
 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	1 de 32

Fecha emisión del informe	día	17	mes	06	año	2024
---------------------------	-----	-----------	-----	-----------	-----	-------------

Proceso:	Gestión de Tecnología de la Información y las Comunicaciones
Procedimiento/operaciones.	Implementación del Sistema de Seguridad de la Información
Líder de Proceso: Jefe(s) Dependencia(s):	Ronald Alexis Martin
Nombre del seguimiento:	Diagnóstico a la implementación del Sistema de Seguridad de la Información (ISO 27001:2022).
Objetivo:	<ul style="list-style-type: none"> • Validar el grado de implementación del Sistema de Seguridad de la Información (NTC ISO 27001:2022). • Identificar oportunidades de mejora en el sistema de gestión.
Metodología	<p>Se realizó las siguientes actividades.</p> <ol style="list-style-type: none"> a. Documentación: Se hizo revisión de la documentación que se encuentra publicada tanto en la Sede Electrónica de la entidad, como la Intranet y, Documentos contenidos en el Sistema Integrado de Gestión. b. Instrumento de Evaluación: Aplicación de Instrumento de Evaluación. c. Validar el nivel de aplicación del sistema de seguridad de información en la entidad. d. Entrevistas con el asignado del seguimiento del Sistema de Seguridad de la Información. e. Análisis de brechas: Se realizó verificación del cumplimiento de los requisitos de la norma ISO 27001:2022, para lo cual se adelantó: <ul style="list-style-type: none"> • Identificación y registro de las evidencias en cada requisito estándar. • Asignación de una valoración a cada requisito, según las evidencias identificadas (escala de valoración de cumplimiento). f. Nivel de Implementación: de acuerdo con la valoración de los requisitos de la norma se muestra el resultado obtenido. g. Presentación de Resultados: a medida del avance, se fueron presentando los resultados en cada unos de los numerales de la norma h. Informe de Diagnóstico: Se presentan los resultados obtenidos, así como se presentan las debilidades encontradas, con el fin de que la entidad aplique los correctivos para dar cumplimiento a la norma de Seguridad de la Información.
Limitaciones o riesgos del proceso de seguimiento	Contar con diferentes fuentes de información que no tienen alienada la información revisada.

Asesor de Control Interno	Equipo Evaluador de control interno
----------------------------------	--

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	2 de 32

Doris Yolanda Ramos Vega	Ana Yancy Urbano Velasco
--------------------------	--------------------------

DESARROLLO DEL SEGUIMIENTO (Temas evaluados – Conclusiones)

Como contexto se parte desde el Decreto 1083 de 2015, Decreto único del Sector Función Pública, modificado por el Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión - MIPG, el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno.

El MIPG complementa y se articula con otros sistemas, modelos y estrategias que establecen lineamientos y directrices en materia de gestión y desempeño para las entidades públicas, tales como el Sistema Nacional de Servicio al Ciudadano y el Sistema de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de **Seguridad de la Información**.

Partiendo del anterior apartado, se resume que el MIPG es el corazón y contempla los sistemas de gestión que son adaptados por las entidades públicas, para el caso de la CNMH se describe el Sistema de Gestión de Seguridad de la Información; que apoya a las siete (7) dimensiones, y las 19 políticas que se enmarcan en cada dimensión.

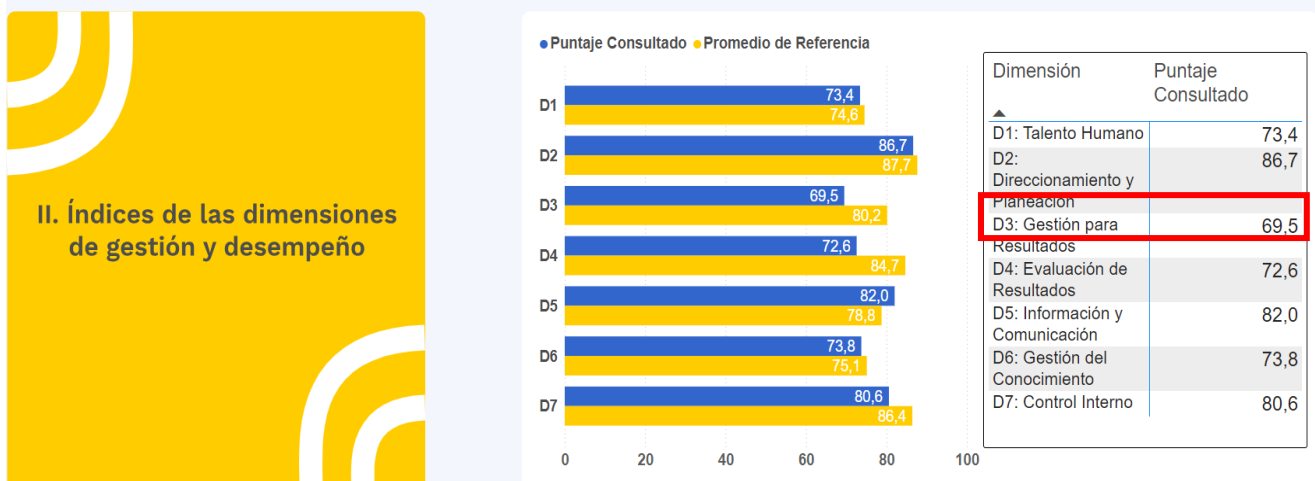
NOTA: Algunas de las políticas que se afectan de manera directa con el Sistema de Gestión de Seguridad de la Información se tiene:

- Talento Humano
- Compras y Contratación Pública (proveedores)
- Gobierno Digital
- Seguridad Digital
- Gestión Documental
- Gestión de la Información Estadística



Ilustración: Del MIPG y el Sistema de Gestión de Seguridad de la Información

De igual manera, se consulta los resultados de la Evaluación del MIPG para la vigencia 2022, de la entidad, la cual muestra los siguientes resultados:



Fuente: consulta resultados FURAG 2022



Observándose que en la tercera Dimensión “Gestión con Valores para Resultados”, que contempla entre las Políticas de Gobierno Digital y Política de Seguridad Digital, es la dimensión con el menor puntaje del FURAG.

I. IMPLEMENTACIÓN DE LA NORMA NTC-ISO-IEC 27001:2022

Cada uno de los requisitos de la ISO/IEC 27001:2022 describe requerimientos específicos, los cuales fueron analizados para identificar el nivel de cumplimiento del estándar. La valoración del cumplimiento se realizó de acuerdo con la siguiente escala:

ESCALA	DESCRIPCIÓN
Cumple	Se cuenta con las evidencias de que la entidad cumple con el requisito.
Cumple Parcialmente	Aunque se evidencian avances en la implementación del requisito, se tienen algunas debilidades que deben ser remediadas para cumplir con el requerimiento.
No Cumple	No se ha iniciado con la implementación de los requisitos o los avances son mínimos.
N/A	Requerimiento no aplica a la entidad

Tabla 1. Escala de Valoración del Cumplimiento de los requisitos

II. NIVEL DE CUMPLIMIENTO DE LOS NUMERALES DE LA NTC ISO/IEC 27001:2022

Los requisitos especificados en los numerales del 4 al 10 son de obligatorio cumplimiento para demostrar conformidad con la Norma ISO/IEC 27001:2022. A continuación, se consolidan los resultados.

NOTA: En el documento de Aplicabilidad de la Entidad, no se menciona que haya excepciones por lo que hace revisión total de la norma.

4.CONTEXTO DE LA ENTIDAD

Este numeral describe los requisitos para comprender el contexto de la Entidad, incluyendo su estructura, objetivos, necesidades y expectativas de las partes interesadas. Esto ayuda a la Entidad a identificar y evaluar los riesgos y oportunidades relevantes para su SGSI.

Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

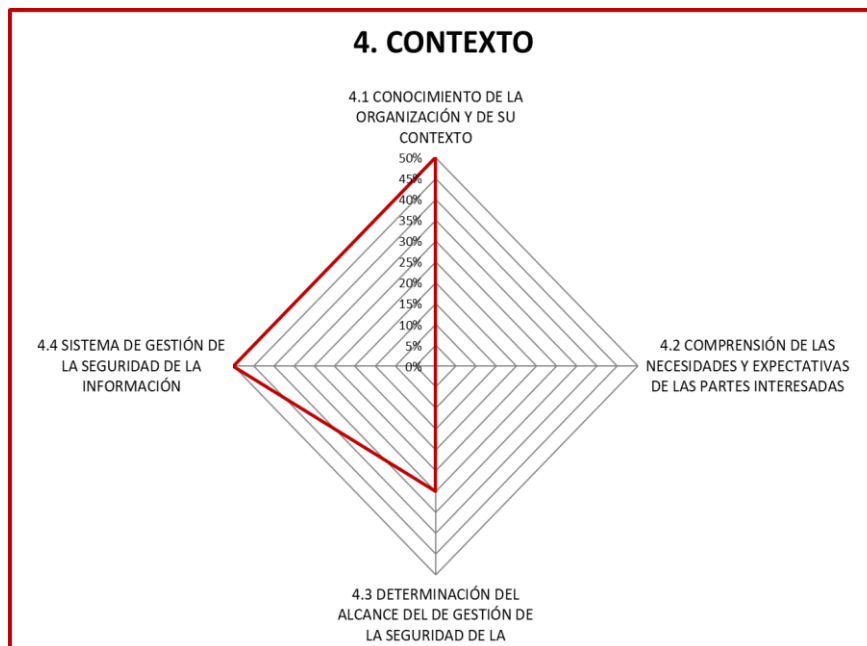
NUMERALES DE LA NORMA	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel deseado
4.1 CONOCIMIENTO DE LA ENTIDAD Y DE SU CONTEXTO	50%	100%



4.2 COMPRESIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	0%	100%
4.3 DETERMINACIÓN DEL ALCANCE DEL DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30%	100%
4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50%	100%
PROMEDIO	33%	100%

Tabla 2. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH – Numeral 4

A continuación se presenta gráficamente el nivel de implementación de los requisitos para el numeral 4 de esta norma:



Gráfica 1. Representa el nivel de implementación de los requisitos -numeral 4

El detalle de la evaluación se presenta en los anexos.

5. LIDERAZGO

Este numeral establece los requisitos de liderazgo y compromiso de la alta dirección para el SGSI. Esto incluye la asignación de roles y responsabilidades, la comunicación de la política de seguridad de la información y el establecimiento de objetivos y planes de mejora continua.

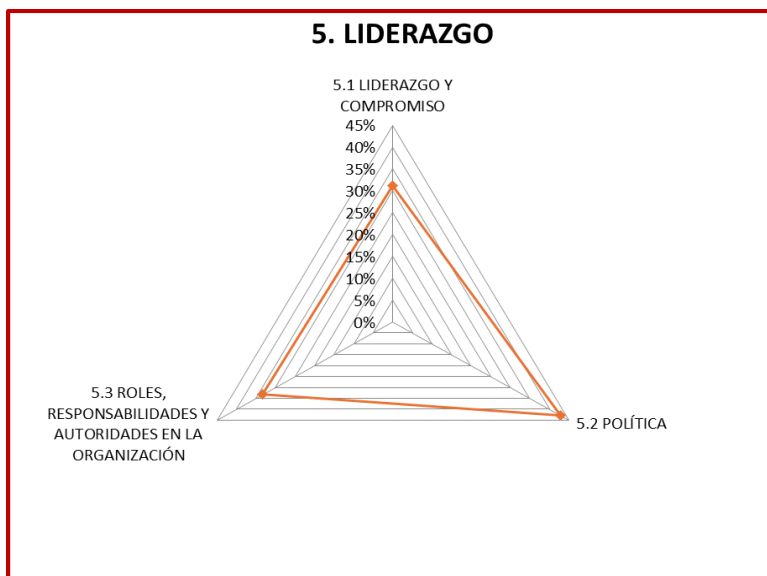


Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

NUMERALES DE LA NORMA	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel deseado
5.1 LIDERAZGO Y COMPROMISO	31%	100%
5.2 POLÍTICA	43%	100%
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ENTIDAD	33%	100%
PROMEDIO AVANCE	36%	100%

Tabla 3. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH – Numeral 5

A continuación se presenta gráficamente el nivel de implementación de los requisitos para el numeral 5 de esta norma:



Gráfica 2. Representa el nivel de implementación de los requisitos -numeral 5

6. PLANIFICACIÓN

Describe los requisitos para planificar el SGSI, incluyendo la identificación y evaluación de riesgos y oportunidades, la definición de objetivos y requisitos de seguridad, la selección de controles de seguridad y la elaboración de planes de implementación.

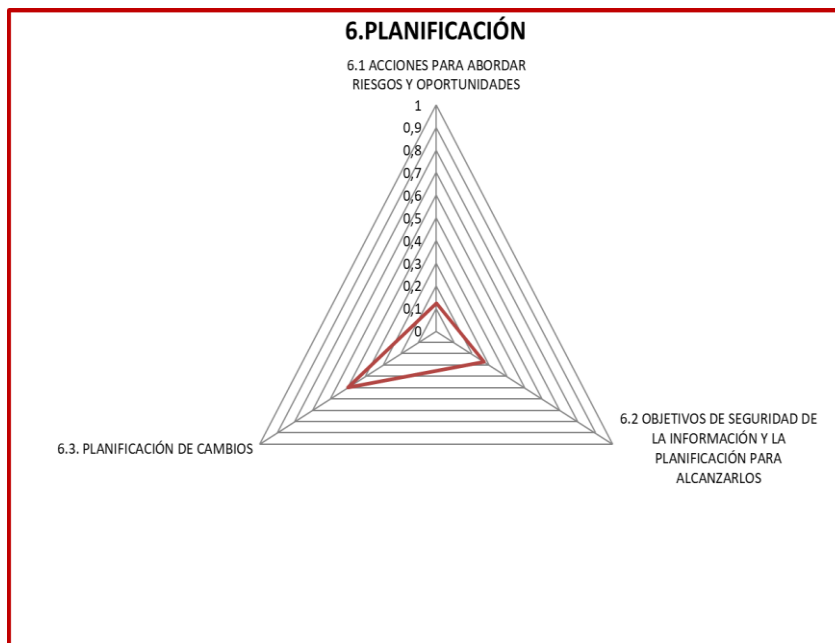


Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

NUMERALES DE LA NORMA	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel Deseado
6.1 ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES	12%	100%
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y LA PLANIFICACIÓN PARA ALCANZARLOS	27%	100%
6.3. PLANIFICACIÓN DE CAMBIOS	50%	100%
PROMEDIO AVANCE	30%	100%

Tabla 4. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH – Numeral 6

A continuación se presenta gráficamente el nivel de implementación de los requisitos para el numeral 6 de esta norma:



