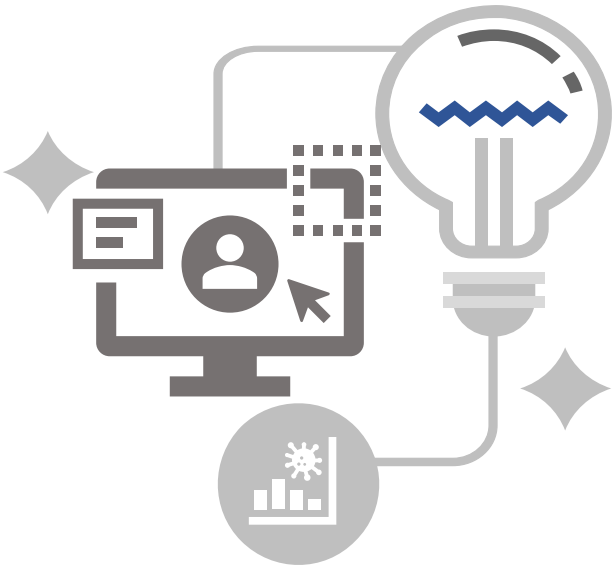

Plan Director para la Implementación del Sistema de Gestión de Seguridad de la Información

Nombre Estudiante: Carol Sthefanny Hernández Ladino

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (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: 28 diciembre 2020

Universitat Oberta de Catalunya

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Copyright © 2020 Carol Sthefanny Hernández Ladino.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

© Carol Sthefanny Hernández Ladino
Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Plan Director para la Implementación del Sistema de Gestión de Seguridad de la Información*
Nombre del autor:	*Carol Sthefanny Hernández Ladino*
Nombre del consultor/a:	*Antonio José Segovia Henares*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	12/2020
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*SGSI, Seguridad, ISO27001*

Resumen del Trabajo:

Teniendo en cuenta la importancia de los requisitos de seguridad de la información en el desarrollo del plan estratégico de la empresa, se hace necesario implementar un Sistema de Gestión de Seguridad de la información basado en la gestión de riesgos con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y los sistemas que la almacenan, transmiten y procesan. Con este fin, se define el Plan Director para la Implementación del Sistema de Gestión de Seguridad de la Información de la empresa a través se realiza un análisis que permita identificar el estado actual de seguridad de la información para así identificar las brechas actuales y definir planes de acción que den cierre a las mismas. Una vez ejecutado el Plan Director, la empresa contará con un SGSI que permita identificar y mitigar los riesgos a los cuales se expone la información para así minimizar costos operativos y financieros, así como, dar cumplimientos a los requerimientos legales, contractuales y regulatorios vigentes.

Abstract:

Considering the importance of information security requirements in the development of the strategic plan of the company, it is necessary to implement an Information Security Management System based on risk management in order to preserve confidentiality, integrity and availability of information and the systems that store, transmit and process it. For this purpose, the Master Plan for the Implementation of the Information Security

Management System of the company is defined through an analysis that allows identifying the current state of information security in order to identify current gaps and define action planes that give closure to them. Once the Master Plan has been executed, the company will have an ISMS that allows it to identify and mitigate the risks to which the information is exposed to minimize operating and financial costs, as well as to comply with the legal, contractual and regulatory requirements in force.

Índice

Lista de figuras

Lista de Tablas

1. Introducción

1.1. Contexto y justificación del Trabajo

Hoy en día los requerimientos de seguridad de la información cobran gran importancia debido al elevado número de amenazas que surgen como parte de la constante evolución tecnológica que se está viviendo actualmente, es por esto que, implementar un Sistema de Gestión de Seguridad de la Información (SGSI) se convierte en un componente indispensable en la conducción y consecución de los objetivos estratégicos definidos por la empresa.

Actualmente la empresa de contact center cuenta con más de 1.800 empleados que atienden solicitudes de clientes y su operación se rige por 5 procesos de negocio, distribuidos de la siguiente manera:

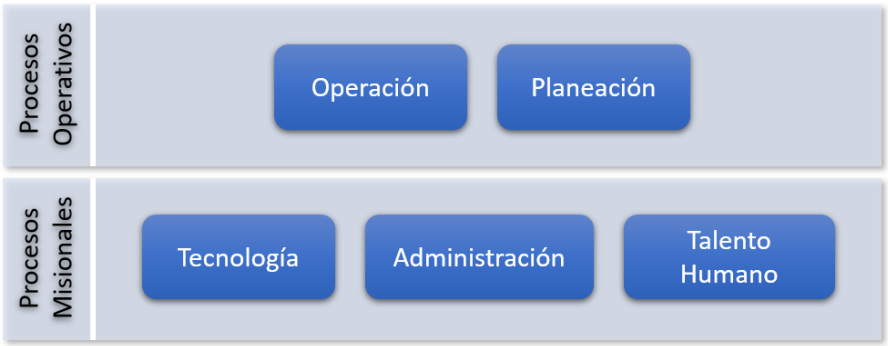

Figura 1 *Mapa de Procesos*

1. **Operación:** Responsable de gestionar la atención del Contact Center, para atender todas las solicitudes asociadas a los servicios de: Telefonía fija y móvil, Televisión por cable y fibra óptica. Su gestión se enfoca en siete líneas de servicio las cuales se encargan de la atención a clientes, soporte técnico y despliegue de campañas. Las líneas de servicio actuales son:

Figura 2 *Líneas de servicio*

2. ***Planeación:*** *Responsable de la centralización y comunicación de los indicadores de la organización.*

3. **Tecnología:** Responsable de gestionar todos los requerimientos de tecnología de información y comunicaciones.
4. **Administración:** Responsable de la gestión administrativa, en la cual atienden temas legales, seguridad física, mantenimientos locativos, entre otros.

5. **Talento Humano:** Responsable de la administración del talento humano para el desarrollo, coordinación, control y promoción del desempeño eficiente del personal.

Su operación se encuentra centralizada en la sede administrativa ubicada en Bogotá y se cuenta con una única sede. A continuación, se muestra el diagrama de red de la infraestructura tecnológica:

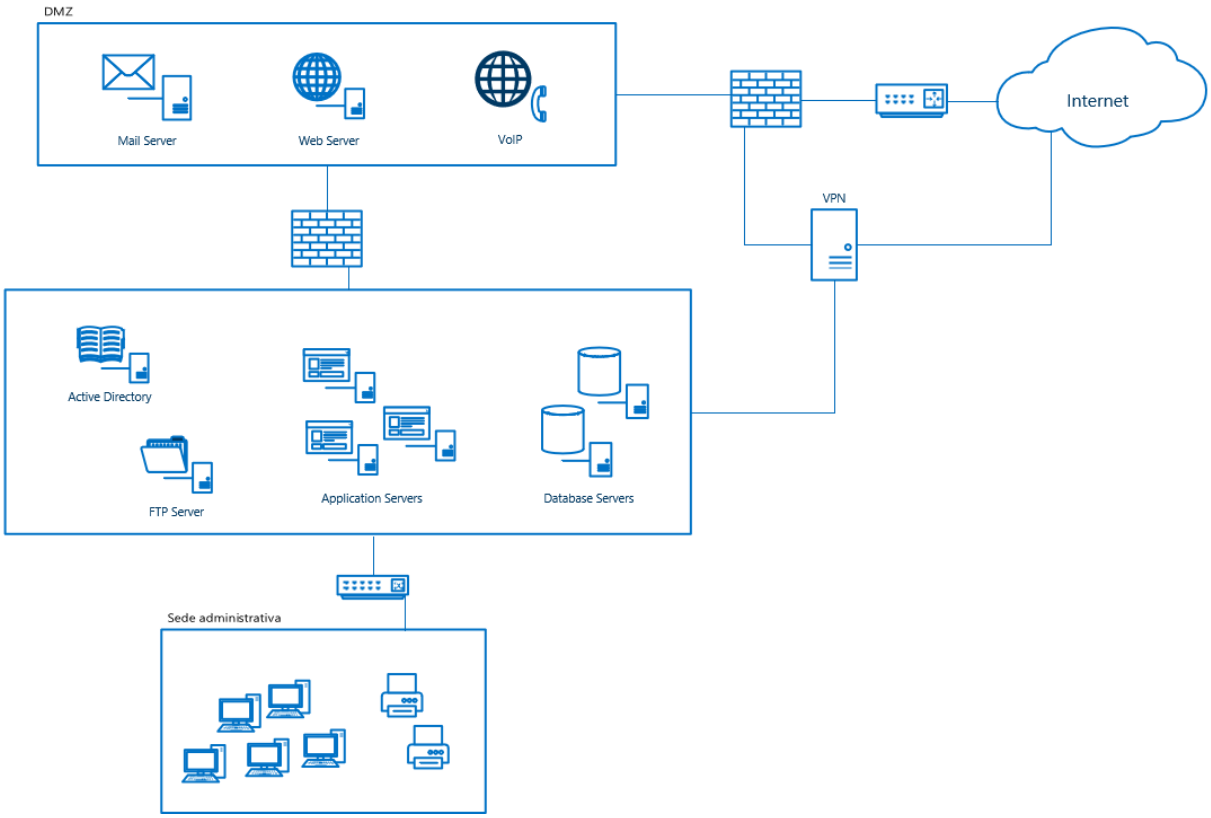

Figura 3 *Diagrama de red*

De acuerdo con la criticidad de la información que es manejada en el proceso de Operación para las líneas de servicio de ventas y retención y teniendo en cuenta las necesidades y expectativas de empleados, clientes, accionistas, proveedores y demás partes interesadas surge la necesidad de proteger los activos de información mediante el adecuado tratamiento de los posibles riesgos de tal forma que se mitiguen los impactos derivados de la materialización de los mismos, para así ofrecer un marco de confianza en el ejercicio de los deberes propios de la empresa.

Así mismo, se identifica la necesidad de integrar la seguridad de la información en los procesos de negocio para así preservar la confidencialidad, integridad y disponibilidad de la información y sistemas que la almacenan, transmiten o procesan mediante la implantación de medidas y controles acordes a la operación y criticidad.

Por lo anterior y entendiendo la importancia de una adecuada gestión de la información, se hace necesario implementar un SGSI que permita identificar y mitigar los riesgos a los cuales se expone la información para así minimizar costos operativos y financieros, así como, dar cumplimientos a los requerimientos legales, contractuales y regulatorios vigentes.

1.2. Alcance del SGSI

El alcance del SGSI ha sido definido en términos de procesos de negocio y de acuerdo con la relevancia de los mismos en la operación de la empresa, es por esto que, el SGSI abarca el proceso de Operación para sus dos líneas de servicios: Ventas y Retención, contemplando los sistemas de información y demás activos que soportan la operación del mismo. De igual forma, se da alcance a la sede administrativa desde la cual son ejecutadas las actividades del proceso.

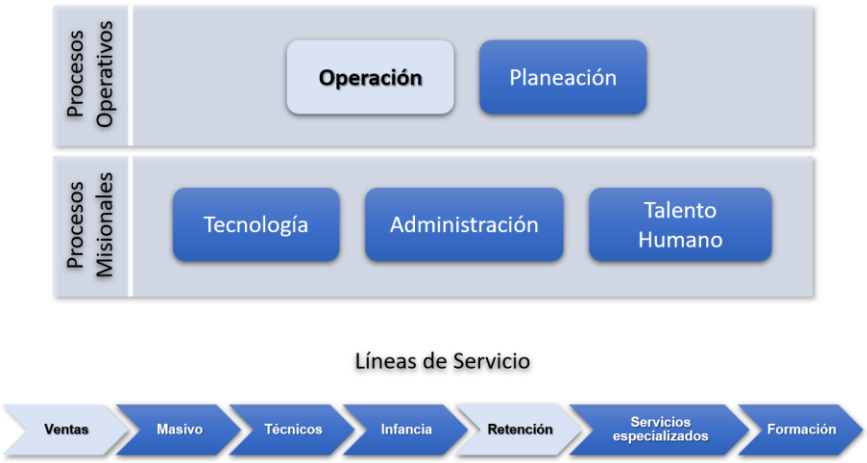

Figura 4 Alcance del SGSI

1.3. Objetivos

Teniendo en cuenta la importancia de proteger la información y así minimizar los impactos derivados de la materialización de riesgos que afecten la integridad, confidencialidad y disponibilidad de la misma y de acuerdo con las expectativas y necesidades de las diferentes partes interesadas, se plantean los siguientes objetivos respecto a seguridad de la información:

- Implementar un modelo Zero Trust en la red entrante VPN que asegure el acceso de cada usuario tanto a las aplicaciones como a la infraestructura tecnológica de la empresa.
- Separar las redes de bases de datos, servidores, impresoras y usuarios con el fin de mejorar la postura de seguridad de la empresa.
- Implementar un modelo cloud que asegure alta disponibilidad de los servicios y aplicaciones que han sido identificados como críticos para así asegurar la continuidad de la plataforma tecnológica.

1.4. Enfoque y método seguido

Implementar el Sistema de Gestión de Seguridad de la Información de la empresa requiere de la dedicación y asignación de esfuerzos para así alcanzar el objetivo propuesto. Actualmente la empresa ha asignado la responsabilidad de seguridad de la información a personas del proceso de Tecnología, sin embargo, esta no es la única responsabilidad que tienen asignada dichas personas, por lo cual se han tenido avances parciales en cuento a la gestión de seguridad de la información.

Así las cosas y reconociendo el esfuerzo realizado, se tomará como insumo la documentación y lineamientos implementados hasta el momento para dar continuidad a la implementación del SGSI de acuerdo con el Plan Director definido, ya que descartar dichos avances significaría una dedicación mayor y una ampliación significativa del plazo en el cual se estima finalizar la implementación.

1.5. Planificación del Trabajo

La implementación del Sistema de Seguridad de la Información se basa en la norma ISO/IEC 27001:2013 y se articulará mediante un proceso de gestión de riesgos que contempla las necesidades de la empresa y partes interesadas.

