes deben indicar las debilidades y fallas de los sistemas y servicios detectados.
A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Aplica	Los incidentes y eventos detectados deben ser evaluados, clasificados y tomar decisiones para determinar las soluciones y aprendizajes para futuros casos.
A.16.1.5 Respuesta a incidentes de seguridad de la información	Aplica	
A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Aplica	
A.16.1.7 Recolección de evidencia	Aplica	Recuperar las evidencias para determinar los causantes y las acciones legales y sanciones.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1 Continuidad de Seguridad de la información		
A.17.1.1 Planificación de la continuidad de la seguridad de la información	Aplica	Determinar la aplicación de etapas como la planeación, implementación y verificación de la continuidad de la seguridad para dar respuesta ante las amenazas que la empresa puede sufrir.
A.17.1.2 Implementación de la continuidad de la seguridad de la información	Aplica	
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	
A.17.2 Redundancias		
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Aplica	Requisito de la política de seguridad para identificar los activos que requieran de ser dotados de redundancia según la exigencia de los procesos involucrados.
A.18 Cumplimiento		
A.18.1 Cumplimiento de requisitos legales y contractuales		
A.18.1.1 Identificación de la legislación aplicable	Aplica	Se debe identificar la documentación legal que afecten a la

		empresa en relación a la seguridad.
A.18.1.2 Derechos propiedad intelectual	Aplica	Establecer parámetros que garanticen el uso legal de software y sistemas
A.18.1.3 Protección de registros	Aplica	Control para aplicar protección de los registros en caso de pérdida, falsificación y acceso no autorizado
A.18.1.4 Privacidad y protección de información de datos personales	Aplica	Control en legislación vigente con respecto a privacidad y protección de datos personal
A.18.1.5 Reglamentación de controles criptográficos.	Aplica	Control para aplicar controles criptográficos actuales
A.18.2 Revisiones de seguridad de la información		
A.18.2.1 Revisión independiente de la seguridad de la información	Aplica	Requisito para gestionar auditorías externas de la seguridad de la información en la empresa
A.18.2.2 Cumplimiento con las políticas y normas de seguridad	Aplica	Requisito para aplicar controles para la revisión del cumplimiento de las políticas y normas de seguridad
A.18.2.3 Revisión del cumplimiento técnico	Aplica	

	Nombres y Apellidos	**Cargo**	**Fecha**	**Firma**
Elaborado				
Revisado				
Aprobado				