Gráfica 3. Representa el nivel de implementación de los requisitos -numeral 6

7. SOPORTE



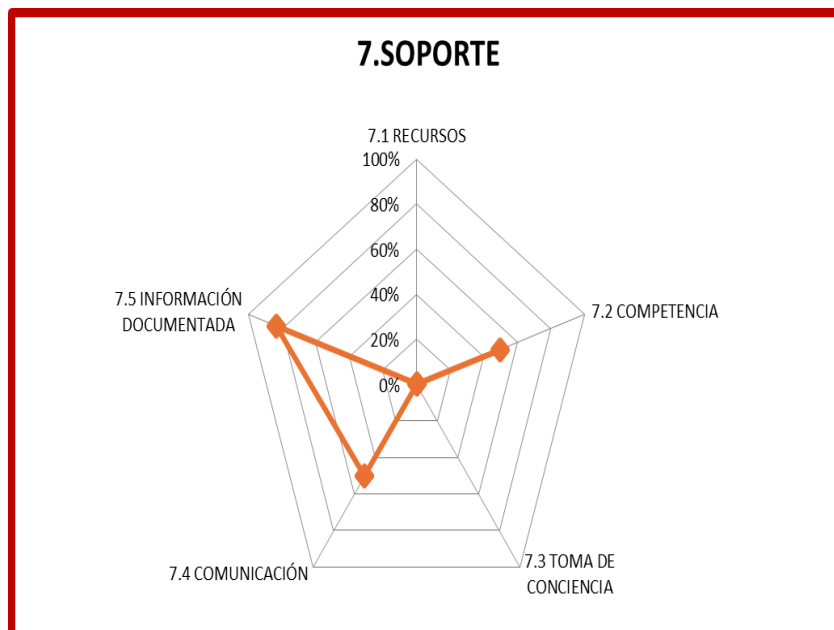
Para este numeral se establece los requisitos para los recursos necesarios para la implementación y mantenimiento del SGSI, incluyendo el personal, la infraestructura y los recursos financieros. También incluye requisitos para la competencia, la toma de conciencia y la comunicación en la Entidad.

Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

RESUMEN NUMERAL	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel Deseado
7.1 RECURSOS	0%	100%
7.2 COMPETENCIA	50%	100%
7.3 TOMA DE CONCIENCIA	0%	100%
7.4 COMUNICACIÓN	50%	100%
7.5 INFORMACIÓN DOCUMENTADA	83%	100%
PROMEDIO AVANCE	37%	100%

Tabla 5. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH – Numeral 7

A continuación se presenta gráficamente el nivel de implementación de los requisitos para el numeral 7 de esta norma:



Gráfica 4. Representa el nivel de implementación de los requisitos -numeral 7



8. OPERACIÓN

Refiere a los requisitos para la implementación y operación del SGSI, incluyendo la gestión de riesgos, la seguridad de la información, el control de acceso, la continuidad del negocio y otros controles de seguridad. También se incluyen requisitos para la documentación y el control de los registros.

Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

RESUMEN NUMERAL	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel Deseado
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL	0%	100%
8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	50%	100%
8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	50%	100%
PROMEDIO AVANCE	33%	100%

Tabla 6. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH — Numeral 8

A continuación se presenta gráficamente el nivel de implementación de los requisitos para el numeral 7 de esta norma:





Gráfica 5. Representa el nivel de implementación de los requisitos -numeral 8

9. EVALUACIÓN DE DESEMPEÑO

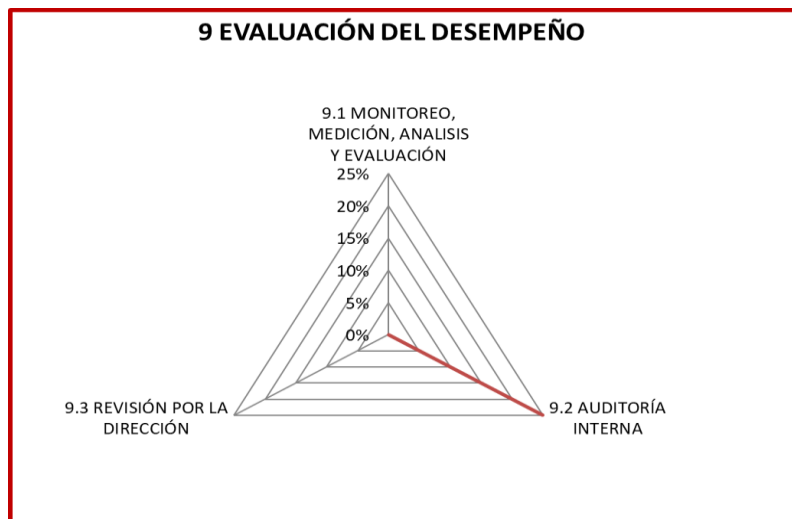
Establece los requisitos para monitorizar, medir, analizar y evaluar el desempeño del SGSI. Esto incluye la realización de auditorías internas, revisiones de gestión y evaluaciones de la conformidad con la norma. También se incluyen requisitos para la mejora continua del SGSI.

Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

RESUMEN NUMERAL	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel Deseado
9.1 MONITOREO, MEDICIÓN, ANALISIS Y EVALUACIÓN	0%	100%
9.2 AUDITORÍA INTERNA	25%	100%
9.3 REVISIÓN POR LA DIRECCIÓN	0%	100%
PROMEDIO AVANCE	8%	100%

Tabla 7. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH - – Numeral 9

A continuación se presenta gráficamente el nivel de implementación de los requisitos para el numeral 9 de esta norma:



Gráfica 6. Representa el nivel de implementación de los requisitos -numeral 9



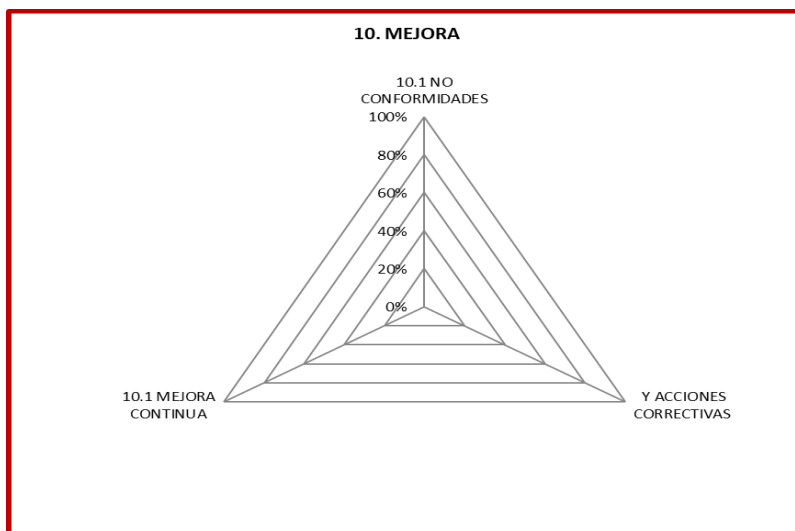
10. MEJORA

Se define como acciones que se traducen en una mejora de los resultados, así que apoya a la identificación y realización de cambios enfocados a conseguir la mejora del rendimiento y resultados de la entidad. La mejora continua es un concepto que es fundamental para las teorías y programas de gestión de la calidad y de la seguridad de la información. La mejora continua es clave para la gestión de la seguridad de la Información

Una vez aplicado el instrumento de evaluación se obtuvo los siguientes porcentajes de aplicación.