Con el fin de lograr la correcta implementación del Sistema, se han definido 6 fases como parte del Plan Director, durante las cuales se trabajarán los componentes fundamentales del SGSI:

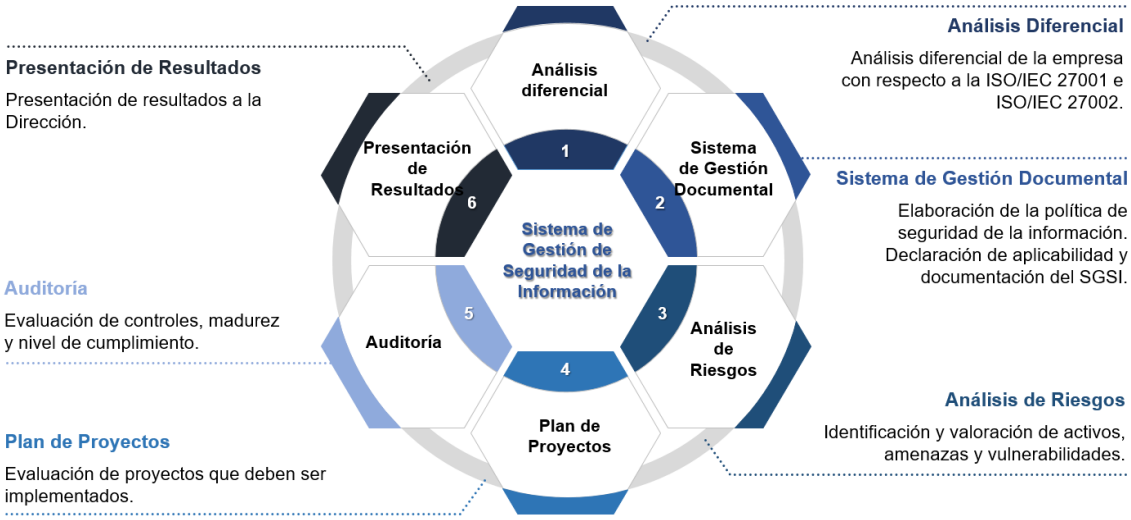

Figura 5 *Fases del Plan Director*

De acuerdo con las fases definidas se realizó la siguiente planeación para dar cumplimiento a los objetivos planteados para cada fase:

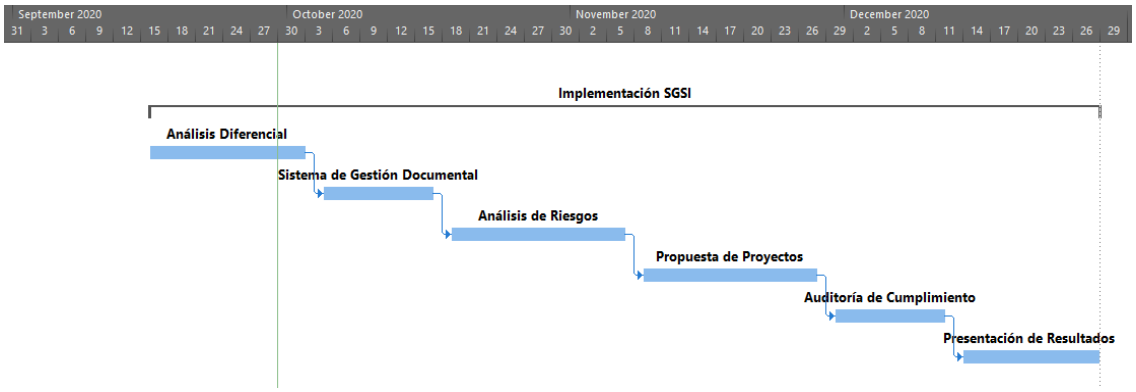

Figura 6 *Diagrama Gantt*

Así las cosas, los hitos esperados de acuerdo con cada una de las fases planteadas son:

Hito Fase 1: Evaluación del estado actual de seguridad de la información en la empresa respecto a la norma ISO/IEC 27001:2013.

Hito Fase 2: Política de Seguridad de la Información, Políticas y procedimientos referentes al Sistema de Gestión de Continuidad de Negocio de acuerdo con la declaración de aplicabilidad.

Hito Fase 3: Evaluación del impacto derivado de la materialización de las amenazas a las cuales pueden estar expuestos los activos de información relevantes para la empresa.

Hito Fase 4: Evaluación de los proyectos que deben ser implementados para lograr el estado de madurez de seguridad de la información deseado.

Hito Fase 5: Evaluación de los controles que permita determinar el nivel de cumplimiento para así definir las acciones de mejora que deben ser implementadas.

Hito Fase 6: Presentación de resultados a la Alta Dirección con el fin de obtener el apoyo para así lograr la implementación de las acciones de mejora que den cierre a las brechas identificadas para lograr el nivel de madurez objetivo.

De acuerdo con los hitos definidos como parte del Plan Director para la Implementación del Sistema de Gestión de Seguridad de la Información se requiere tener acceso a la información referente a seguridad de la información que se tiene hasta el momento, así como, el plan estratégico definido. Por otra parte, se requiere del apoyo de la Alta Dirección para asignar los recursos financieros, personas y aprobar la implementación de los proyectos definidos para alcanzar el nivel objetivo de seguridad de la información.

1.6. Sumario de productos obtenidos

En línea con los objetivos planteados como parte del Plan Director para la Implementación del Sistema de Gestión de Seguridad de la Información de la empresa se han identificado los siguientes productos:

- **Evaluación del estado actual:** Describe el estado el estado actual de seguridad de la información en el cual se encuentra la empresa respecto a la norma ISO/IEC 27001 y el estándar ISO/IEC 27002, el cual permitirá establecer las acciones que deben ser implementadas para alcanzar el nivel objetivo de seguridad.

- **Política de Seguridad de la Información:** Establece los principales lineamientos en materia de seguridad de la información que deben ser cumplidos por los empleados, directivos y proveedores.

- **Declaración de aplicabilidad:** Define los controles de seguridad de la información que deben ser aplicados de acuerdo con el alcance definido para el SGSI y el estándar ISO/IEC 27002.

- **Documentación del SGSI:** Incluye los documentos requeridos para la implementación del Sistema de Gestión de Seguridad de la Información, dentro de los cuales se contemplan: Estructura de Gobierno de Seguridad de la Información, Metodología de análisis de riesgos, Procedimiento de revisión por la Dirección, Procedimiento de auditorías internas e Indicadores de seguridad de la información.

- **Matriz de Riesgos de Seguridad de la Información:** Contiene los activos de información con su respectiva valoración para determinar su relevancia en la empresa. Así mismo, contiene las amenazas y vulnerabilidades con su respectiva valoración de impacto que permita determinar el nivel de riesgo.

- **Plan de proyectos:** Describe los proyectos que deben ser implementados con el fin de dar cierre a las brechas identificadas respecto al estado actual de seguridad de la información en la empresa.

- **Evaluación de la madurez:** Describe el nivel de cumplimiento respecto a los controles definidos en el estándar ISO/IEC 27002 que son aplicables a la empresa.

- **Presentación de resultados:** Contiene el resumen ejecutivo del análisis y resultados obtenidos de la ejecución de cada una de las fases planteadas como parte del Plan Director.

1.7. Descripción de los demás capítulos de la memoria

Con el fin de implementar el SGSI, inicialmente se realizará un análisis que permita determinar la situación actual respecto a seguridad de la información, los resultados de este análisis se describen en el capítulo 2 de este documento. Por otra parte, entendiendo los requerimientos documentales planteados en la norma ISO/IEC 27001 se define el esquema documental del SGSI el cual se detalla en el capítulo 3. Como resultado de las dos fases anteriores, se identifican los proyectos que deben ser implementados para lograr dar cierre a las brechas identificadas y lograr la correcta implementación del SGSI, la descripción y detalle de los proyectos propuestos se encuentra en el capítulo 4 de este documento.

Teniendo en cuenta que en el estándar ISO/IEC 27002 se definen 114 controles que deben ser implementados, por lo cual se hace necesario realizar una evaluación que determine el nivel de cumplimiento respecto a dichos controles, los resultados de la evaluación realizada se encuentran en el capítulo 5.

2. Evaluación del estado actual de seguridad de la información

A lo largo del tiempo, la empresa se ha esforzado por definir requisitos de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de la información, por lo cual se han realizado definiciones y se han implementado procedimiento en aras de alcanzar dicho objetivo. Actualmente se está trabajando para lograr la implementación del Sistema de Gestión de Seguridad de la Información, por lo cual es de suma importancia poder identificar el estado actual respecto a la norma ISO/IEC 27001 y el estándar ISO/IEC 27002.

2.1. Análisis diferencial ISO/IEC 27001

Con el fin de determinar el estado actual de seguridad de la información en la empresa para así poder establecer claramente el punto de partida, se realizó un análisis diferencial frente a los requisitos que establece la norma. Para cada uno de los requisitos se realizó un análisis detallado respecto a definiciones, documentación, implementación y operación de procedimientos acordes a lo requerido y se asignó un porcentaje de cumplimiento.

En nivel de cumplimiento de cada uno de los requisitos se determina a partir de la siguiente escala:

Rango	Descripción
0% - 50%	No se ha implementado el requisito o se ha trabajo en definiciones iniciales, sin embargo, aún no son formales.
51% - 89%	Implementación parcial del requisito.
90% - 100%	Se da cumplimiento a los requisitos planteados.

Tabla 1 *Escalas de nivel de cumplimiento*

Resultados obtenidos:

De acuerdo con los resultados obtenidos, se pueden identificar los aspectos en los cuales se deben centrar los esfuerzos con el fin de lograr la correcta implementación del SGSI, a continuación, se muestra la gráfica donde se establece el estado actual para cada uno de los requisitos:

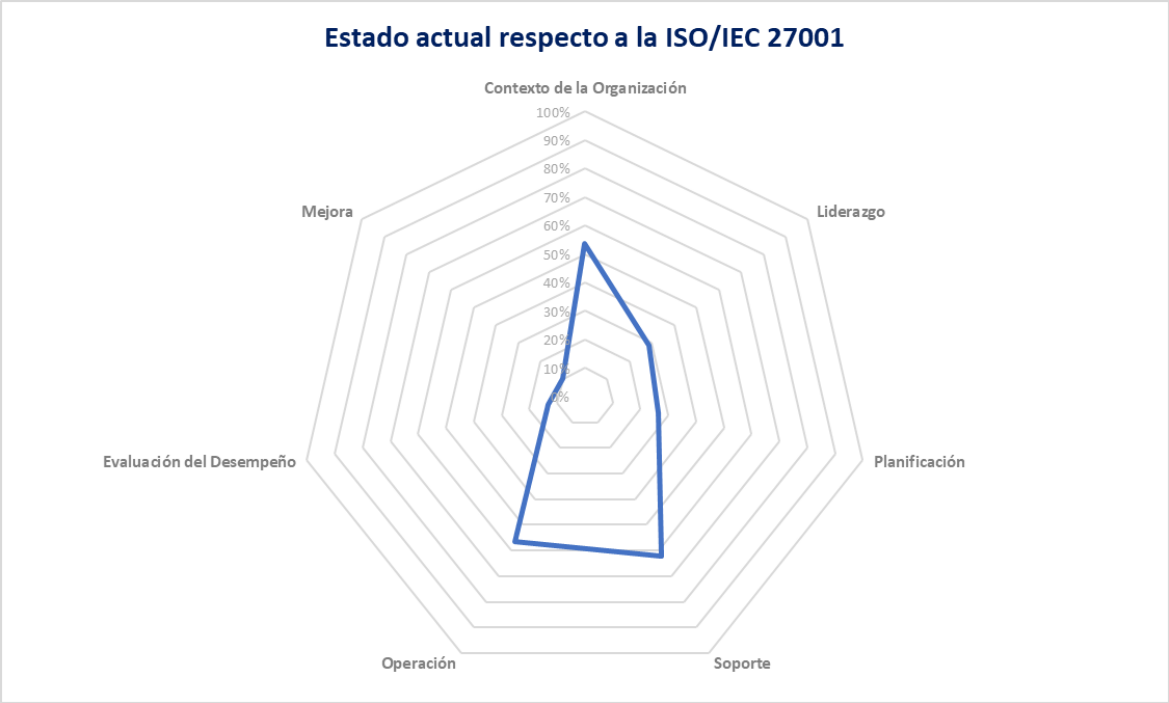

Figura 7 *Estado actual ISO/IEC 27001*

Los resultados detallados del análisis realizado se describen en el Anexo 1. Análisis Diferencial.

2.2. Análisis diferencial ISO/IEC 27002

Al igual que en el análisis diferencial de la norma ISO/IEC 27001, se realizó un análisis respecto a las definiciones, implementación y operación de los controles establecidos en el estándar ISO/IEC 27002. Es importante aclarar que dicho análisis no establece el nivel de cumplimiento de los controles, el análisis se realizó con el fin de conocer el estado actual para así poder identificar los puntos en los cuales se deben centrar los esfuerzos.

Para determinar el nivel de cumplimiento se contemplaron las mismas escalas relacionadas en la *Tabla 1 Escalas de nivel de cumplimiento*, las cuales fueron utilizadas para el análisis diferencial ISO/IEC 27001.

Resultados obtenidos:

A continuación, se muestran los resultados obtenidos de acuerdo con cada uno de los dominios de control establecidos en el estándar:

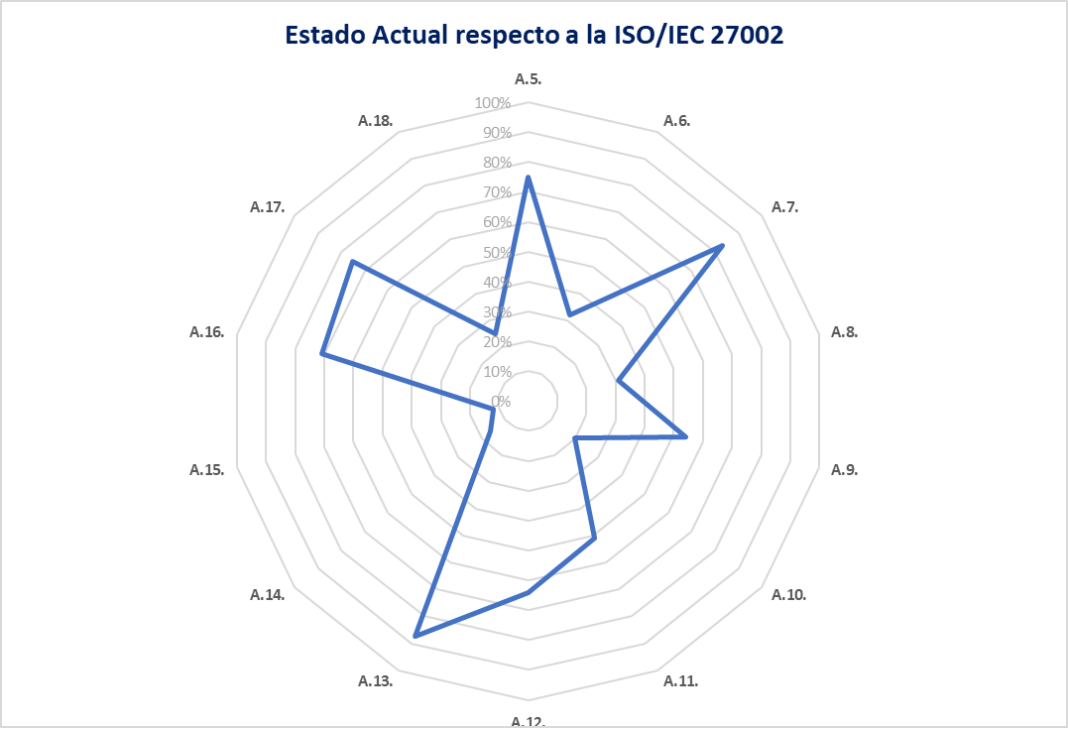

Figura 8 *Estado actual ISO/IEC 27002*

Los resultados detallados del análisis realizado se describen en el Anexo 1. Análisis Diferencial. La evaluación de cumplimiento de los controles se realizará como parte de las actividades definidas para la Fase 5 de este Plan.