RESUMEN NUMERAL	NIVEL DE IMPLEMENTACIÓN	
	Nivel Actual	Nivel Deseado
10.1 MEJORA CONTINUA	0%	100%
10.2 NO CONFORMIDAD Y ACCIÓN CORRECTIVA	0%	100%
PROMEDIO AVANCE	0%	100%

Tabla 8. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH — Numeral 10



Gráfica 7. Representa el nivel de implementación de los requisitos -numeral 10

ANEXO A

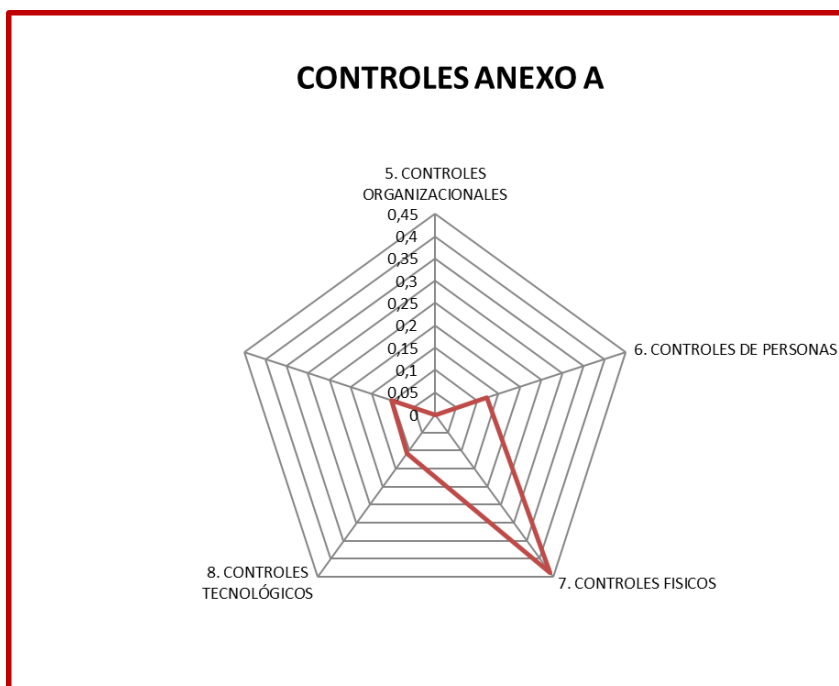
En este apartado, se describen los controles que se tienen dispuestos por la norma para el sistema de gestión de



seguridad de la información, que las entidades deben adoptar e implementar.

CAPÍTULOS	NIVEL DE IMPLEMENTACIÓN	
	NIVEL ACTUAL	NIVEL DESEADO
5. CONTROLES ORGANIZACIONALES	12%	100%
6. CONTROLES DE PERSONAS	44%	100%
7. CONTROLES FISICOS	11%	100%
8. CONTROLES TECNOLÓGICOS	10%	100%
PROMEDIO	19%	100%

Tabla 9. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH – Anexo A



Gráfica 8. Representa el nivel de implementación de los requisitos -Anexo A

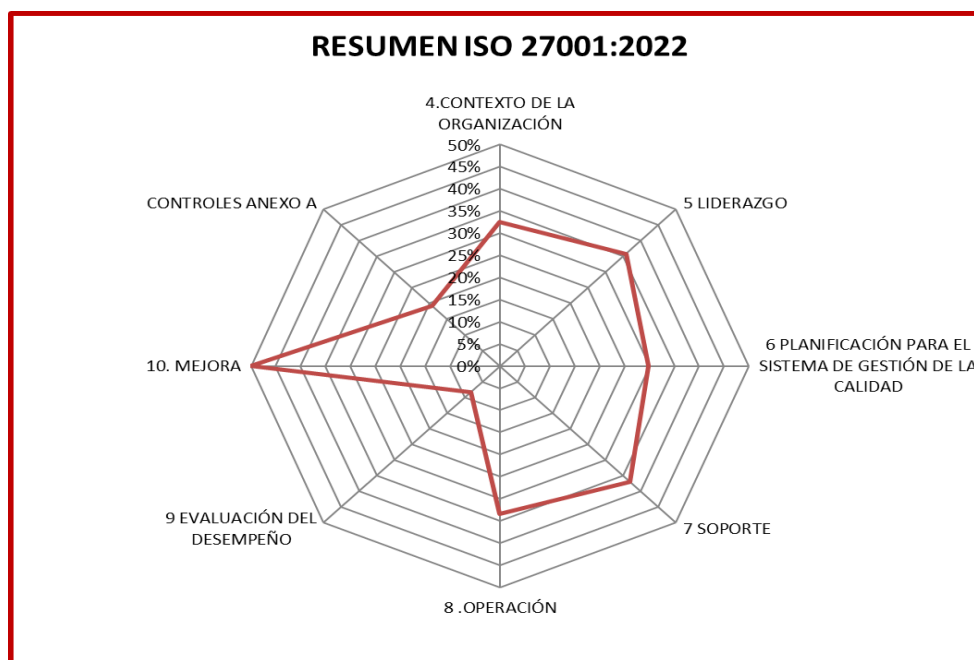


CONCLUSIONES


En el Diagnóstico adelantado para el Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001:2022, arroja los siguientes resultados de manera consolidada por numeral:

NUMERALES DE LA NORMA	% IMPLEMENTACIÓN
4.CONTEXTO DE LA ENTIDAD	33%
5 LIDERAZGO	36%
6 PLANIFICACIÓN PARA EL SISTEMA DE GESTIÓN DE LA CALIDAD	30%
7 SOPORTE	37%
8 .OPERACIÓN	33%
9 EVALUACIÓN DEL DESEMPEÑO	8%
10. MEJORA	50%
CONTROLES ANEXO A	19%
TOTAL GENERAL	31%

Tabla 9. Detalle del nivel de implementación requisitos ISO/OEC 27001:2022- CNMH – resumen numerales y Anexo A



Gráfica 8. Representa el nivel de implementación de los requisitos de todos los numerales

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	14 de 32

Es recomendable ampliar y fortalecer los esfuerzos en el mejoramiento de implementación del Sistema de Seguridad de la Información, así como el fortalecimiento del plan de continuidad de negocio para abordar una variedad más amplia de escenarios de interrupción. Esta mejora contribuirá a una respuesta más eficiente y eficaz ante situaciones de crisis, minimizando el impacto en las operaciones.

Además, se sugiere comprometer esfuerzos con el fin de completar la parte documental de los requisitos exigibles para la norma ISO 27001:2022, lo que permitirá mantener la alineación con las últimas mejores prácticas y requisitos actualizados. Esta actualización asegurará que el sistema de gestión de seguridad de la información sea relevante y robusto en el entorno en constante evolución de la ciberseguridad. En general, la entidad implementará mejoras para enfrentar los desafíos de seguridad de la información y mantener y asegurar la confianza de sus partes interesadas, así como velar por el cumplimiento de los pilares de la seguridad de información (Integridad, Confidencialidad y Disponibilidad).

Por lo anterior, se sugiere implementar un plan de mejora que aborde los puntos que requieren de fortalecimiento para dar cumplimiento a lo descrito en la norma ISO 27001:2022.

**MATRIZ PARA PLAN DE MEJORAMIENTO
(Metodología para elaboración – fecha de entrega)**

No	DESCRIPCION DEL HALLAZGO	RECOMENDACION

PLAN DE MEJORAMIENTO Y/O ACCIONES DE MEJORA


Basados en los resultados obtenidos del Diagnóstico del Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001:2022, se debe formular el respectivo plan de mejoramiento a fin de fortalecer y mejorar este sistema, teniendo en cuenta lo descrito en el presente informe, así:

4.CONTEXTO DE LA ENTIDAD:

- **Conocimiento de la Entidad y de su contexto**

El CNMH debe determinar las problemáticas externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA: La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	15 de 32

Entidad, considerado en el numeral 5.4.1 de la NTC-ISO 31000:2018 (*Comprensión de las Organizaciones y su contexto*)

Revisada la información se observó:

- ✓ En el texto descrito del contexto de la entidad consultado en las fuentes: a) Plan Estratégico 2022-2026 Centro Nacional de Memoria y, b) Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002; c) Página Web, y d) Intranet. A este contenido se debe integrar lo referente a la seguridad de la información para el conocimiento de los usuarios y partes interesadas. De igual manera, no se observó que describa las cuestiones (problemáticas externas e internas) que pueden afectar el sistema.
- ✓ En lo que respecta a Visión y Misión, se debe actualizar dado que en la página web, como la Intranet se presenta información diferente, versus la información contenida en "Plan estratégico 2022-2026 de la entidad"

- **Comprensión de las necesidades y expectativas de las partes interesadas**


La entidad debe determinar:

- a. Las partes interesadas que son relevantes al sistema de gestión de la seguridad de la información; y
- b. Los requisitos relevantes de estas partes interesadas
- c. Cuales de estos requisitos pueden ser abordados a través del sistema de gestión de seguridad de la información

NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.