3. Esquema documental del Sistema de Gestión de Seguridad de la Información

3.1. Política de Seguridad de la Información

Para la empresa es de vital importancia contar con un entorno seguro en el que pueda desarrollar sus actividades, razón por la cual asume la seguridad de la información como una responsabilidad asociada a la protección contra amenazas que puedan afectar la integridad, disponibilidad y confidencialidad, incluyendo también a las personas, instalaciones, sistemas y tecnología sobre la que se soporta y procesa dicha información, velando especialmente por el cumplimiento normativo, la preservación de la buena imagen y sostenibilidad de la empresa.

Es por esto que, la empresa adopta un Sistema de Gestión de Seguridad de la Información como la herramienta que permita identificar y minimizar los riesgos a los cuales se expone la información, reducir costos operativos y financieros, establecer la cultura de seguridad de la información y asegurar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Teniendo en cuenta lo anterior, tanto empleados como proveedores o terceros, que acceden interna o externamente a cualquier activo de información son responsables de su protección, por lo cual utilizarán los recursos que la empresa pone a su disposición siguiendo los lineamientos establecidos y velando por la correcto funcionamiento de los controles de seguridad implementados, así mismo, notificarán cualquier situación que detecten que pueda suponer un riesgo para la empresa o personas que la integran siguiendo los procedimientos definidos para tal fin, de esta forma, se dará cumplimiento a lo establecido en esta política.

La Alta Dirección es responsable de impulsar el desarrollo e implementación de la política, así como, de velar por el cumplimiento, divulgación y revisión periódica de la misma.

El incumplimiento de esta política podría derivar en un proceso disciplinario, civil o penal a que haya lugar, según los dispuesto en el Reglamento Interno de Trabajo y demás leyes y normativa vigentes.

3.2. Procedimiento de Auditorías Internas

Teniendo en cuenta que uno de los aspectos de gran importancia para asegurar la mejora continua del Sistema de Gestión de Seguridad de la Información es la revisión periódica para determinar el nivel de cumplimiento frente a los lineamientos, procedimientos y controles de seguridad de la información que la empresa decidió implementar, se hace necesario realizar auditorías internas que permitan identificar oportunidades de mejora, para así trabajar en la implementación de acciones de mejora y de esta forma mantener la certificación ISO 27001 para la empresa.

Para garantizar la consecución de los objetivos de la función de auditoría, es fundamental desarrollar un procedimiento de auditoría interna alineada a los requisitos de seguridad de la información definidos por la empresa. Como parte del procedimiento de auditoría interna se han definido tres fases fundamentales:

1. Definición del programa de auditoría
2. Ejecución del programa de auditoria
3. Seguimiento de la auditoría

3.2.1. Definición del programa de auditoría

De acuerdo con las necesidades identificadas respecto a seguridad de la información, así como, los resultados de las auditorías anteriores, anualmente se debe definir el programa de auditoría para el SGSI el cual debe contemplar:

- Objetivos del programa de auditoría
- Alcance del programa de auditoría
- Objetivos de cada una de las auditorías a realizar
- Alcance de cada una de las auditorías a realizar
- Métodos de auditoría
- Criterios de evaluación
- Cronograma

Una vez definidos los aspectos base del programa de auditoría, se debe definir el equipo de auditoría que ejecutará el programa garantizando que los auditores cuentan con las competencias requeridas en relación con los objetivos definidos para cada auditoría. Teniendo en cuenta que las auditorías relacionadas con el SGSI pueden requerir de conocimientos específicos, se hace necesario que los auditores responsables cuenten con las siguientes competencias:

- Conocer la norma ISO/IEC 27001 y el estándar ISO/IEC27002.
- Entender los fundamentos y conceptos generales de la gestión de seguridad de la información.
- Entender conceptos generales acerca del funcionamiento de sistemas de información e implementación de controles de seguridad de la información.

- Conocer el proceso de certificación ISO 27001 para empresas.

Así mismo, es necesario que cuente con la siguiente formación académica de acuerdo con las funciones a desempeñar:

- Ingeniero de sistemas, electrónica, telecomunicaciones o a fines.
- Especialización o maestría en seguridad de la información, seguridad informática y/o auditoría de sistemas de información.
- Certificación auditor interno o líder ISO27001:2013.

Con experiencia mínima de 2 años realizando auditorías al Sistema de Gestión de Seguridad de la Información, auditorías a los controles de seguridad de la información o auditorías a los Sistemas de Gestión. De acuerdo con las funciones a desempeñar, cada auditor debe ser: imparcial, honesto, diplomático, firme, discreto, ético, seguro de sí mismo, perceptivo, con alta capacidad de observación, con habilidades de comunicación y compromiso.

En caso de no contar con auditores con las competencias requeridas, será necesario considerar la ejecución de auditorías externas que permitan determinar el nivel de cumplimiento frente a los requisitos del SGSI.

De igual forma, se deben identificar los recursos financieros y humanos requeridos para la ejecución de la auditoría, para así asegurar que el programa podrá ser ejecutado acorde con la planeación realizada.

Por último, el programa de auditoría será socializado con el Comité de Auditoría con el fin de obtener su aprobación.

3.2.2. Ejecución del programa de auditoría

Con base en el cronograma definido, para iniciar cada auditoría se debe realizar una reunión de apertura con los responsables de atender la auditoría de acuerdo con los objetivos y alcance definidos. Como parte, de esta reunión se solicitará la documentación correspondiente para así realizar un análisis previo e identificar los aspectos claves que serán validados durante la revisión en campo. La fecha de la revisión en campo será acordada con el auditado, respectando la planeación realizada. Durante la revisión de campo se solicitarán las evidencias que permitan determinar el nivel de cumplimiento de los procedimientos o controles de seguridad de la información de acuerdo con el objetivo y alcance definido. Posteriormente, el equipo de auditor realizará un análisis detallado de las evidencias obtenidas y documentará las no conformidades y oportunidades de mejora identificadas.

Tanto las no conformidades como las oportunidades de mejora serán socializadas con el auditado en la reunión de cierre de la auditoría, una vez obtenida su aprobación se

documentará el informe final, sobre el cual el auditado deberá definir los planes de acción que den cierre a las brechas identificadas.

Los resultados de las auditorías realizadas serán socializados con el Comité de Seguridad.

El informe de auditoría será documentado siguiendo el modelo definido en el Anexo 2. Informe de Auditoría.

3.2.3. Seguimiento de la auditoría

Una vez definidos los planes de acción que den cierre a las no conformidades y oportunidades de mejora identificadas, se deberá realizar un seguimiento periódico basado en las fechas de cierre definidas por el auditado. En caso de identificar incumplimientos, estos deberán reportados al comité de seguridad para así tomar acciones que garanticen la implementación de los planes de acción definidos.

Paralelo al seguimiento de los planes de acción, se deberán realizar las demás auditorías definidas en el programa de auditoría.

3.2.4. Diagrama de flujo

A continuación, se muestra el diagrama de flujo para el procedimiento de auditorías internas del SGSI definido:

Fase 1: Definición del programa de auditoría

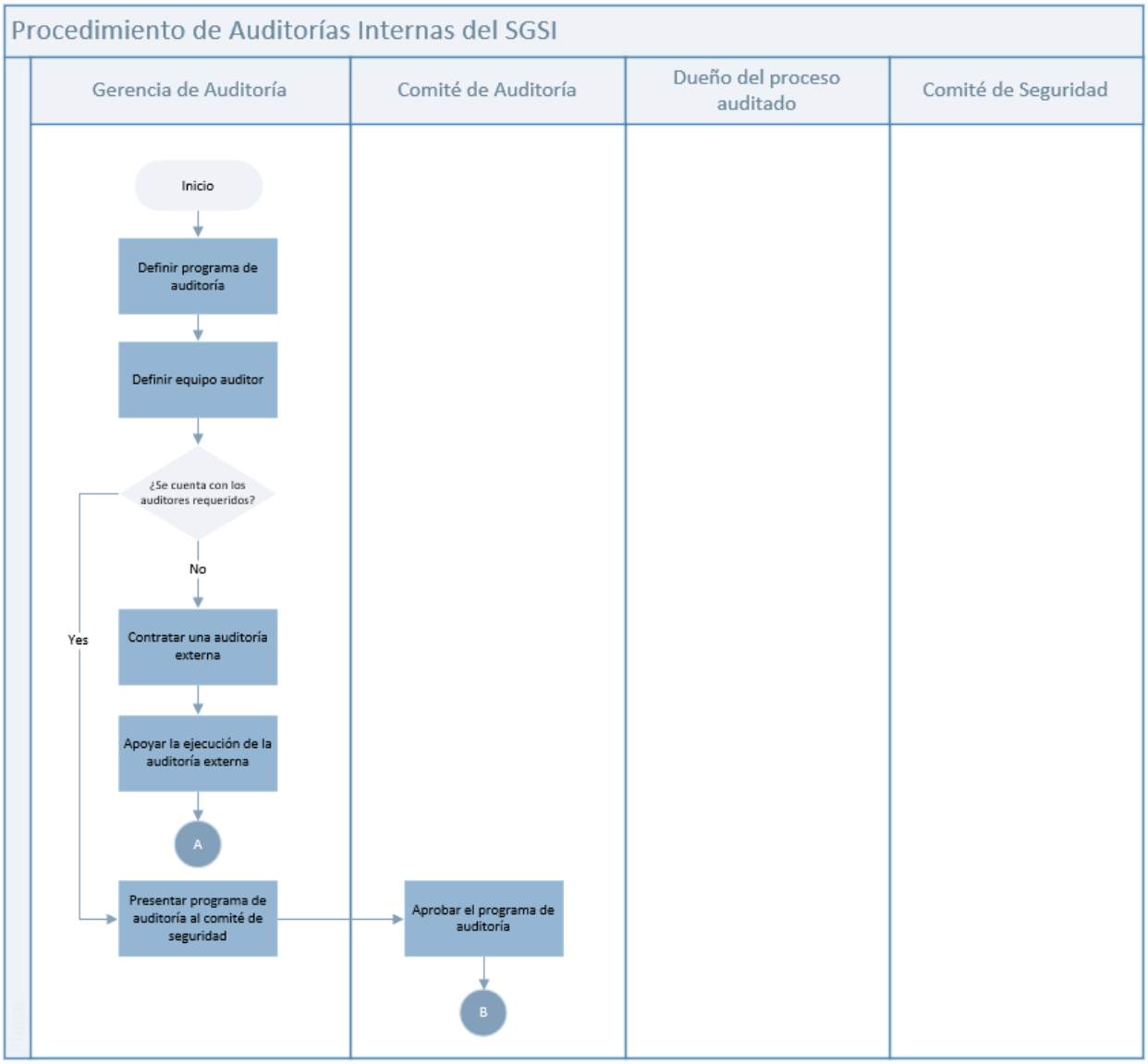

Figura 9 *Procedimiento auditorías internas SGSI – Fase 1*

Fase 2: Ejecución del programa de auditoría

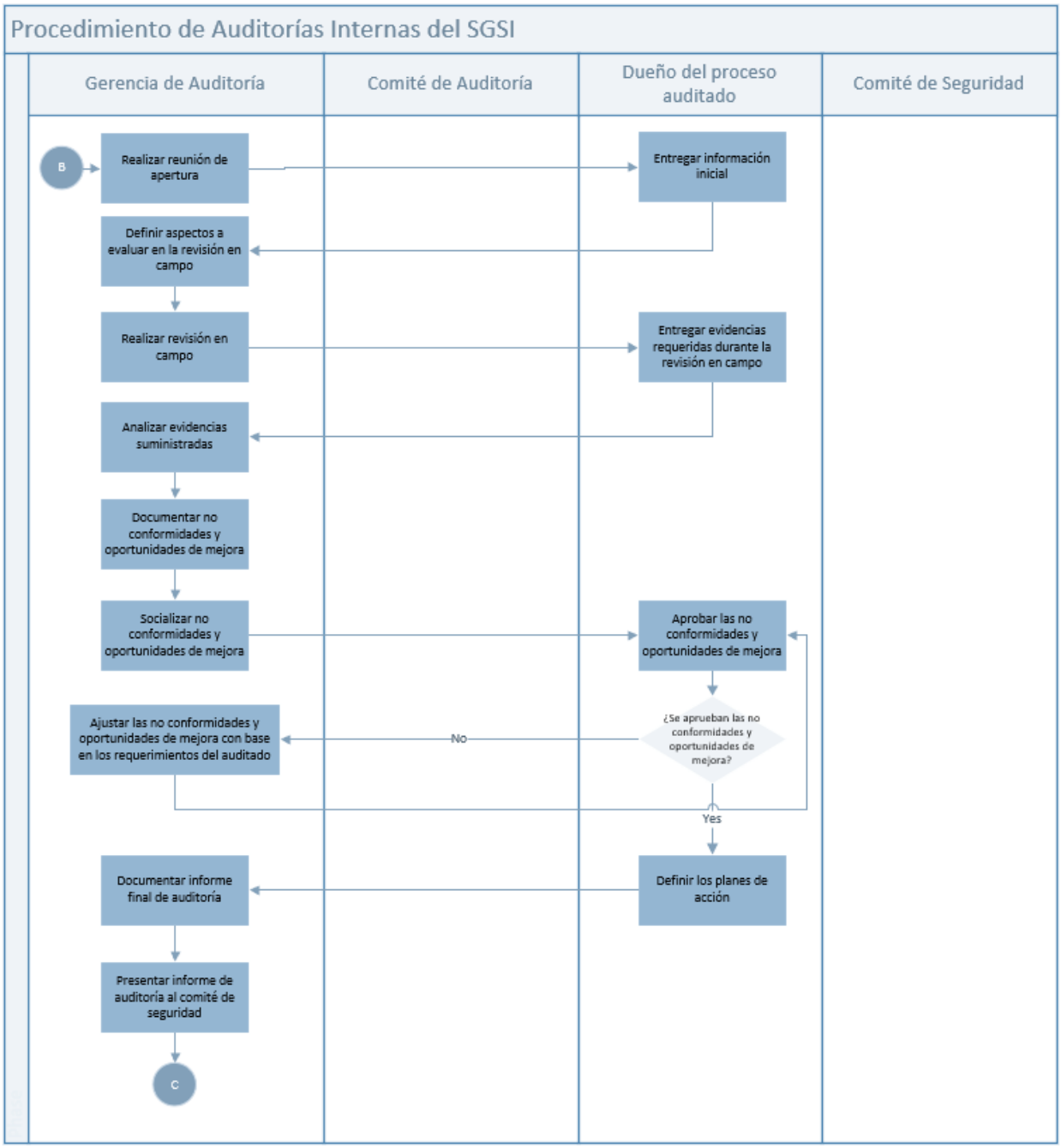

Figura 10 *Procedimiento auditorías internas SGSI – Fase 2*

Fase 3: Seguimiento de la auditoría

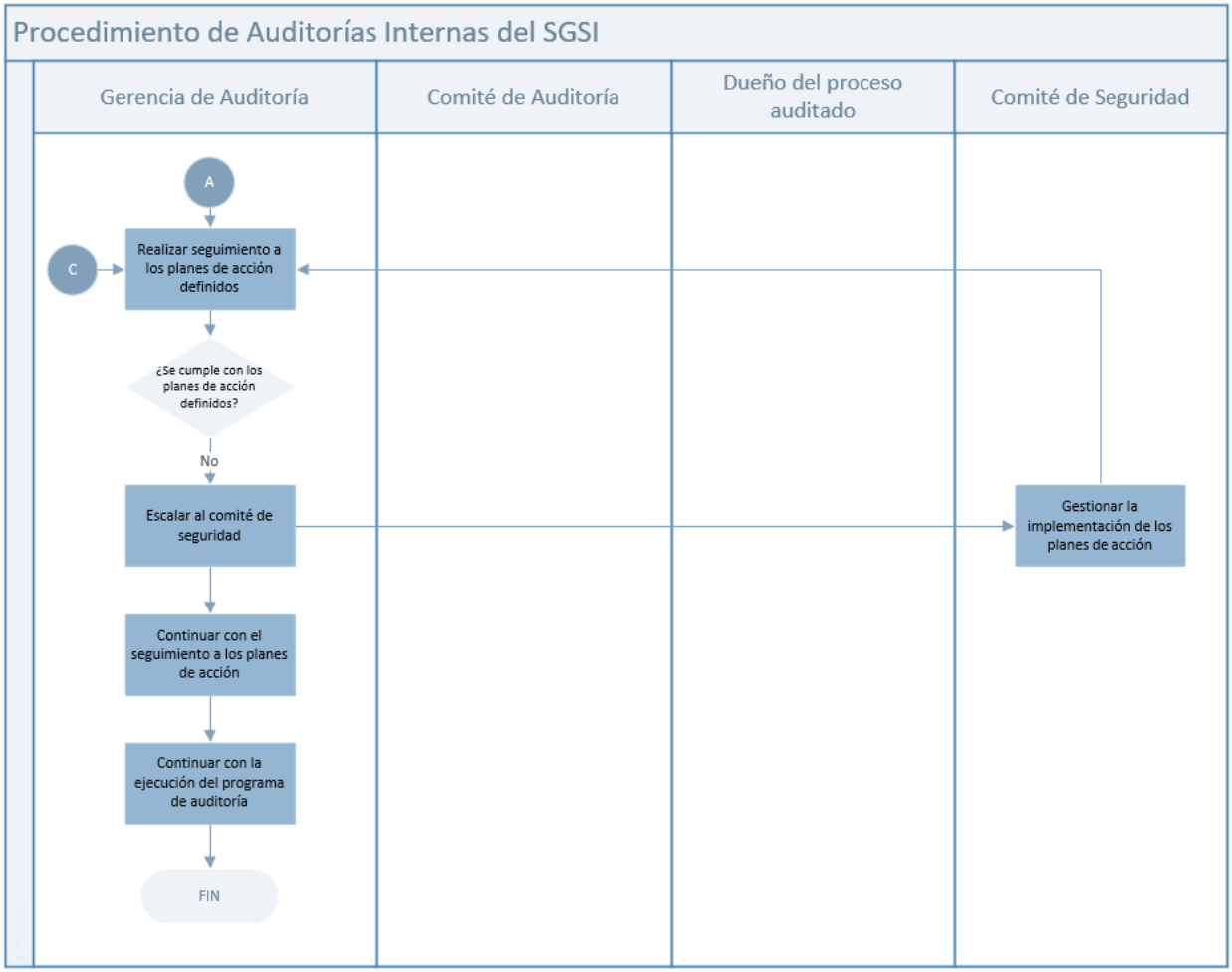

Figura 11 *Procedimiento auditorías internas SGSI – Fase 3*

3.2.5. Planeación de la auditoría

En el Anexo 3. Programación auditoría se muestra el cronograma definido para auditar y verificar el nivel de cumplimiento de cada uno de los controles especificados en el estándar ISO/IEC 27002, la planeación se realizó a tres años teniendo en cuenta que es el periodo durante el cual se mantiene la vigencia de la certificación ISO27001 para la empresa.

3.3. Gestión de Indicadores

La base principal para garantizar el correcto funcionamiento del SGSI es la mejora continua a través de una revisión periódica, tanto del estado de la documentación que da soporte al sistema, como de los controles y planes de acción correctivos definidos

ante posibles adversidades en el proceso, con este fin, se definen los criterios básicos para realizar la medición, análisis y evaluación del desempeño del SGSI:

Indicador 1:

NOMBRE DEL INDICADOR	Implementación de políticas
OBJETIVO DEL INDICADOR	Medir el nivel de implementación de las políticas de seguridad definidas a nivel estratégico por la empresa
TENDENCIA	Positiva
FORMULA	$\frac{No.políticas\ implementadas}{No.políticas\ definidas}\ x\ 100$
META SATISFACTORIA	95% - 100%
META SOBRESALIENTE	85% - 95%
META MÍNIMA	80%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Semestral

Indicador 2:

NOMBRE DEL INDICADOR	Ejecución del presupuesto de seguridad de la información
OBJETIVO DEL INDICADOR	Medir el nivel de cumplimiento en la ejecución anual del presupuesto asignado a seguridad de la información
TENDENCIA	Positiva
FORMULA	$\frac{Presupuesto\ ejecutado}{Presupuesto\ asignado}\ x\ 100$
META SATISFACTORIA	98% - 100%
META SOBRESALIENTE	91% - 97%
META MÍNIMA	90%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Trimestral

Indicador 3:

NOMBRE DEL INDICADOR	Monitoreo riesgos de seguridad de la información
OBJETIVO DEL INDICADOR	Monitorear los riesgos de seguridad de la Información para identificar aquellos que se encuentren por encima de los niveles de tolerancia aceptables
TENDENCIA	Negativa
FORMULA	$\frac{No.\,riesgos\ residuales\ fuera\ de\ los\ niveles\ de\ tolerancia\ aceptables}{No.\,total\ de\ riesgos\ identificados}\ x\ 100$
META SATISFACTORIA	0% - 5%
META SOBRESALIENTE	5% - 10%
META MÍNIMA	15%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Trimestral

Indicador 4:

NOMBRE DEL INDICADOR	Sensibilización y capacitación en seguridad de la información
OBJETIVO DEL INDICADOR	Medir el cumplimiento en la ejecución del programa de capacitación y sensibilización.
TENDENCIA	Positiva
FORMULA	$\frac{No.\,actividades\ ejecutadas\ en\ el\ periodo\ evaluado}{No.\,actividades\ planeadas\ en\ el\ periodo\ evaluado}\ x\ 100$
META SATISFACTORIA	95% - 100%
META SOBRESALIENTE	90% - 94%
META MÍNIMA	85%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Trimestral

Indicador 5:

NOMBRE DEL INDICADOR	Gestión de incidentes de seguridad de la información
OBJETIVO DEL INDICADOR	Medir la efectividad de la gestión de incidentes de seguridad de la información que afecten la confidencialidad, integridad o disponibilidad de la información
TENDENCIA	Positiva
FORMULA	$\left(\frac{No.\,eventos\,reportados\,que\,son\,incidentes}{No.\,total\,de\,eventos\,reportados} \; x \; \frac{No.\,eventos\,reportados\,que\,son\,incidentes}{No.\,total\,de\,incidentes\,materializados}\right) x\,100$
META SATISFACTORIA	90% - 100%
META SOBRESALIENTE	80% - 89%
META MÍNIMA	75%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Semestral

Indicador 6:

NOMBRE DEL INDICADOR	Gestión de vulnerabilidades
OBJETIVO DEL INDICADOR	Medir la gestión realizada sobre las vulnerabilidades identificadas.
TENDENCIA	Positiva
FORMULA	$\frac{No.\,vulnerabilidades\,cerradas}{No.\,vulnerabilidades\,identificadas}\,x\,100$
META SATISFACTORIA	95% - 100%
META SOBRESALIENTE	85% - 94%
META MÍNIMA	80%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Trimestral

Indicador 7:

NOMBRE DEL INDICADOR	Protección de los portales web
OBJETIVO DEL INDICADOR	Medir el grado de protección de los portales expuestos a Internet de la organización ante ataques web
TENDENCIA	Positiva
FORMULA	$\frac{No.\,ataques\ web\ bloqueados}{No.\,ataques\ identificados}\ x\ 100$
META SATISFACTORIA	100%
META SOBRESALIENTE	97% - 99%
META MÍNIMA	96%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Mensual

Indicador 8:

NOMBRE DEL INDICADOR	Protección antimalware
OBJETIVO DEL INDICADOR	Medir el grado de protección de los equipos de la organización ante ataques de malware
TENDENCIA	Positiva
FORMULA	$\frac{No.malware\ bloqueado}{No.malware\ identificado}\ x\ 100$
META SATISFACTORIA	100%
META SOBRESALIENTE	97% - 99%
META MÍNIMA	96%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Mensual

Indicador 9:

NOMBRE DEL INDICADOR	Protección contra phishing
OBJETIVO DEL INDICADOR	Medir el grado de protección ante campañas de phishing
TENDENCIA	Positiva
FORMULA	$\frac{No.\,campañas\,de\,phishing\,bloqueadas}{No.\,campañas\,de\,phishing\,identificadas}\ x\ 100$
META SATISFACTORIA	100%
META SOBRESALIENTE	97% - 99%
META MÍNIMA	96%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Trimestral

Indicador 10:

NOMBRE DEL INDICADOR	Protección contra phishing
OBJETIVO DEL INDICADOR	Medir el nivel de concientización de los empleados ante campañas de phishing
TENDENCIA	Negativa
FORMULA	$\frac{No.\,empleados\,victimas\,ante\,campañas\,de\,phishing}{No.\,total\,de\,empleados}\ x\ 100$
META SATISFACTORIA	0%
META SOBRESALIENTE	1% - 5%
META MÍNIMA	6%
UNIDAD DE MEDIDA	Porcentaje (%)
FRECUENCIA DE MEDICIÓN	Trimestral

La medición de cada uno de los indicadores la realizará el responsable del SGSI en la empresa de acuerdo con la periodicidad definida y apoyado en las evidencias entregadas por los responsables de la ejecución de cada uno de los controles.

3.4. Procedimiento de revisión de la Alta Dirección

En aras de asegurar la idoneidad, eficacia y mejora continua del sistema, se requiere que la Alta Dirección realice revisiones periódicas referentes a la gestión de seguridad de la información, para esto y como parte del compromiso adquirido por la Alta Dirección frente al desempeño del SGSI, se ha definido que semestralmente se realizará una revisión que contemple los siguientes aspectos:

- Resultados de las auditorías realizadas la SGSI dentro del periodo evaluado.
- Estado de implementación de los planes de acción definidos de acuerdo con las no conformidades y oportunidades de mejora identificadas durante las auditorías.
- Resultados del análisis de riesgos de seguridad de la información.
- Estado de implementación de los planes de tratamiento para mitigar los riesgos de seguridad de la información que fueron identificados fuera de los niveles tolerables.
- Estado de implementación de los planes de acción definidos con base en los resultados de revisiones previas realizadas por la Alta Dirección.
- Cambios en los procesos de negocio que impacten la gestión de seguridad de la información.
- Cumplimiento de los objetivos de seguridad de la información definidos.

Como resultado de la revisión realizada, se deberá generar un informe formal donde se indiquen las oportunidades de mejora identificadas respecto al desempeño del SGSI con los planes de acción correspondientes, así como, los responsables y fechas de ejecución.

Como parte de las revisiones, se requiere el apoyo de los responsables de auditoría y gestión de riesgos de seguridad de la información, quienes suministrarán la información necesaria para determinar el cumplimiento de los aspectos a evaluar. De igual forma, el Chief Information Security Officer (CISO) será el responsable de realizar seguimiento de los planes de acción definidos con base en os resultados de la revisión.