Dentro de la información consultada:

- ✓ Estrategia de Cultura y Apropiación de TI 2023, publicado en la web <https://centrodememoriahistorica.gov.co/wp-content/uploads/2023/04/Estrategia-de-cultura-y-apropiacion.pdf>, se menciona las partes interesadas internas.
- ✓ En la sede electrónica/Transparencia/ 8, Información Específica para Grupos de Interés, en este link se encuentra la Información para niños, niñas y adolescentes; Información para mujeres, Información para grupos étnicos.
- ✓ Manual del Sistema Integrado de Gestión V9, numeral 3, Partes Interesadas en el accionara del CNMH se describe que son: Víctimas y organizaciones de víctimas, Organizaciones sociales y de derechos humanos, Academia y centros de pensamiento, Otras entidades del Estado (Orden Nacional y Territorial), Personas desmovilizadas, Sociedad en su conjunto.
<https://intranet.centrodememoriahistorica.gov.co/visorpdf.php?id=577&pdf=1>

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	16 de 32

Por lo anterior, se debe construir un documento donde se describa de las partes interesadas:

- Cuales pueden afectar el Sistema de Gestión de Seguridad de la Información
- Incluir los requisitos legales y reglamentarios, como los contractuales.
- las problemáticas externas e internas

- **Determinación del alcance del de gestión de la seguridad de la información**

La Entidad debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, se debe considerar:

- a. Las problemáticas externas e internas referidas en el contexto.
- b. Los requisitos referidos en las necesidades y expectativas de las partes interesadas.
- c. Las interfaces y dependencias entre las actividades realizadas por la Entidad, y las que realizan otras organizaciones.

El alcance debe estar disponible como información documentada.

Una vez revisada la documentación se encontró que:

En el **Manual del Sistema de Gestión de Seguridad de la Información**

- En el alcance se describe los procesos misionales:
 - Acuerdos de la Verdad
 - Difusión de la Memoria Histórica
 - Gestión de Investigaciones
 - Registro Acopio y Procesamiento
 - Servicios Información, Archivo y Colecciones
- Procesos de Soporte:
 - Gestión de Talento Humano
 - Gestión de las TIC

Al observar el mapa de procesos de la entidad, allí no se describen los procesos: a) Acuerdo de la Verdad; b) Gestión de Investigaciones; c) Registro Acopio y Procesamiento; y, d) Servicios Información, Archivo y Colecciones. Por lo cual requiere que este documento sea actualizado.

Se debe describir en algún instrumento de la entidad, las interfaces que deban ser contempladas tanto en el interior de la entidad como con otras organizaciones.

- **Sistema de Gestión de la Seguridad de la Información**

La Entidad debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la



seguridad de la información, de acuerdo con los requisitos de esta norma.

Dentro de lo revisado, no se observó que se haya realizado la implementación de todos sus requisitos, así como la mejora continua del Sistema, por lo que se deben implementar esfuerzos adicionales para dar cumplimiento a lo requerido.

Por otra parte, se observó:

- Plan Estratégico de Tecnologías de la Información PETI 2024, en este documento no se referencia la Norma NTC ISO 27001.
- Se debe velar por la articulación de los documentos que soportan el Sistema de Seguridad de la Información y/o que se encuentran por definir para dar cumplimiento a este numeral, que todos se encuentren alineados y actualizados, tal y como se observó en el Sistema Integrado de Información
- Al consultar el documento “Manual de Seguridad de la Información, por las dos fuentes resaltadas en la siguiente imagen, se observan que se visualizan versiones diferentes del Manual uno de la Vigencia 2014 y otro de la Vigencia 2021; por lo que se requiere unificar.

Proceso Estratégico

Mostrar 10 registros Filtrar Búsqueda:

Listado de subcategorías

#	Nombre	Descripción
1	A- Gestión Ambiental	Documentos Gestión Ambiental
2	I - Gestión de Seguridad de la Información	Documentos Gestión de seguridad de la información
3	Q - Modelo Operación por Procesos	Documentos Modelo de Operación por Procesos
4	SST- Seguridad y Salud en el trabajo	Documentos Gestión de Seguridad y Salud en el Trabajo

Mostrando 1 a 4 de 4 registros Anterior 1 Siguiente


Mostrar 10 registros Filtrar Búsqueda:

Listado de archivos

No	Archivo	Tamaño	Fecha	Opciones
1	SIP-MA -004 v1 Manual Buenas Prácticas Ambientales	627.5 KBytes	21/04/2022	Ver archivo
2	(Q) SIP-MA-001 v10 Manual del Sistema Integrado de Gestión	727 KBytes	26/04/2024	Ver archivo
3	(Q-I SST) SIP-PO V4 Administración del Sistema Integrado de Gestión.	241.1 KBytes	26/02/2021	Ver archivo
4	(Q) SIP-PR-001 Elaboración, Actualización o Anulación de la información documentada. v5	553.6 KBytes	09/02/2021	Ver archivo
5	(Q) SIP-PR-007 v6 Administración de riesgos.	432.3 KBytes	22/01/2024	Ver archivo
6	(Q) Mapa de riesgos Institucional	341.1 KBytes	20/05/2024	Descargar este archivo
7	(Q) SIP-FT-004 Listado Maestro de Control de Información Documentada V3	127.7 KBytes	29/11/2018	Descargar este archivo
8	(Q) SIP-FT-001 V3 Acta	66.2 KBytes	10/08/2018	Descargar este archivo
9	(Q) SIG-FT-022 V1 Formulario Instructivo	65.7 KBytes	30/06/2016	Descargar este archivo
10	(I) SIP-MA-002 v2 Manual sistema gestión seguridad información	642.8 KBytes	07/12/2021	Ver archivo

Mostrando 1 a 10 de 82 registros Anterior 1 2 3 4 5 ... 9 Siguiente

Imagen. Consulta de Sistema Integrado de Información

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	18 de 32

5. LIDERAZGO

- **Liderazgo y compromiso**


La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información así:

- asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la entidad;
- asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la entidad;
- asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;
- comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información;
- asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos;
- dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;
- promoviendo la mejora continua, y
- apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

Al hacer la revisión de la documentación se observó que:

- ✓ Se encontró poca documentación lo referente al Liderazgo y compromiso de la Alta Dirección, por lo tanto, se encuentra debilidades en:
 - Se describen políticas de seguridad de la información; sin embargo, se debe hacer una introducción que enmarque la misionalidad, y a quienes impacta (partes internas y externas). Adicional, se deben revisar los objetivos trazados en este sistema con el fin de poderles medir y hacer seguimiento.
 - No se observa que se haya realizado seguimiento a los resultados del sistema de seguridad de la Información.
 - Falta realizar socializaciones e interiorización del tema de Seguridad de la Información en todos los niveles de la entidad
 - Desde la Alta dirección, se deben generar acciones para que se mejore todo lo relacionado con el Sistema de Seguridad de la Información
 - Se debe mejorar los roles y definir los responsables, con sus obligaciones frente al cumplimiento del Sistema de Seguridad de la Información, con el fin de contribuir a la mejora continua y asegurar la información que impacta en la misionalidad y operatividad de la entidad.