A continuación, se muestra el diagrama de flujo del procedimiento de revisión que debe realizar la Alta Dirección:

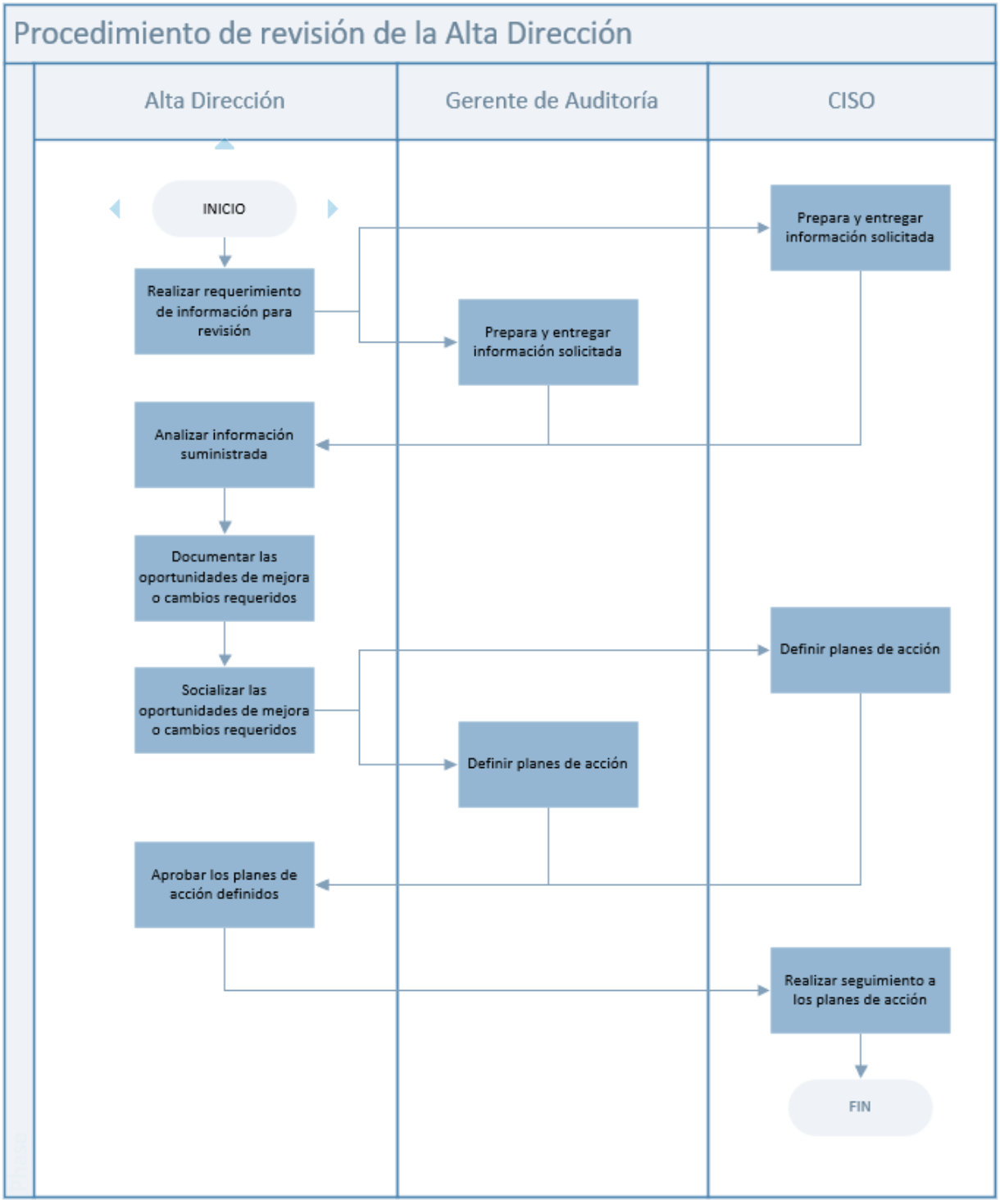

Figura 12 *Procedimiento de revisión de la Alta Dirección*

3.5. Gestión de roles y responsabilidades

Con el fin de lograr el desarrollo, implementación, gestión y mejora continua del Sistema de Gestión de Seguridad de la Información se definen los roles involucrados y sus principales responsabilidades. Así las cosas, se ha creado el Comité de Seguridad que será presidido por el Chief Information Security Officer (CISO) y tendrá la responsabilidad de garantizar y proporcionar el apoyo, recursos y estrategias de negocio necesarias para el correcto funcionamiento del SGSI.
Las principales responsabilidades del Comité de Seguridad, en relación con el SGSI son:

- Revisar y aprobar las políticas subyacentes de la Política de Seguridad de la información, como parte del Marco Normativo de Seguridad de la Información.
- Proporcionar los recursos necesarios para la planificación, implementación, revisión y mejora del SGSI.
- Establecer estrategias efectivas para el desarrollo, implementación, monitoreo y mejora del SGSI.
- Revisar y apoyar el desarrollo e implantación de las normas específicas de cada unidad de negocio, de modo que estén alineadas con el Marco Normativo de Seguridad de la Información y la Política de Seguridad de la Información.
- Supervisar el estado del SGSI.
- Revisar y aprobar los cambios que afecten a la implantación, operatividad, alcance y/o mantenimiento del SGSI.
- Informar los cambios estratégicos en el SGSI que puedan afectar a los objetivos de seguridad o negocio.
- Aprobar las excepciones de la Política de Seguridad de la Información.
- Comunicar la necesidad de cambio en el comportamiento organizacional y su importancia para el negocio.
- Proporcionar las herramientas necesarias para el desarrollo de materiales de formación en materia de seguridad de la información necesarios para comunicar la importancia de la protección de los activos de información.

3.5.1. Miembros del Comité de Seguridad

Teniendo en cuenta la estructura organizacional de la empresa, el Comité de Seguridad estará conformado por:

- Chief Information Security Officer (CISO)
- Chief Executive Officer (CEO)
- Oficial de Protección de Datos
- Director de Tecnología
- Director Administrativo y Financiero
- Director Jurídico
- Gerente de Auditoría

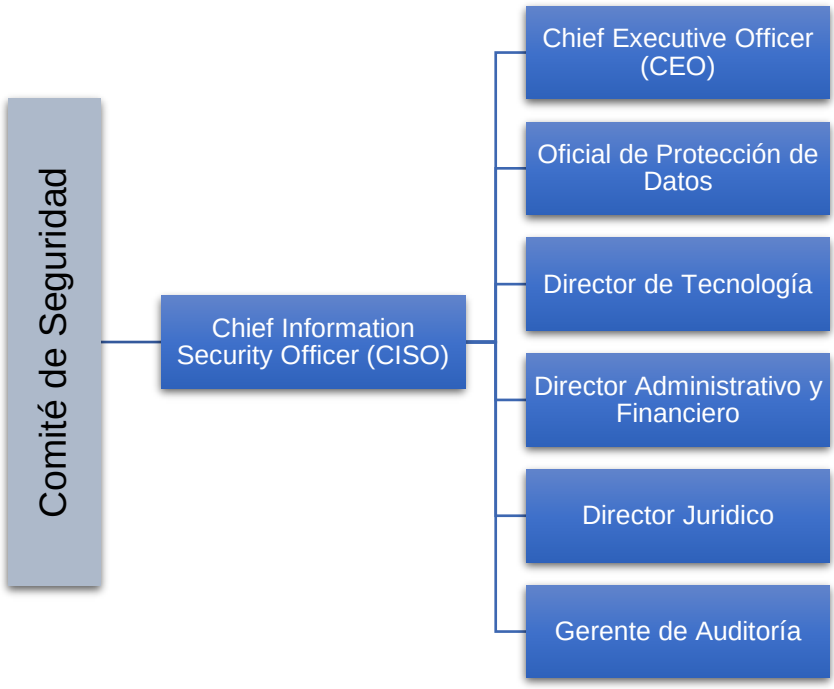

Figura 13 *Estructura Comité de Seguridad*

Cualquier otro Director o Gerente podrá ser invitado ad hoc a participar en el Comité de Seguridad de acuerdo con los temas a tratar o gestionar.

Responsabilidades Chief Information Security Officer (CISO)

Será responsable de monitorear, coordinar y hacer un seguimiento continuo del gobierno, operación y revisión del SGSI, activar los planes de acción requeridos para su mejora e informar al Comité de Seguridad sobre el estado del SGSI. Las principales responsabilidades son:

- Velar por la seguridad de la información en la empresa.
- Coordinar la gestión, mantenimiento y la mejora continua del SGSI, tal y cómo se establece en la Política de Seguridad de la Información.
- Asegurar que los controles de seguridad de la información estén implementados, sean efectivos y cubran los riesgos en materia de seguridad de la información.
- Determinar los métodos para implementar y hacer cumplir las políticas de seguridad de la información, así como asesorar al comité de seguridad y a la Alta Dirección en cuestiones relacionadas con seguridad de la información.

- Asegurar que se ejecuten los programas de sensibilización y capacitación en materia de seguridad de la información y que se realicen auditorías de seguridad, informes y seguimiento de forma periódica.
- Actualizar el Marco Normativo de Seguridad de la Información bajo la Política de Seguridad de la Información y demás estándares de buenas prácticas en materia de seguridad de la información.
- Informar sobre el estado y la evolución del SGSI al Comité de Seguridad.
- Promover y asegurar la definición, aplicabilidad y vigencia de las políticas, procedimientos y guías que afecten la seguridad de la información.
- Velar por el mantenimiento y comunicación de los roles y responsabilidades definidos para empleados y proveedores en materia de Seguridad de la Información.
- Asegurar la definición de procedimientos y directrices de seguridad de la información en el proceso de planificación y ejecución de proyectos u otras iniciativas a nivel corporativo.
- Velar por el cumplimiento de requerimientos legales y contractuales relacionados con la seguridad de la información.
- Asegurar las acciones necesarias para desarrollar el seguimiento y la medición del desempeño de la gestión de seguridad de la información para conseguir la mejora continua del sistema.
- Monitorizar de forma general los incidentes de seguridad de la información para conseguir que se resuelvan de una manera efectiva y oportuna.
- Revisar y controlar el nivel de exposición a riesgos de seguridad de la información.
- Gestionar los riesgos del SGSI.
- Promover la cultura de seguridad de la información en la organización.
- Apoyar el desarrollo del Comité de Seguridad del SGSI.
- Realizar seguimiento al cierre de las acciones correctivas asociadas con el SGSI.

Responsabilidades Chief Executive Officer (CEO)

- Aprobar y apoyar los objetivos corporativos de seguridad de la información y los componentes del marco de gestión de seguridad de la información, demostrando así el compromiso de cumplir con los requisitos relacionados con la seguridad de la información.
- Apoyar y garantizar el cumplimiento de las políticas, normas, procedimientos y prácticas de seguridad de la información, así como el de leyes y reglamentos aplicables en materia de seguridad de la información y protección de datos.
- Proveer los recursos necesarios para la planificación, implementación, revisión y mejora del SGSI.
- Revisar y validar los cambios estratégicos que afecten al SGSI.
- Apoyar el desarrollo de las sesiones de revisión por la dirección del SGSI.

- Aplicar el proceso disciplinario ante los incidentes de seguridad de la información originados por empleados.
- Realizar monitoreo general de incidentes críticos de seguridad de la información para promover su resolución efectiva y oportuna.

Responsabilidades Oficial de Protección de Datos

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- Coordinar la definición e implementación de los controles para la protección de datos personales.
- Impulsar una cultura de protección de datos.
- Mantener un inventario de las bases de datos personales y clasificarlas según su tipo.
- Analizar las responsabilidades de cada cargo de la organización para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos
- Realizar un entrenamiento general en protección de datos personales para todos los empleados.
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la empresa.
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las políticas de tratamiento de la información personal.

Responsabilidades del Director de Tecnología

- Implementar los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir, de acuerdo con los lineamientos dados por el CISO.
- Reportar los resultados de las pruebas periódicas de vulnerabilidades sobre los diferentes sistemas de información para detectar oportunidades de mejora a nivel de seguridad de la información.
- Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados y mantener informado al Comité de Seguridad.
- Trabajar con la alta dirección y los dueños de los procesos en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
- Evaluar los requisitos de seguridad de la información que deben ser adoptados en el desarrollo de nuevos proyectos.

Responsabilidades del Director Administrativo y Financiero

- Realizar el análisis costo / beneficio de la implementación de controles de seguridad de la información.
- Aprobar el presupuesto anual de seguridad de la información.

Responsabilidades del Director Jurídico

- Verificar el cumplimiento de las obligaciones legales y regulatorias relacionadas con la seguridad de la información.
- Estar al tanto de los cambios normativos respecto a Seguridad de la Información, informándose de las consecuencias para las actividades de la empresa y proponiendo las medidas oportunas para adecuarse al nuevo marco normativo.
- Definir los requisitos contractuales que deben cumplir los proveedores y demás terceros de acuerdo con los lineamientos de Seguridad de la Información establecidos.
- Asesor al Comité de Seguridad frente a la respuesta que se debe dar como parte de la respuesta ante los incidentes de seguridad de la información que se puedan materializar.

Responsabilidades del Gerente de Auditoría

- Realizar revisiones periódicas para determinar el nivel de cumplimiento de los requisitos de seguridad de la información.
- Realizar seguimiento frente a los planes de acción definidos para dar cierre a las brechas de seguridad de la información identificados.
- Reportar al Comité de Seguridad los avances frente a las acciones de mejora definidas.

Adicional a los miembros del comité, se requiere el apoyo de diferentes áreas, procesos y personas para el correcto funcionamiento de Sistema de Gestión de Seguridad de la Información. A continuación, se describen las responsabilidades:

Coordinación de infraestructura tecnológica:

- Remediación de las vulnerabilidades reportadas por el fabricante correspondiente o identificadas en herramientas de detección automáticas.
- Monitoreo, reporte y tratamiento de los incidentes de seguridad informática.
- Actividades de hardening definidas para las plataformas que componen la infraestructura tecnológica.

- Validar el cumplimiento de las prácticas de desarrollo de código seguro para las aplicaciones.
- Implementar la política de control de acceso para los sistemas de información y aplicaciones.
- Implementar los controles de seguridad de la información aplicables a la plataforma tecnológica.

Dueño del activo:

- Clasificar los activos de información que se encuentran a su cargo de acuerdo con los niveles de criticidad definidos.
- Velar por la correcta aplicación de controles de seguridad de acuerdo con la criticidad de cada activo de información.
- Revisar periódicamente los controles de acceso que han sido asignados a la información que se encuentra a su cargo.
- Definir los requerimientos respecto a las copias de seguridad de la información de su proceso.

Empleados:

Todos los empleados de la empresa tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información, lo que debe quedar incluido en los contratos.

3.6. Metodología de Análisis de Riesgos

Teniendo en cuenta que uno de los pilares del Sistema de Gestión de Seguridad de la Información es la gestión de riesgos, es fundamental definir e implementar una metodología de riesgos de seguridad de la información que establezca los lineamientos para la identificación y valoración de activos de información, amenazas y vulnerabilidades, para así, definir las acciones de mejora que deben ser implementadas para mitigar la materialización de los riesgos identificados.

Con base en lo anterior, se define la metodología de riesgos de seguridad de la información la cual deberá ser implementada como parte del SGSI. Las valoraciones de riesgos de seguridad de la información deberán ser realizadas como mínimo una vez al año. De igual forma, se deberán realizar cuando se presenten cambios o se generen proyectos que afecten la infraestructura tecnológica u operación de los procesos respecto a seguridad de la información.

El modelo a seguir para el análisis de riesgos de seguridad de la información se fundamenta en los siguientes pasos:

Figura 14 *Análisis de riesgos de seguridad de la información*

1. Identificación y valoración de activos de información

Para la empresa se define que un activo de información puede ser cualquier objeto tangible o intangible que tiene un valor y que puede ser vulnerado ocasionando consecuencias para la empresa.

Así las cosas, se han definido las siguientes categorías para clasificar los activos de información:

- Información (Digital o física)
- Aplicaciones o sistemas de información
- Servicios
- Hardware
- Redes de comunicaciones
- Instalaciones
- Personas (empleados o terceros)

Una vez se han sido identificados los activos de información, es necesario determinar su nivel de criticidad para la empresa, de esta forma, se podrá determinar en que se deben centrar los esfuerzos para implementar medidas de protección. Es por esto que, la valoración de cada activo se realiza teniendo en cuenta los principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad. Para cada principio se han definido escalas que permitan determinar su criticidad:

Confidencialidad	
Valor	Descripción
4	Secreta
3	Confidencial
2	Uso Interno
1	Pública

Integridad	
Valor	Descripción
3	Alto
2	Medio
1	Bajo

Disponibilidad	
Valor	Descripción
3	Alto
2	Medio
1	Bajo

Tabla 2 *Criterios valoración principios de seguridad*

Para determinar el nivel de criticidad del activo se aplicará la siguiente formula:

$$Criticidad = Confidencialidad * 40\% + Integridad * 30\% + Disponibilidad * 30\%$$

Los porcentajes para cada uno de los principios se han definido teniendo en cuenta la naturaleza de negocio, por lo cual, mantener la confidencialidad es uno de los factores más importante ya que se tiene acceso a información personal de los clientes.

De igual forma, y como parte de la valoración del activo es importante determinar el valor que representa para la empresa el daño de dicho activo. Se ha definido una escala de valores cualitativos que permita estimar los efectos causados:

Valor	Criterio
Alto	El daño genera un impacto severo para el negocio
Medio	El daño genera un impacto grave para el negocio
Bajo	El daño genera un impacto menor para el negocio
Despreciable	El daño es irrelevante para el negocio

Tabla 3 *Criterios valoración asociada a daños*

Como parte de la identificación del activo, se debe determinar el dueño del activo dentro de la empresa, quien será el responsable de asegurar que se cumplan con las medidas de protección de acuerdo con su nivel de criticidad.

2. Identificación y valoración de amenazas

Una amenaza tiene el potencial de causar un incidente afectando de manera directa o indirecta los activos de información de la empresa. Por lo anterior, se deben identificar las amenazas y vulnerabilidades relacionadas que puedan afectar los activos de información que han sido identificados como críticos para así determinar el nivel de riesgo inherente. La identificación de amenazas se debe realizar de acuerdo con las categorías de activos de información definidas.

Para cada amenaza identificada es necesario determinar la probabilidad de ocurrencia, así como, el impacto que podría generar, para esto se han definido las siguientes escalas:

N°	NIVEL	CRITERIO CUANTITATIVO	CRITERIO CUALITATIVO
5	**Muy Alta**	Ha ocurrido por lo menos una vez en los últimos 6 meses.	La probabilidad de que ocurra es casi segura.
4	**Alta**	Ha ocurrido por lo menos una vez en los últimos dos años.	La probabilidad de que ocurra es muy posible.
3	**Media**	Ha ocurrido por lo menos 1 vez en los últimos 3 años.	La probabilidad de que ocurra es posible
2	**Baja**	Ha ocurrido en los últimos 5 años.	La probabilidad que ocurra NO es muy posible
1	**Muy baja**	Ha ocurrido por lo menos una vez en los últimos 10 años.	La probabilidad que ocurra es mínima.

Tabla 4 *Escalas de probabilidad*

N	NIVEL	REPUTACIONAL	LEGAL	OPERACIONAL
5	**Severo**	La afectación de la imagen de puede ser tal que repercute a nivel internacional.	Incumplimiento de las obligaciones legales que generen el cierre total o parcial de la operación.	Parada de la operación de todos los procesos misionales.
4	**Mayor**	La afectación de la imagen puede ser tal que repercute a nivel nacional a través de los medios de comunicación.	Obligaciones legales que resulten en sanciones o multas económicas significativas.	Retraso de un proceso misional o varios procesos no misionales.
3	**Considerable**	La afectación de la imagen puede ser tal que repercute a nivel regional a través de los medios de comunicación.	Obligaciones legales que generen llamados de atención de entidades externas.	Parada de un proceso no misional.
2	**Menor**	La afectación de la imagen puede ser tal que repercute a nivel local	Requerimientos de información por parte de entes regulatorios	Retraso de un proceso no misional.
1	**Insignificante**	Se generan inquietudes en los clientes las cuales por ser atendidas y solucionadas directamente por la empresa.	Incumplimiento de las obligaciones legales	Afectación a activos específicos.

Tabla 5 *Escala de impactos*

Con el fin de determinar el nivel de riesgo inherente, se tendrán en cuenta las valoraciones de probabilidad e impacto basado en la siguiente matriz:

			PROBABILIDAD				
			Muy Baja	Baja	Media	Alta	Muy Alta
			1	2	3	4	5
IMPACTO	Severo	5	Moderado	Alto	Extremo	Extremo	Extremo
	Mayor	4	Moderado	Alto	Alto	Extremo	Extremo
	Considerable	3	Moderado	Moderado	Alto	Alto	Extremo
	Menor	2	Bajo	Moderado	Moderado	Alto	Alto
	Insignificante	1	Bajo	Bajo	Moderado	Moderado	Moderado

Tabla 6 *Matriz nivel de riesgo*

3. Identificación de controles de seguridad

Una vez identificado el nivel de riesgo inherente, es fundamental identificar los controles de seguridad de la información que se encuentran actualmente implementados y que podrían llegar a mitigar las amenazas identificadas. Es importante tener claridad acerca de la naturaleza del control (preventivo o correctivo) para así determina si el control reduce la probabilidad o el impacto del riesgo identificado.

4. Cálculo del riesgo residual estimado

Previo al cálculo del nivel de riesgo residual es importante calcular la probabilidad e impacto residual estimados, teniendo en cuenta los controles que han sido aplicados. En caso de que el control aplicado sea de naturaleza preventivo se reducirá la probabilidad de ocurrencia, cuando el control es de naturaleza correctivo se reducirá el impacto. De esta forma se calculará el riesgo residual estimado teniendo como base la matriz de nivel de riesgo relacionada en la Tabla 6.

5. Tratamiento del riesgo

Con base en los niveles de riesgo residual identificados, se debe realizar un adecuado tratamiento teniendo en cuenta el nivel de exposición que puede representar para la empresa. A continuación, se relacionan las acciones que se deben llevar a cabo para realizar un adecuado tratamiento de los riesgos basado en los niveles de tolerancia definidos por la empresa:

Nivel de Riesgo	Acciones a tomar	
EXTREMO	Gestionar el riesgo inmediatamente	Plantear planes de tratamiento de riesgos y gestionar los recursos necesarios para su implementación dándole prioridad a estos mismos dentro del plan de tratamiento de riesgos puesto que es donde se podría ver más afectada la empresa.
ALTO	Gestionar el riesgo lo más pronto posible	Plantear planes de tratamiento de riesgos y gestionar los recursos necesarios para su implementación. Estos planes tendrían una prioridad menor que aquellos que estén asociados a riesgos de nivel Extremo, sin embargo, deberán ser considerados y asignados los recursos necesarios para que en el término de un año se logre su implementación y por ende la reducción del nivel de riesgo.
MODERADO	Monitorear los riesgos	No se generan planes de tratamiento para los riesgos que queden en este nivel de riesgo. El monitoreo de los riesgos será anual, el cual se realizará cuando se lleve a cabo la revisión de los riesgos tal como plantea el procedimiento para la gestión de riesgos de Seguridad de la Información.
BAJO	Aceptar los riesgos	No se generan planes de tratamiento para los riesgos que queden en este nivel de riesgo. Estos riesgos son aceptados y queda a consideración del propietario de riesgo si desea revisarlos en el siguiente año.

Tabla 7 *Acciones a tomar por nivel de riesgo*

3.7. Declaración de Aplicabilidad

De acuerdo con los controles establecidos en la ISO/IEC 27002, se hace necesario definir cuáles deben ser implementados en la empresa teniendo en cuenta la operación de los procesos de negocio. Luego de realizar un análisis detallado, se identificó que los 114 controles aplican por lo cual se requiere que sean implementados y operados de acuerdo con los lineamientos de seguridad de la información. El análisis detallado puede ser consultado en el Anexo 4. Declaración de aplicabilidad.

4. Análisis de riesgos de seguridad de la información

Con el fin de realizar una gestión de riesgos de seguridad de la información basada en las necesidades de la empresa, se ha realizado la identificación y valoración de activos de información y de amenazas para así poder determinar las medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

Los resultados detallados del análisis de riesgos de seguridad de la información se encuentran en el Anexo 5. Matriz Activos y Riesgos. A continuación, se muestra un resumen de los resultados obtenidos:

Identificación y valoración de activos:

Se identificaron 49 activos de información para las categorías de: aplicaciones o sistemas de información, hardware, servicios, información, instalaciones, personas y redes de comunicación.

Evaluación riesgo residual:

De acuerdo con la criticidad de los activos de información, se realizó la identificación de amenazas con base en la categoría de activo identificada. La valoración del riesgo inherente se realizó teniendo en cuenta la probabilidad e impacto. Posteriormente se identificaron los controles de seguridad que están siendo aplicados actualmente, con el fin de evaluar el riesgo residual estimado. Así las cosas, se identificaron:

- 1 amenazas en nivel de riesgo extremo
- 8 amenazas en nivel de riesgo alto
- 40 amenazas en nivel de riesgo moderado
- 5 amenaza en nivel de riesgo bajo

5. Plan de Proyectos

Con base en el análisis de riesgos de seguridad de la información y con el objetivo de evolucionar el nivel de cumplimiento de los controles definidos en el estándar ISO/IEC 27002, se ha definido un proyecto macro el cual abarca diferentes fases que buscan dar solución a las brechas identificadas de seguridad de la información:

Nombre del proyecto
Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios.
Objetivo del proyecto
• Actualización de los servicios de tecnología de la empresa apalancados en nubes públicas. • Diseño e implementación de controles de última generación para la protección por ciberataques de los sistemas de información. • Diseño e implementación de controles internos para la protección contra fallas humanas en la administración de la plataforma tecnológica.
Stakeholders
• Alta Dirección • Chief Information Security Officer (CISO) • Director de Tecnología
Especificaciones técnicas
Como parte del proyecto se contempla la implementación de 5 servicios en la nube, para los cuales se detallan las actividades que deben ser ejecutadas para su correcta implementación:
Active Directory
Consideraciones: ▪ Directorio Segregado OnPremise con sincronización de contraseñas mediante Azure DirSyc. ▪ No se expondrán servicios desde la red interna, solamente el Active Directory tendrá acceso a Azure AD con WhiteListing. **Actividades:** ▪ Implementación de Azure AD, en este caso comandara los servicios en la nube de Azure (suscripciones) y en los servicios gestionados de Microsoft 365 (Correo y demás aplicaciones). ▪ Implementación de políticas hibridas e integración con Microsoft Intune. ▪ Implementación de reglas de login por niveles de riesgo.

- Implementación de MFA.

Mail Server

- Exportación de los datos a los servicios de Microsoft 365, con licencias completas E5.
- Puesta en funcionamientos del portal de Microsoft Intune para dispositivos por fuera de la red.
- Implementación de BYOD con políticas de seguridad hibridas. Esto apalancara los controles de fuga de información y errores de los usuarios.
- Desactivación de los servicios internos de correo electrónico.

Al ser un servicio SaaS se tendrá transferencia del riesgo al CSP para las siguientes amenazas:

- *Caída del Sistema por agotamiento de recursos*
- *Emanaciones Electromagnéticas*
- *Fallo de servicios de comunicaciones (por parte del servicio y del CSP, la probabilidad es muy baja)*
- *Acceso no autorizado*
- *Desactivación y desaprovisionamiento de los servicios onpremise.*

Web Server

Consideraciones:

- Para los web server se implementaran NSG dentro de la redes internas de las suscripciones.

Actividades

- Implementación de Azure Firewall para las publicaciones externas.
- Implementación de Application Gateway (WAF) para los servicios web.
- Creación de reglas.
- Desactivación y desaprovisionamiento de los servicios onpremise.

***NOTA**: Estos servicios deberían de ser implementados como servicios PaaS o IaaS, posiblemente con k8s autoescalable.*

VoIP

- Configurar Microsoft Teams como proveedor de servicios integrados de comunicaciones.
- Configurar VoIP Cloud para Servicios BPX en los cuales se presten los servicios desde Onpremise o cualquier lugar con conexión a internet.

Database

- Implementar en Azure SQL los servicios de bases de datos.
- Activar redundancia entre regiones.

Generalidades para otros servicios del backend
• Para los servicios de backend se pondrán servidores como IaaS. • Los servicios tendrán la implementación de JIT o Bastion Host para el acceso ya sea desde onpremise o servicios nube. • Todos los servicios tendrán backup delta diario full semanal con el fin de apalancar los procesos de mitigación del riesgo de errores de administración en los servicios del CSP. • Integración de Azure RMS con el fin de apalancar los procesos de control de acceso y de fuga de información. • Asignación de roles.
Cambios en la red
• El firewall será utilizado como proxy para la salida a internet. • Todos los equipos internos dentro del dominio usaran los servicios de protección avanzada EDR, Firewall y Antivirus.
Duración estimada
6 meses
Costo estimado
USD 50.000 – Costo de la consultoría por 6 meses* USD 13,722.78 – Valor mensual servicios Azure

**Teniendo en cuenta los recursos actuales de la empresa, se hace necesario contratar personal experto para la ejecución del proyecto, por lo cual se debe considerar contratar un servicio de consultoría que contemple 3 consultores expertos en la implementación de servicios en la nube y un líder de proyecto.*

Con el fin de tener una referencia de los costos asociados a la implementación de los servicios en la nube, a continuación, se detallan los costos mensuales para cada servicio:

Tipo de servicio	Región	Descripción	Costo mensual estimado (USD)
Virtual Machines	West US 2	6 B2MS (2 vCPU, 8 GB de RAM) x 730 Horas; Windows – (solo SO); Pago por uso; 0 discos de sistema operativo administrados: S4, 100.000 unidades de transacción; Tipo de transferencia interregional, 5 GB de transferencia de datos de salida de West US 2 a Asia Oriental	$449.46