- **Política:**

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	19 de 32

La alta dirección debe establecer una política de la seguridad de la información que:

- a) sea adecuada al propósito de la Entidad;
- b) incluya objetivos de seguridad de la información y la planificación para alcanzarlo o que proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información;
- c) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; y
- d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de la seguridad de la información debe:

- e) estar disponible como información documentada;
- f) comunicarse dentro de la Entidad; y
- g) estar disponible para las partes interesadas, según sea apropiado

Al revisar la documentación existente, se observa que:

- ✓ Se deben articular todos los documentos y relacionarlos desde el manual del Sistema de Gestión de Seguridad de la Información con los demás instrumentos que se quieran crear para apalancar el cumplimiento de la norma ISO 27001 con el fin de tener unidad de información.
- ✓ Definir objetivos que sean alcanzables y medibles
- ✓ Definir en los objetivos quienes, cuando y como se van a ejecutar, así como evaluar su cumplimiento
- ✓ Se debe generar estrategias para la divulgación y conocimiento al interior de la entidad y las partes interesadas, así como su documentación y hacer público a las partes interesadas con el fin de que todos aporten al cumplimiento de la Seguridad de la Información

• Roles, Responsabilidades y Autoridades en la Entidad

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

La alta dirección debe asignar la responsabilidad y autoridad para:

- a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;
- b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la Entidad.

Al revisar la documentación existente, se observa que:

- Si bien en el Manual de Seguridad de la Información, no describe de manera detallada los roles y responsabilidades, por el contrario, se describen de manera general. Es por esto, que deben ser descritos de



manera clara y así que no se pierda la línea de responsabilidad. En el Manual de Sistema Integrado de Gestión, se define que como parte del Sistema de Gestión de Seguridad se tienen los siguientes lineamientos:

- ✓ Política de Transferencia de la Información SIP-PC-011 -Vr 1 de 2016, allí no hay descripción de responsables.
- ✓ Política de Tratamiento de la Información y Datos Personales SIP-PC-015 v3. En el numeral VIII, indica que el Área Responsable de la Atención de Peticiones, Consultas y Reclamos se encuentra a cargo de la Dirección Administrativa y Financiera del Centro Nacional de Memoria Histórica (actualizar, rectificar, suprimir datos)
- ✓ Política de Gobierno Digital SIP-PC-016 versión 1 de 2019. Se indica que declara que todos los funcionarios y contratistas son responsables de ejecutar esta política, pero no hay responsabilidades definidas como quien la lidera.
- ✓ Política de seguridad y privacidad de la información (SIP-PC-013); este documento no fue ubicado en el Sistema Integrado de Gestión de la entidad; es por ello que se recomienda actualizar este manual o en su efecto generar el documento relacionado.

- Procedimiento de Gestión de Roles y Privilegios - SIP-PR-009 versión 9 de fecha 2016, este documento habla de los accesos a usuarios y accesos no autorizados a los sistemas y servicios de CNMH; pero en tema de roles y responsabilidades no detalla mayor información.

Se requiere que se unifique en un solo instrumento las diferentes responsabilidades de la adopción al sistema de Seguridad de la Información. Se observan varios documentos con la asignación de responsabilidades del sistema de seguridad.

Ahora bien, en el Manual del Sistema de Gestión de Seguridad de la Información, se indica que “[...]Se define que el SGSI estará dentro de la Oficina Asesora de Planeación y contará con un profesional encargado de la Seguridad de la Información que será el responsable por este sistema [...]”; sin embargo, al indagar con el Grupo de Planeación sobre este profesional, nos informan que la documentación relacionada con la Seguridad de la Información se encuentra asociados al Proceso de TIC. Por lo anterior, es prioritario que se determine quien será el responsable del Sistema y por lo consecuente se actualicen los documentos frente a este punto.

Al no tener una cabeza visible de este sistema, no se observa que se haya reportado el desempeño del sistema de seguridad de la información, de igual manera no se cuenta con evidencia de sobre esta actividad.

6. PLANIFICACIÓN PARA EL SISTEMA DE GESTIÓN DE LA CALIDAD

- **Acciones para abordar riesgos y oportunidades**

La entidad debe considerar las problemáticas referidas en el numeral “4.1. *Conocimiento de la Entidad*” y, “4.2 *Comprensión de las necesidades y expectativas de las partes interesadas*” con el fin de poder determinar los riesgos y oportunidades de tal manera que:



- a) asegurarse de que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos;
- b) prevenir o reducir efectos indeseados; y
- c) lograr la mejora continua.
- d) La Entidad debe planificar:
- e) las acciones para tratar estos riesgos y oportunidades; y
- f) la manera de:
 - 1) integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información,
 - 2) evaluar la eficacia de estas acciones.


Al revisar la documentación, no se encontró en ninguno de los documentos que se haya abordado este tema; por lo que se requiere sea documentado y puesto en producción para asegurar que se definan los riesgos respectivos del Sistema.

- **Apreciación de riesgos de la seguridad de la información**

La entidad debe definir y aplicar un proceso de apreciación de riesgos de la seguridad de la información que:

- a) establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan:
 1. Los criterios de aceptación de riesgos; y
 2. los criterios para ejecutar la apreciación de riesgos de la seguridad de la información;
- b) asegure que las apreciaciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables;
- c) identifique los riesgos de la seguridad de la información:
 1. aplicar el proceso de apreciación de riesgos de la seguridad de la información para identificar los
 2. riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información; e
 3. identificar a los dueños de los riesgos;"
- d) analice los riesgos de la seguridad de la información:
 1. Apreciar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados de la Seguridad de la Información, es decir: *"aplicar el proceso de apreciación de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información"*
 2. Apreciar la probabilidad realista de que ocurran los riesgos identificados anteriormente.
 3. determinar los niveles de riesgo.
- e) evalúe los riesgos de seguridad de la información:
 1. comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en los criterios de aceptación del riesgo y criterios de apreciación de los mismos.
 2. priorizar los riesgos analizados para el tratamiento de riesgos.

Por lo anterior, la entidad debe contar con información documentada acerca del proceso de apreciación de

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	22 de 32

riesgos de la seguridad de la información; en la actualidad se adolece esta información.

- **Tratamiento de riesgos de la seguridad de la información**

La entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para:

- seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la apreciación de riesgos;
- determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información;

NOTA La entidad puede diseñar los controles necesarios, o identificarlos de cualquier fuente.

- comparar los controles determinados y necesarios para la implementar las opciones escogidas para el tratamiento de los riesgos de la seguridad de la información, así como los controles descritos en el Anexo A, y verificar que no se pasen por alto controles necesarios.

NOTA 2. El Anexo A “Objetivos de control y Controles Referencia” de la Norma ISO 27001, contiene una lista amplia de posibles controles de seguridad de la información. Para lo cual se debe consultar este documento y asegurarse que no se pasen por alto los controles necesarios.

NOTA 3 Los controles de seguridad de la información listados en el Anexo A no son exhaustivos y pueden ser necesarios controles de seguridad de la información adicionales.


- producir una declaración de aplicabilidad que contenga:
 - los controles necesarios
 - la justificación de las inclusiones,
 - si es necesaria la implementación de controles de seguridad de la información o no, y
 - la justificación para la exclusión de los controles del Anexo A;
- formular un plan de tratamiento de riesgos de la seguridad de la información; y
- obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información.