Tipo de servicio	Región	Descripción	Costo mensual estimado (USD)
Virtual Machines	West US	2 D2 v3 (2 vCPU, 8 GB de RAM) x 730 Horas; Windows – (solo SO); Pago por uso; 0 discos de sistema operativo administrados: S4, 100 unidades de transacción; Tipo de transferencia interregional, 5 GB de transferencia de datos de salida de Oeste de EE. UU. a Asia Oriental	$305.19
Azure SQL Database	East US	Base de datos única, Núcleo virtual, Almacenamiento de copia de seguridad RA-GRS, Uso general, Aprovisionado, Gen 5, Redundancia local, 1, instancias 6 vCore, 3 año de reserva, 500 GB de almacenamiento, 500 GB de almacenamiento de copia de seguridad	$919.84
Azure Kubernetes Service (AKS)	West US	1 A3 (4 vCPU, 7 GB de RAM) nodos x 730 Horas; Pago por uso; 0 discos de SO administrados: S4, 0 clústeres	$175.20
Azure Cost Management and Billing		El gasto administrado de Azure es gratuito. Hay otras características premium disponibles de forma gratuita hasta diciembre de 2018, momento en el que pasarán a ser de pago (un 1 % del gasto administrado para AWS y Google Cloud Platform).	$0.00
Application Gateway	East US	Nivel Basic, tamaño de instancia Pequeña: 1 instancias con horas de puerta de enlace x 730 Horas, 0 GB de unidades de datos procesados, 5 GB de unidades de zona	$18.25
IP Addresses	East US	6 direcciones IP dinámicas, 0 direcciones IP estáticas, 0 reasignaciones	$14.60
Application Gateway	East US	Nivel Basic, tamaño de instancia Pequeña: 1 instancias con horas de puerta de enlace x 730 Horas, 0 GB de unidades de datos procesados, 5 GB de unidades de zona	$18.25
Azure Active Directory	West US 2	1800 users Premium P1, 0 users Premium P2, Standard tier, 730 directory objects, Horas de bosque de usuarios {5, Horas de bosque de recursos {7}.	$10,909.50
Azure Firewall	West US	1 unidades de firewall lógico x 730 Horas, 0 GB Datos procesados	$912.50
		Total	**$13,722.78**

Tabla 8 *Costos servicios en la nube*

Planeación del proyecto

Con base en el planteamiento anterior, donde se especifican los servicios que deben ser migrados a la nube, a continuación, se propone el cronograma a seguir para su implementación:

Name	Duration	Start	Finish	Predecessors
Planeacion	**12 days**	**1/4/21 8:00 AM**	**1/19/21 5:00 PM**	
Kickoff	2 days	1/4/21 8:00 AM	1/5/21 5:00 PM	
Reuniones Individuales	10 days	1/6/21 8:00 AM	1/19/21 5:00 PM	2
Levantamiento de Informacion	10 days	1/6/21 8:00 AM	1/19/21 5:00 PM	2
Implementacion	**100 days**	**1/20/21 8:00 AM**	**6/8/21 5:00 PM**	**1**
Preparaciones Generales	15 days	1/20/21 8:00 AM	2/9/21 5:00 PM	
Preparacion Nube y creacion de suscripcion	10 days	1/20/21 8:00 AM	2/2/21 5:00 PM	1
Creacion de maquinas IaaS	10 days	2/10/21 8:00 AM	2/23/21 5:00 PM	7;10
Creacion de Servicios PaaS	10 days	2/10/21 8:00 AM	2/23/21 5:00 PM	7;10
Creacion de NSG y Arquitectura de red	5 days	2/3/21 8:00 AM	2/9/21 5:00 PM	7
Implmenetacion de Azure Bastion	5 days	2/24/21 8:00 AM	3/2/21 5:00 PM	8
Active Directory	**17 days**	**3/3/21 8:00 AM**	**3/25/21 5:00 PM**	**11**
Implmenetacion Azure AD	5 days	3/3/21 8:00 AM	3/9/21 5:00 PM	11
Syncronizacion Azure AD	2 days	3/10/21 8:00 AM	3/11/21 5:00 PM	13
Implementacion de Seguridad basica de Azure MFA	6 days	3/10/21 8:00 AM	3/17/21 5:00 PM	11;13
Politicas Hibridas	3 days	3/18/21 8:00 AM	3/22/21 5:00 PM	15
Movimiento a red Interna	3 days	3/23/21 8:00 AM	3/25/21 5:00 PM	13;14;15;16
Mail Server	**18 days**	**3/26/21 8:00 AM**	**4/20/21 5:00 PM**	**12**
Sincronizacion de usuarios	2 days	3/26/21 8:00 AM	3/29/21 5:00 PM	15
Sincronizacion de Intune	2 days	3/30/21 8:00 AM	3/31/21 5:00 PM	19
Politicas de BYOD	10 days	4/1/21 8:00 AM	4/14/21 5:00 PM	20
Apagado y desarprovisionamiento	4 days	4/15/21 8:00 AM	4/20/21 5:00 PM	19;20;21
Servicios Web	**20 days**	**3/3/21 8:00 AM**	**3/30/21 5:00 PM**	
Implementacion de Azure FW	5 days	3/3/21 8:00 AM	3/9/21 5:00 PM	11
Implementacion de Application Gateway	5 days	3/3/21 8:00 AM	3/9/21 5:00 PM	11
Creacion de reglas	7 days	3/10/21 8:00 AM	3/18/21 5:00 PM	24;25
Configuracion de Servicios PaaS	8 days	3/19/21 8:00 AM	3/30/21 5:00 PM	26
VOIP	**10 days**	**3/31/21 8:00 AM**	**4/13/21 5:00 PM**	**23**
COnfiguracion de Ms Teams	5 days	3/31/21 8:00 AM	4/6/21 5:00 PM	27
Configuracion de Servicico PBX Cloud	5 days	4/7/21 8:00 AM	4/13/21 5:00 PM	29
Bases de Datos	**48 days**	**3/26/21 8:00 AM**	**6/1/21 5:00 PM**	
Implementacion de Azure SQL	10 days	3/26/21 8:00 AM	4/8/21 5:00 PM	17
Aseguramiento de Azure SQL	10 days	4/9/21 8:00 AM	4/22/21 5:00 PM	32
Cambios en la Red OnPremise	8 days	4/23/21 8:00 AM	5/4/21 5:00 PM	33
Validacion Proxy	5 days	5/5/21 8:00 AM	5/11/21 5:00 PM	34
Implementacion de Agentes en equipos	20 days	5/5/21 8:00 AM	6/1/21 5:00 PM	34
Cierre de Proyectos	**5 days**	**6/2/21 8:00 AM**	**6/8/21 5:00 PM**	
Reunion de Cierre	5 days	6/2/21 8:00 AM	6/8/21 5:00 PM	36

Figura 15 *Planeación del proyecto*

La definición del proyecto de migración de diferentes servicios a la nube surge de la necesidad de mitigar los riesgos de seguridad de la información que fueron identificados durante el análisis de riesgos de seguridad de la información, de acuerdo con el planteamiento del proyecto, a continuación, se muestra cada riesgo identificado con qué servicio podría ser mitigado:

Riesgos Identificados		Proyectos				
Categoría Activo	Amenazas	Active Directory	Mail Server	Web Server	VoIP	Database
Redes de comunicaciones	Caída del sistema por agotamiento de recursos	x	x	x	x	x
Redes de comunicaciones	Corte de Suministro eléctrico	x		x	x	x
Redes de comunicaciones	Errores del administrador	x		x	x	x
Redes de comunicaciones	Emanaciones electromagnéticas	x	x	x	x	x
Redes de comunicaciones	Fallo de Servicios de Comunicaciones	x	x	x	x	x
Hardware	Caída del sistema por agotamiento de recursos	x	x	x	x	x
Hardware	Errores de mantenimiento / actualización de equipos	x		x	x	x
Hardware	Errores del administrador	x		x	x	x
Hardware	Avería de Origen Físico o lógico	x		x	x	x
Personas	Indisponibilidad del personal			x		
Servicios	Errores del administrador			x		
Servicios	Manipulación errada de la configuración			x		
Servicios	Alteración accidental de la configuración			x		
Servicios	Vulnerabilidades del software			x	x	
Información	Fugas de información		x	x		x
Información	Alteración accidental de la información	x		x		
Información	Almacenamiento de información en repositorios no autorizados			x		
Aplicaciones o sistemas de información	Fugas de información		x	x		x
Aplicaciones o sistemas de información	Errores del administrador			x		
Aplicaciones o sistemas de información	Errores de mantenimiento			x		
Aplicaciones o sistemas de información	Errores de los usuarios			x		

Riesgos Identificados		Proyectos				
Categoría Activo	Amenazas	Active Directory	Mail Server	Web Server	VoIP	Database
Aplicaciones o sistemas de información	Vulnerabilidades del software			x	x	
Aplicaciones o sistemas de información	Acceso no autorizado	x	x	x	x	x

Tabla 9 *Relación riesgos versus proyectos*

Al realizar la implementación del proyecto planteado, la empresa evolucionará respecto al nivel de cumplimiento de los controles ISO/IEC 27002, teniendo en cuenta el impacto que tiene la migración de los servicios a la nube y los beneficios que puede generar respecto a seguridad de la información. De acuerdo con el análisis realizado se identificó que los siguientes controles tendrán una evolución al implementar el proyecto:

Controles ISO 27002		Proyectos				
		Active Directory	Mail Server	Web Server	VoIP	Database
A.6.2.2	Teletrabajo	x		x		x
A.9.1.1	Política de control del acceso	x	x	x		
A.9.1.2	Acceso a redes y a servicios en red	x	x	x		
A.9.2.1	Registro de usuarios 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		x		
A.9.2.5	Revisión de los derechos de acceso de usuarios	x		x		
A.9.2.6	Retiro o ajuste de los derechos de acceso	x				
A.9.3.1	Uso de información de autenticación secreta	x		x		
A.9.4.1	Restricción de acceso a la información			x		x
A.9.4.3	Sistema de gestión de contraseñas	x		x		x
A.9.4.4	Uso de programas utilitarios privilegiados	x				
A.9.4.5	Control de acceso a códigos fuente de programas			x		x
A.10.1.1	Política sobre uso de controles criptográficos		x	x		x
A.10.1.2	Gestión de llaves		x	X		
A.12.1.2	Gestión de cambios		x	x		
A.12.1.3	Gestión de capacidad		x	x		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación			x		
A.12.2.1	Controles contra códigos maliciosos		x	x	x	x

Controles ISO 27002		Proyectos				
		Active Directory	Mail Server	Web Server	VoIP	Database
A.12.3.1	Respaldo de la información		x	x		
A.12.4.1	Registro de eventos		x	x		x
A.12.4.2	Protección de la información del registro		x	x		x
A.12.4.3	Registros de administrador y de operador		x	x	x	x
A.12.4.4	Sincronización de relojes		x	x	x	x
A.12.5.1	Instalación de software en sistemas operativos	x		x		
A.12.6.1	Control de las vulnerabilidades técnicas		x	x		
A.12.6.2	Restricciones sobre la instalación de software	x	x	x		
A.12.7.1	Controles de auditorías de sistemas de información	x	x	x	x	x
A.13.1.1	Controles de las redes		x	x	x	
A.13.1.2	Seguridad de los servicios de red		x	x	x	
A.13.1.3	Separación en las redes		x	x	x	
A.13.2.1	Política y procedimientos de transferencia de información		x	x		
A.13.2.2	Acuerdos sobre transferencia de información		x	x		
A.13.2.3	Mensajería electrónica		x			
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	x	x	x	x	x
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	x	x	x	x	x
A.14.1.3	Protección de transacciones de los Servicios de las aplicaciones	x	x	x	x	x
A.14.2.1	Política de desarrollo seguro	x	x	x	x	x
A.14.2.2	Procedimiento de control de cambios en sistemas	x	x	x	x	x
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	x	x	x	x	x
A.14.2.4	Restricciones en los cambios a los paquetes de software	x	x	x	x	x
A.14.2.5	Principios de construcción de los sistemas seguros	x	x	x	x	x
A.14.2.6	Ambiente de desarrollo seguro	x	x	x	x	x
A.14.2.7	Desarrollo contratado externamente	x	x	x	x	x
A.14.2.8	Pruebas de seguridad de sistemas	x	x	x	x	x
A.14.2.9	Prueba de aceptación de sistemas	x	x	x	x	x
A.14.3.1	Protección de Datos de Prueba	x	x	x	x	x
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	x	x	x	x	x
A.15.2.2	Gestión de cambios en los servicios de los proveedores	x	x	x	x	x
A.16.1.1	Responsabilidades y procedimientos	x	x	x	x	x

Controles ISO 27002		Proyectos				
		Active Directory	Mail Server	Web Server	VoIP	Database
A.16.1.2	Reporte de eventos de seguridad de la información	x	x	x	x	x
A.16.1.3	Reporte de debilidades de seguridad de la información	x	x	x	x	x
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	x	x	x	x	x
A.16.1.5	Respuesta a incidentes de seguridad de la información	x	x	x	x	x
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	x	x	x	x	x
A.16.1.7	Recolección de evidencia	x	x	x	x	x
A.17.1.1	Planificación de la continuidad de la seguridad de la información	x	x	x	x	x
A.17.1.2	Implementación de la continuidad de la seguridad de la información	x	x	x	x	x
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	x	x	x	x	x
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	x	x	x	x	x

Tabla 10 *Relación controles versus proyectos*

Con base en el alcance planteado en el proyecto, se estima que una vez se finalice su implementación, se tendría un mayor nivel de cumplimiento de los controles como se muestra en la gráfica:

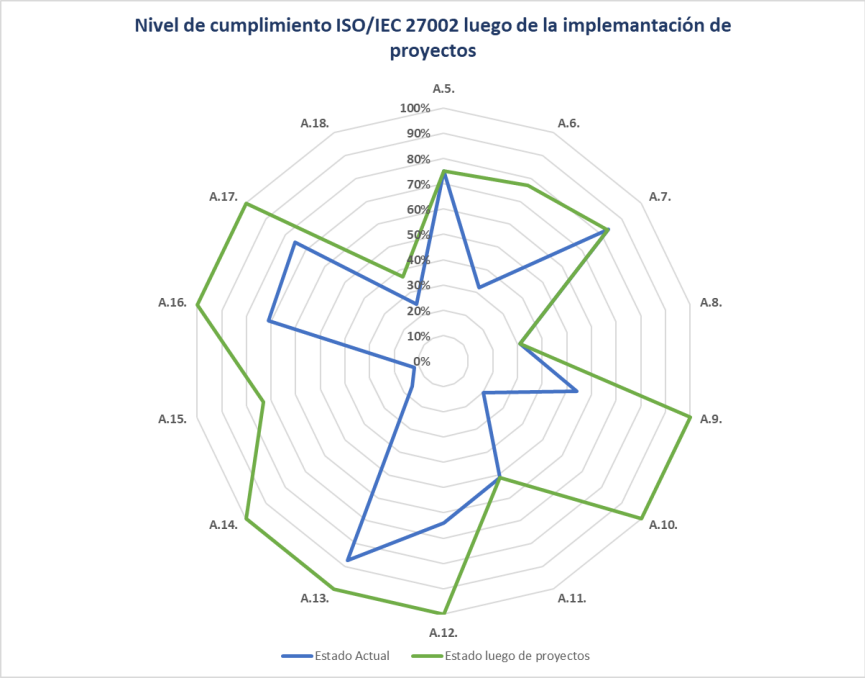

Figura 16 *Cumplimiento ISO/IEC 27002*

6. Auditoría de Cumplimiento

Con el objetivo de evaluar el nivel de madurez para cada uno de los controles del estándar ISO/IEC 27002:2013, se realizó una auditoría en la cual se revisaron uno a uno los 114 controles planteados en el estándar. Como parte de la auditoría se realizó una revisión documental, entrevistas con los responsables de los controles y visitas tanto a las instalaciones físicas administrativas como a los centros de datos y cableado. Como resultado de la auditoría se identificaron 42 no conformidades y 15 oportunidades de mejora, para las cuales se dan recomendaciones con el fin de dar cierre a las brechas identificadas.