La entidad debe controlar la información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.

NOTA El proceso de apreciación y tratamiento de riesgos de la seguridad de la información se debe alinear con los principios y directrices genéricas suministradas en la ISO 31000

La entidad cuenta con el “Procedimiento Administración del Riesgo--SIP-PR-007 de fecha 22/01/2024”, este documento cuenta con la definición de Riesgo de Seguridad de la Información, sin embargo, debe incluir el manejo que se debe aplicar a los riesgos de seguridad de la información identificados en la entidad, su respectiva apreciación y tratamiento a seguir, con el fin de contar con un lineamiento claro a seguir.

En cuanto al documento de Aplicabilidad, se debe cambiar el título de “Observaciones” por Justificación de la

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	23 de 32

Inclusión, adicional le falta que se describa si requiere aplicarse un control diferente al descrito en el Anexo A.

- **Objetivos de seguridad de la información y la planificación para alcanzarlos**

La entidad debe establecer los objetivos de seguridad de la información en las funciones y niveles relevantes. Los objetivos de seguridad de la información deben:

- ser coherentes con la política de seguridad de la información;
- ser medibles (si es posible);
- tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la apreciación y del tratamiento de los riesgos;
- ser comunicados; y
- ser actualizados, según sea apropiado.
- esta como información documentada

La entidad debe tener la información documentada sobre los objetivos de la seguridad de la información. Así como cuando se hace la planificación para alcanzar los objetivos de la seguridad de la información, la Entidad debe determinar:


- lo que se va a hacer;
- que recursos se requerirán;
- quién será responsable;
- cuando se finalizará; y
- cómo se evaluarán los resultados.

Si bien se cuenta con el Manual del Sistema de Gestión de Seguridad de la Información y en su numeral 5.2. *Objetivos del SGSI*; estos deben ser alineados frente a la política que se determine, no todos los objetivos descritos allí son medibles, de otra parte, no se observa que recursos se tienen, quien es el responsable de cada objetivo y como se evaluarán los resultados.

- **Planificación de cambios**

Cuando la entidad determine la necesidad de cambios en el sistema de gestión de seguridad de la información, los cambios deben ser llevados a cabo de manera planeada.

Al revisar el documento “Plan de Continuidad del Negocio TIC - GTC-PR-006 V1 de fecha 30/01/2014”, en este no hace referencia a los cambios que pueda surgir por el tema de Seguridad de la Información en la entidad, es por ello, que debe contarse con un instrumento que refleje lo que pueda aplicar la entidad ante algún cambio que sufra el Sistema de Seguridad de la Información.

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	24 de 32

7. SOPORTE

- **Recursos**

La Entidad debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

La entidad en su Manual del Sistema de Seguridad de la Información SIP-MA-0002 versión 002, en su Numeral 9.1.1. Soporte, tiene un ítem de “Recursos”; que lo menciona de manera general; sin embargo, no se observa que se determinen recursos para el sistema de seguridad de la información (establecimiento, implementación, mantenimiento y mejora continua). Siendo este un punto de partida importante para establecer y mantener un sistema de seguridad de información en cualquier entidad. Por lo anterior, la entidad debe proveer de recursos financieros y recursos humanos para lograr una adecuada implementación del Sistema de Gestión de Seguridad de la Información.

- **Competencia**

La Entidad debe:

- determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, y
- asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;
- cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y
- conservar la información documentada apropiada, como evidencia de la competencia.


NOTA: Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

En los documentos revisados no se observa que se detalle la competencia de las personas que vayan a liderar el sistema de seguridad de la información; así mismo en entrevista con el profesional de la Dirección de Administrativa y Financiera, indica que esto no se tiene descrito en la entidad. Es importante, contar con un equipo que tenga las competencias para mantener el sistema de seguridad de la información.

- **Toma de Conciencia**

Las personas que realizan el trabajo bajo el control de la entidad (empleados públicos, contratistas) deben tomar conciencia de:

- la política de la seguridad de la información;
- su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	25 de 32

- beneficios de una mejora del desempeño de la seguridad de la información; y
- c) las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.

En los documentos revisados no se observa que se adelante haga de manera exhaustiva una toma de conciencia al interior de la entidad sobre el sistema de seguridad de la información; por lo que se hace necesario desde la Alta Dirección impartir directrices sobre el asunto, con el fin de contribuir al sistema de seguridad de la información.

- **Comunicación**

La entidad debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

- a) el contenido de la comunicación;
- b) cuándo comunicar;
- c) a quién comunicar;
- d) quién debe comunicar; y
- e) los procesos para llevar a cabo la comunicación.

Si bien, la entidad cuenta con instrumentos generados desde el proceso de “Comunicación Interna”; se debe generar un plan de comunicaciones para el Sistema de Seguridad de la Información que cuente con los anteriores requisitos.

- **Información Documentada**


El sistema de gestión de la seguridad de la información de la Entidad debe incluir:

- a) la información documentada requerida por esta Norma; y
- b) la información documentada que la entidad ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA: El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una entidad a otra, debido a:

- a) el tamaño de la Entidad y a su tipo de actividades, procesos, productos y servicios,
- b) la complejidad de los procesos y sus interacciones, y
- c) la competencia de las personas."

Si bien se cuenta dentro los documentos el “Manual del Sistema de Gestión de Seguridad de la Información”, este se debe fortalecer, adicional documentar todo lo que se encuentra pendiente para dar cumplimiento a esta norma, y alinearlos con los demás documentos existentes.

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	26 de 32

- **Creación y actualización**

Cuando se crea y actualiza información documentada, la Entidad debe asegurarse de que lo siguiente sea apropiado:

- la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
- el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);
- la revisión y aprobación con respecto a la idoneidad y adecuación.

La entidad cuenta con un procedimiento "*Elaboración, Actualización y Control de Información Documentada*" - Código SIP-PR-001, Versión 005 de fecha 09/02/2021; sin embargo, se observó que muchos de los documentos consultados para soportar el Sistema de Gestión de Seguridad de la Información requieren ser actualización y, otros temas que se han mencionado en este documento se encuentran sin documentar.

8. OPERACIÓN

- **Planificación y control Operacional**


La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en (Acciones para abordar Riesgos y Oportunidades). La Entidad también debe implementar planes para lograr los objetivos de la seguridad de la información.

De igual manera la entidad debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado y controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario. Así como asegurar que los procesos contratados externamente estén controlados.

En los documentos revisados, no se observa que se haya planificado, implementado y controlado las necesidades de los requisitos de sistema de seguridad de la información; así como la determinación de los riesgos y oportunidades de este.

- **Valoración de Riesgos de la Seguridad de Información**

La entidad debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en la

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	27 de 32

apreciación de los riesgos. De igual manera la entidad debe conservar la información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.

Hasta el momento no se ha evidenciado, que la entidad haya realizado o este realizando la valoración de los riesgos de seguridad, es por esto que es importante contar con los instrumentos y lineamiento claros para hacer este ejercicio.

- **Tratamiento de Riesgos de la Seguridad de la Información**

La entidad debe implementar el plan de tratamiento de riesgos de la seguridad de la información, así como conservar la información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.

Al desarrollar esta actividad y documentarla dará cumplimiento de este requisito.

9. EVALUACIÓN DEL DESEMPEÑO

En la revisión adelantada no se observó que se esté dando cumplimiento a:

- **Monitoreo, medición, análisis y evaluación**

La entidad debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información y determinar:


- qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información;
- los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles.

- cuando se debe llevar a cabo el seguimiento y la medición;
- quién debe llevar a cabo el seguimiento y la medición;
- cuando se deben analizar y evaluar los resultados del seguimiento y la medición;
- quién debe analizar y evaluar estos resultados.

La entidad debe conservar esta información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.

Una vez revisada la documentación se observó:

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	28 de 32

Se debe dejar documentado en algún instrumento: a que se le va hacer seguimiento, incluido procesos y controles. Métodos de seguimiento, análisis, evaluación cuando se realizará la medición y seguimiento, quien ejecutará las acciones de seguimiento y medición, cuando se realizará el análisis y evaluación de los resultados.

- **Auditoría interna**

- **Generalidades**

La entidad debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a) es conforme con:

1. los propios requisitos de la Entidad para su sistema de gestión de la seguridad de la información; y
2. los requisitos de esta Norma;

b) esta implementado y mantenido efectivamente

Una vez culminado el ejercicio del diagnóstico de implementación del sistema, y al finalizar el plan de mejora se debe programar un seguimiento a la implementación del sistema, incluyendo la parte documental y socialización al interior de la entidad.

- **Programa de auditoría interna**


La entidad debe planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes.

Adicional debe considerar la importancia de los procesos involucrados y los resultados de las auditorías previas (en caso de existir resultados). Para cumplir lo anterior se debe:

- a) definir los criterios y el alcance de cada auditoría;
- b) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;
- c) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y
- d) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de la auditoría.

Una vez revisada la evidencia, se observó:

Esta actividad se debe programar una vez se cuente con la implementación del sistema, incluyendo la parte

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	29 de 32

documental y socialización al interior de la entidad, con el fin de ir validando el avance en esta materia.

Atendiendo los lineamientos de normas internacionales, la Oficina de Control Interno puede coordinar la programación general de las auditorías, a fin de contar con un panorama completo de los procesos auditores que se llevarán a cabo durante la vigencia.

En cuanto a su ejecución la segunda línea de defensa correspondientes (calidad, seguridad y salud en el trabajo, ambiental, seguridad de la información, entre otros) podrán llevarlos a cabo autónomamente con sus auditores formados en tales temas, o en caso de no contar con personal certificado y competente deben ser contratadas estas auditorías.

- **Revisión por la dirección**


La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la Entidad a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

La revisión por la dirección debe incluir consideraciones sobre:

- a) el estado de las acciones con relación a las revisiones previas por la dirección;
- b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;
- c) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a:
 1. no conformidades y acciones correctivas;
 2. seguimiento y resultados de las mediciones;
 3. resultados de la auditoría; y
 4. cumplimiento de los objetivos de la seguridad de la información;
- d) retroalimentación de las partes interesadas;
- e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y
- f) las oportunidades de mejora continua.

La Entidad debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección, y en ellas relacionar las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

En el ejercicio de revisión, no se obtuvo evidencia de que esto se haya realizado, por lo que se debe implementar estas revisiones con el fin de validar el compromiso de la Alta Dirección con este sistema. Adicional, para futuras revisiones por la Dirección, se deben contemplarse todas las entradas descritas en este numeral. Adicionalmente, se debe dejar documentada, las decisiones tomadas y las oportunidades de mejora y en general los resultados obtenidos de la revisión.

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	30 de 32

10. MEJORA

- **Mejora Continua**

La Entidad debe mejorar continuamente la sostenibilidad, adecuación y efectividad del sistema de gestión de la seguridad de la información.

En el ejercicio de revisión, no se obtuvo evidencia de que se esté realizando actividades para demostrar la mejora en el Sistema de Seguridad de la Información.

- **No Conformidad y Acción Correctiva**

En el momento que se determine una no conformidad, la entidad debe:

a) reaccionar ante la no conformidad, y según sea aplicable

1. tomar acciones para controlarla y corregirla, y
2. hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

1. la revisión de la no conformidad
2. la determinación de las causas de la no conformidad, y
3. la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas, y


e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La Entidad debe conservar información documentada adecuada, como evidencia de:

- f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y
- g) los resultados de cualquier acción correctiva.

Si bien, el proceso de Control Interno tiene definido un instrumento "Formulación Plan de Mejoramiento" - Código CIT-PR-002, Versión 004, de fecha: 10/09/2019", este instrumento se debe fortalecer para que se contemple la eficacia de las acciones que se determinen para un hallazgo; así mismo se debe velar por que se conserve toda la documentación asociada a un hallazgo.

 Centro Nacional de Memoria Histórica	Informe de Seguimiento y/o evaluación	CÓDIGO:	CIT-FT-006
		VERSIÓN:	002
		PÁGINA:	31 de 32

- **ANEXO A**

Este anexo cuenta con cuatro (4) secciones o capítulos así

1. Organizacionales: con 37 controles.
2. Tecnológicos: con 34 controles.
3. Físicos: con 14 controles.
4. De personas: con 8 controles.

Para la versión 2022, se describen 11 nuevos controles en este Anexo A son:

1. Supervisión de la seguridad física.
2. Inteligencia de amenazas.
3. Gestión de la configuración.
4. Eliminación de la información.
5. Enmascaramiento de datos.
6. Prevención de fuga de datos.
7. Seguimiento de actividades.
8. Seguridad de la información para el uso de servicios en la nube.
9. Filtrado web.
10. Configuración segura.
11. Preparación de las TIC para la continuidad del negocio.

Estos al ser nuevos, requieren que se documenten y se implementen de manera adecuada. A continuación, se consolida los resultados por capítulos así:

- ✓ **CONTROLES ORGANIZACIONALES**

Este capítulo cuenta con 37 controles, y como resultado de la aplicación del Diagnóstico se observó que solo se tiene un 12% de implementación, y aunque cuenta con alguna documentación esta debe ser revisada y actualizada para que de el cumplimiento total; de otra parte, se debe documentar aquellos que no se te tienen descritos en algún instrumento. De igual manera, se deben establecer mesas de trabajo con los responsables con el fin de abordar las debilidades y fortalecer aquellas existentes.

- ✓ **CONTROLES DE PERSONAS**

Este capítulo cuenta con 8 controles y como resultado de la aplicación del Diagnóstico se observó que la entidad tiene un 44% de implementación; al igual que el anterior capítulo se debe documentar aquellos que no se te tienen descritos en algún instrumento. De igual manera, se deben establecer mesas de trabajo con los responsables con el fin de abordar las debilidades y fortalecer aquellas existentes.



✓ **CONTROLES FÍSICOS**

Este capítulo cuenta con 14 controles y como resultado de la aplicación del Diagnóstico se observó que la entidad tiene un 11% de implementación; al igual que el anterior capítulo se debe documentar aquellos que no se tienen descritos en algún instrumento. De igual manera, se deben establecer mesas de trabajo con los responsables con el fin de abordar las debilidades y fortalecer aquellas existentes.

✓ **CONTROLES TECNOLÓGICOS**

Este capítulo cuenta con 34 controles y como resultado de la aplicación del Diagnóstico se observó que la entidad tiene un 10% de implementación; al igual que el anterior capítulo se debe documentar aquellos que no se tienen descritos en algún instrumento. De igual manera, se deben establecer mesas de trabajo con los responsables con el fin de abordar las debilidades y fortalecer aquellas existentes.

El detalle de cada uno de los controles los pueden consultar en el anexo adjunto.

ANEXOS

Como anexo de consulta se tiene:

- Instrumento de Evaluación de la ISO 27001

FIRMAS RESPONSABLES

Evaluador:

Ana Yancy Urbano Velasco – Contratista Control
Interno

Vo. Bo.

Doris Yolanda Ramos - Asesor de Control Interno