De igual manera se realizó una evaluación con el fin de determinar el nivel de madurez de los controles. La evaluación se realizó siguiendo el Modelo de Madurez de la Capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproductible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 11 *Modelo de Madurez de la Capacidad CMM*

Resultados obtenidos:

Una vez realizada la auditoría y consolidados los resultados, se obtuvo el nivel de madurez para cada uno de los 114 controles, los resultados se muestran a continuación:

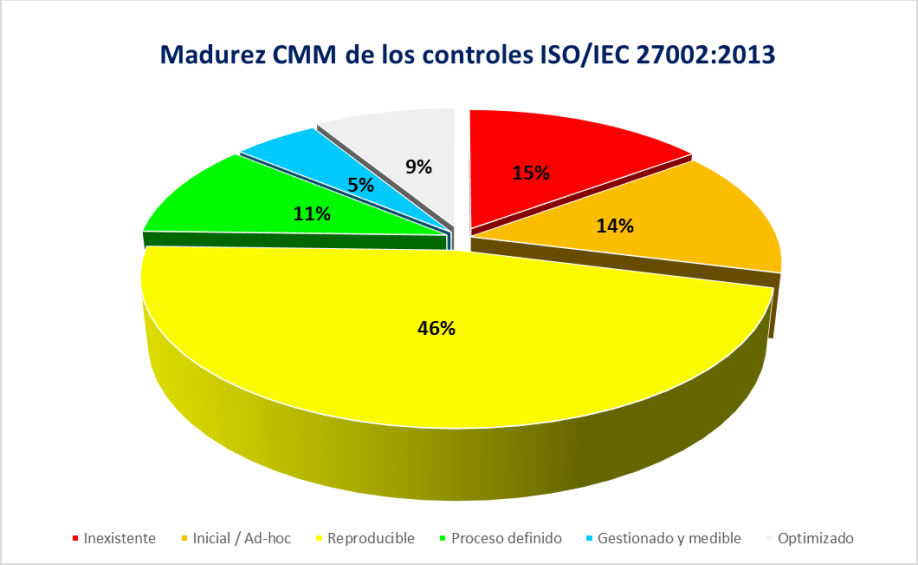

Figura 17 Madurez CMM de los controles

Así mismo, se realizó un análisis del nivel de madurez por dominios que plantea el estándar, los cuales fueron comparados con el nivel objetivo de seguridad de la información de la empresa, los resultados se muestran a continuación:

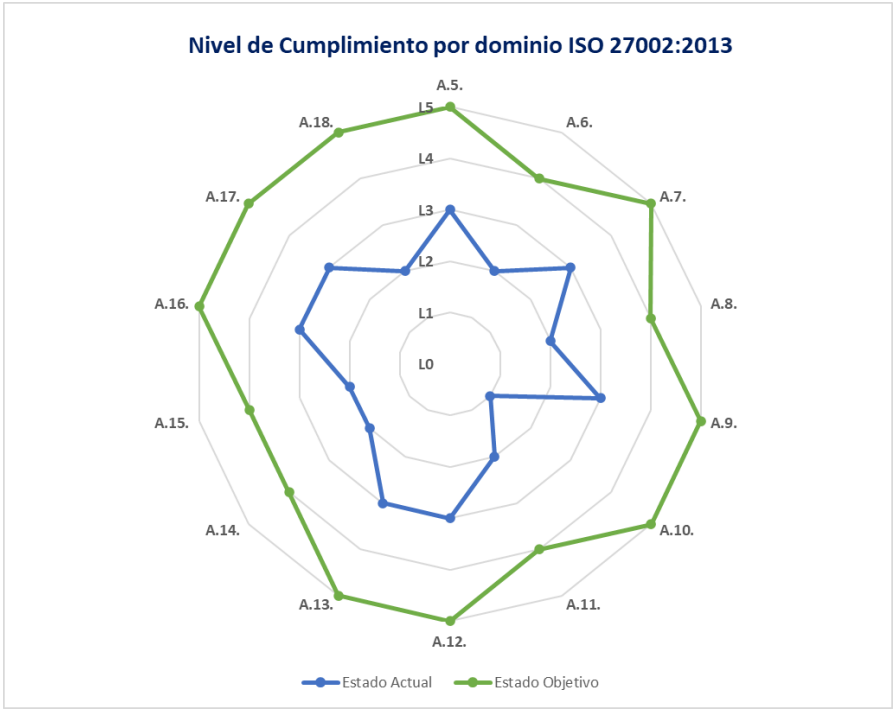

Figura 18 *Nivel de cumplimiento por dominio*

Con base en los resultados obtenidos, se evidencia que existe un gran porcentaje de controles en niveles de poca madurez, lo cual representa una brecha de seguridad para la empresa, ya que a pesar de tener implementados controles aún existen vacíos que exponen a la empresa a la materialización de incidentes de seguridad de la información que puedan generar un impacto severo en cuanto a la operación y reputación de esta.

Los resultados detallados de la auditoría se relacionan en el Anexo 6. Informe de Auditoría Controles ISO27002. De igual forma, en el Anexo 7. Evaluación Madurez, se relaciona el detalle de la calificación dada a cada control con base en los resultados de la auditoría.

7. Conclusiones

Una vez finalizado el trabajo y desarrollados los objetivos planteados se han llegado a las siguientes conclusiones:

- Con base en los resultados del análisis de riesgos de seguridad de la información se identificó la necesidad de implementar un modelo cloud que mejore la postura de seguridad en la plataforma tecnológica de la empresa, por lo cual, se definió el proyecto “Implementación de controles de seguridad y actualización tecnológica holística para la protección de los sistemas de información de la compañía y la eficiente prestación de los servicios”. Así mismo, con la implementación de dicho proyecto se da cumplimiento al objetivo de separar las redes de la empresa. Por lo anterior se evidencia que a lo largo del desarrollo del Plan Director se generó conciencia al interior de la empresa, por lo cual se asignado recursos humanos y económicos para la mejora de las condiciones de seguridad de la información en la empresa.

- El Plan Director fue ejecutado de acuerdo con la planificación definida. Se dio cumplimiento a cada una de las fases dentro de los tiempos establecidos y siguiendo la metodología planteada. Los resultados de cada una de las fases permitieron identificar acciones de mejora que al ser implementadas darán cierre a las brechas de seguridad de la información actuales de la empresa. A lo largo del desarrollo del Plan Director se contó con la participación de diferentes personas de la empresa que están involucradas en la gestión de seguridad de la información.

- Con las actividades desarrolladas como parte del Plan Director se establecieron bases como la política de seguridad de la información, el comité de seguridad, la metodología de auditoría, la metodología de riesgos de seguridad de la información, indicadores y la declaración de aplicabilidad, lo cual refleja el compromiso por parte de la empresa al gestionar su desarrollo e implementación. Así mismo, lo anteriormente definido permite la mejora continua del sistema de gestión de seguridad de la información.

- Con el fin de dar total cumplimiento a la implementación del sistema de gestión de seguridad de la información, se requiere definir proyectos futuros orientados a la identificación, documentación y clasificación de los activos de información, de igual forma, es necesario trabajar en la definición de planes de capacitación y sensibilización que permitan generar mayor nivel de conciencia de seguridad de la información en todos los empleados.

- A lo largo del desarrollo del Plan Director para la implementación del sistema de gestión de seguridad de la información, se evidenció la importancia de contar con el compromiso de la Alta Dirección ya que se requiere de su aprobación respecto a los lineamientos de seguridad de la información que se deberán cumplir en la empresa y por parte de los interesados, así como, se requiere la asignación de recursos económicos y la asignación de responsabilidades a personas de la empresa para asegurar la correcta gestión de seguridad de la información.

8. Glosario

- **ACTIVO DE INFORMACIÓN:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (información, aplicaciones, servicios, hardware, redes de comunicaciones, personas) que tenga valor para empresa.

- **AMENAZA:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **BASE DE DATOS PERSONALES:** Conjunto organizado de Datos Personales que sea objeto de Tratamiento.

- **CONFIDENCIALIDAD:** La confidencialidad es una característica que se aplica a la información. Proteger y preservar la confidencialidad de la información significa garantizar que no esté disponible o se da a conocer a entidades/personas/procesos no autorizadas.

- **CONTROL:** Salvaguarda o contramedida para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. En una definición más simple, es una medida que modifica el riesgo. (ISO/IEC 27000).

- **CONTROL DE ACCESO:** El control de acceso de la información incluye tanto la autorización, como la restricción de los accesos. Se refiere a todas las medidas que se toman para autorizar y restringir selectivamente la entrada, el contacto, o el uso de los activos. Los controles de autorización y restricción se deben establecer de acuerdo con los requerimientos del negocio y de Seguridad de la Información.

- **COPIAS DE SEGURIDAD:** Copia parcial o total de información considerada importante para la Compañía. Información que puede estar almacenada en el disco duro, bases de datos u otro medio de almacenamiento. Las copias de seguridad por lo general se generan en cintas de respaldo, discos duros externos y centros de datos alternos.

- **DISPONIBILIDAD:** La disponibilidad es una característica que se aplica a los activos. Un activo está disponible si es accesible y utilizable cuando es necesitado por una entidad autorizada. Todos los activos deben estar a disposición de las entidades autorizadas cuando dichas entidades requieran acceder o utilizar dichos activos.

- **DUEÑO DEL ACTIVO**: Área o persona (cargo) que tiene la responsabilidad de clasificar un activo de información, autorizar el acceso y velar por que se implementen controles que disminuyan el riesgo por pérdida de la integridad, confidencialidad y

disponibilidad de este. Un propietario es una persona o entidad a la que se ha dado la responsabilidad formal por la seguridad de un activo o una categoría de activos. No significa que el activo pertenece al dueño en un sentido legal.

- **IMPACTO:** Cambio adverso en el nivel de los objetivos del negocio logrados. (ISO/IEC 27005:2008).

- **INCIDENTE DE SEGURIDAD:** Cualquier situación o hecho que genera un daño, afectación o que supone una vulneración a los activos o políticas definidas.

- **INFORMACIÓN:** Se trata del conjunto de datos, añadidos, procesados y relacionados, de manera que pueden dar pauta a la correcta toma de decisiones según el fin previsto.

- **INTEGRIDAD:** Preservar la integridad de la información significa proteger la exactitud y completitud de la información y los métodos que se utilizan para procesarla y gestionarla.

- **INSTALACIONES:** Se define como cualquier servicio, infraestructura o cualquier ubicación física en donde se lleva a cabo el procesamiento de la información o se almacena.

- **PROBABILIDAD:** Oportunidad que algo suceda esté o no definido, medido, determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos generales o matemáticos (cómo la probabilidad numérica o la frecuencia en un periodo determinado) (ISO 31000:2009).

- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. (ISO/IEC 27005:2008).

- **SEGURIDAD DE LA INFORMACIÓN:** Proceso de preservación de la confidencialidad, integridad, y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

- **TRATAMIENTO DEL RIESGO:** Proceso de selección e implementación de medidas para modificar el riesgo. (ISO/IEC 27002:2005).

- **VULNERABILIDAD:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 27002:2005).

9. Bibliografía

- *Fernández Luis, Fernández Pedro. Cómo implantar un SGSI según ISO/IEC27001. ALFAOMEGA AENOR EDICIONES. 1° Edición. 2019*

- *Bravo Mendoza Oscar, Sánchez Celi Marleny. Gestión Integral de Riesgos. Bogotá D.C, 2006*

- *Cano Jeimy José. Manual de un CISO: reflexiones no convencionales sobre la gerencia de la seguridad de la información. Ra-Ma S.A. Editorial y Publicaciones. 1° Edición. 2017*

- *Killmeyer Jan. Information Security Architecture. Auerbach Publications. Bocan Ratón, FL. 2006*

- *ISACA. Manual de preparación para el examen CRISC. 6° Edición. Buenos Aires.*

- *Organización Internacional de Normalización (ISO), Comisión Electrónica Internacional (IEC). ISO/IEC 27001:2013 Information Technology - Security Techniques – Information Security Management Systems – Requirements. Suiza, 2013*

- *Organización Internacional de Normalización (ISO), Comisión Electrónica Internacional (IEC). ISO/IEC 27002:2013 Information Technology - Security Techniques – Code of practice for information security controls. Suiza, 2013*

- *Organización Internacional de Normalización (ISO), Comisión Electrónica Internacional (IEC). ISO/IEC 27005:2011 Information Technology – Security Techniques – Information Security Risk Management. Suiza. 2011*

- *Consejo Superior de Administración Electrónica del Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid. 2012*

10. Anexos

- **Anexo 1. Análisis Diferencial**

  Resultados del análisis diferencial realizado para establecer el estado actual de seguridad de la información respecto a la norma ISO/IEC 27001 y el estándar ISO/IEC 27002.

Anexo 1. Análisis Diferencial.xlsx

- **Anexo 2. Informe de Auditoría**

  Modelo del informe de auditoría el cual deberá ser documentado para cada una de las auditorías definidas dentro del programa de auditoría.

Anexo 2. Informe de Auditoría.docx

- **Anexo 3. Programación auditoría**

  Cronograma de ejecución de la auditoría para revisión de los 114 controles definidos en el estándar ISO 27002.

Anexo 3. Programación Audit

- **Anexo 4. Declaración de aplicabilidad**

  Listado de los 114 controles definidos en el estándar ISO 27002 donde se detalla la justificación de su aplicabilidad, estado actual y documentación relacionada.

Anexo 4. Declaracion Aplicabi

- **Anexo 5. Matriz Activos y Riesgos**

  Matriz de activos de información y evaluación de las amenazas identificadas por categoría de activo.

  Anexo 5. Matriz Activos y Riesgos.xls

- **Anexo 6. Informe de Auditoría Controles ISO27002**
  Informe de la auditoría realizada para la revisión del diseño e implementación de los controles del estándar ISO/IEC 27002:2013.

  Anexo 6. Informe de Auditoría Contro

- **Anexo 7. Evaluación Madurez**

  Resultados de la auditoría realizada para establecer el nivel de madurez de los controles del estándar ISO/IEC 27002:2013.

  Anexo 7. Evaluacion Madurez.xlsx