CORPORACION PARA EL DESARROLLO SOSTENIBLE DEL URABA

CORPOURABA

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MSPI

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

PESI

2022-2025

Revisión enero de 2023

Apartadó, 31 de Enero de 2023

Acta de Aprobación del Comité Institucional de Gestión y Desempeño 100-01-03-01-0002 del 31 de enero del 2023

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN 4
1. OBJETIVO 6
1.1. Objetivos específicos 6
2. ALCANCE DEL PESI 6
3. MARCO NORMATIVO 7
4. Política de Seguridad y Privacidad de la Información 9
5. ANÁLISIS DE LA SITUACIÓN ACTUAL 11
5.1 Análisis de brecha MSIP 11
5.1 Análisis de brecha Transición de IPv4 a IPv6. 13
5.1 Gestión de Información 13
6 ANÁLISIS DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN 14
7 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 14
7.1 Seguridad Del Recurso Humano: 15
7.2 Gestión De Activos: 15
7.3 Control De Acceso: 15
7.4 Criptografía: N/A 15
7.5 Seguridad Física Y Del Entorno: 15
7.6 Seguridad De Las Operaciones: 15
7.7 Seguridad De Las Comunicaciones: 15
7.8 Relaciones Con Los Proveedores: 15
7.9 Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información: 15
7.10 Gestión De Incidentes De Seguridad De La Información: 16
7.11 Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio: 16
7.12 Plan de sensibilización y apropiación del MSPI para toda la entidad. 16
8 ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 16
8.1 Gobierno de SI 16
Organigrama Corporativo 17
Organigrama de SI 18

8.2 Responsable de Seguridad de la Información: 18
8.3 Equipo del Proyecto: 19
9 SEGUIMIENTO Y REVISIÓN DEL MSPI 19
10 PLANIFICACIÓN DE ACTIVIDADES DEL MSPI 21
10.1 Proyección de presupuesto área de SI 24
11. Plan de Comunicaciones del PESI 26
11.1. Alcance 26
11.2. Red de formadores de formadores 27

INTRODUCCIÓN

La seguridad de la información, según ISO/IEC 27001:2013, consiste en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 VERSION 2013, 2013), para lo cual, el proyecto busca dar respuesta a las exigencias que el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, (MinTic), presenta para todas entidades públicas.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse a los siguientes componentes:

TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

TIC para Gobierno Abierto que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

Este documento indica, definiendo plazos anuales, cuáles serán las labores que realizará la entidad con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las actividades para la administración y la seguridad informática pueden clasificarse en varias categorías como son: seguridad funcional, coordinación, documentación, certificación, acreditación, administración de configuraciones de sistemas y de seguridad informática y manejo de riesgos.

Este documento se elabora con el objetivo de orientar a la Corporación para dar cumplimiento con lo solicitado en el Decreto 612 de 2018 y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 1078 de 2015 y los instrumentos para implementar la Estrategia de Gobierno en Línea (Ahora Gobierno Digital), dentro de los cuales se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información.

En el presente documento se adoptó la concepción, metodología, lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC-, que conforman la Estrategia de Gobierno Digital, la cual está soportada en los LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI) [1] y el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN[2].

[1] LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI). Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2018

[2] MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2016.

1. OBJETIVO

Liderar y establecer las estrategias para la gestión de seguridad y privacidad de la Información en CORPOURABA que permitan minimizar los riesgos de pérdida de activos de la información y estén alineadas a la estrategia y modelo integrado de gestión y acordes con las necesidades de la Entidad y los lineamientos del programa de Gobierno Digital.

1.1. Objetivos específicos

El PESI[3] de la CORPORACIÓN PARA EL DESARROLLO SOSTENIBLE DEL URABA –CORPOURABA- cuenta con los siguientes objetivos específicos acordes con las necesidades de la Entidad y las dimensiones de Gobierno Digital:

- Definir las responsabilidades relacionadas con el manejo de la seguridad, durante el transcurso del año en La Corporación.
- Establecer una metodología de gestión de la seguridad clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Garantizar que los usuarios tienen acceso a la información a través medidas de seguridad con la garantía de calidad y confidencialidad.
- Implementar las auditorías externas para identificar las debilidades del sistema y las áreas a mejorar.
- Garantizar la continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Definir el plan para la transición de IPv4 a IPv6 .
- Integración con otros sistemas de gestión (ISO 9001, ISO 14001, SGSST).

2. ALCANCE DEL PESI

El PESI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos que se ejecutan en CORPOURABA y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la Entidad y está articulado de manera global en relación con la seguridad de la información.

[3] Plan Estratégico de las Seguridad de la Información y Comunicaciones (PESI)

3. MARCO NORMATIVO

Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (CONGRESO NACIONAL, 1999).

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. (CONGRESO DE LA, 2014)

Decreto 103 de 2015: Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información. (PRESIDENCIA DE LA, 2015)

Decreto 2609 de 2012: Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica. (MINISTERIO DE, 2012)

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS, 2012)

Ley 1273 de 2009: Ley la cual se crea y se protege el bien jurídico de la información y los datos personales. (CONGRESO D. C.,

Ley 1581 de 2012: Ley Estatutaria por la cual se reglamenta el artículo 15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales. (CONGRESO D. C., http://www.alcaldiabogota.gov.co, 2012).

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. (CONGRESO D. L., 2000)

CONPES 3975: POLÍTICA NACIONAL PARA LA TRANSFORMACIÓN DIGITAL E INTELIGENCIA ARTIFICIAL

CONPES 3995: POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL.

Decreto 620 de 2020, "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

Resolución 1126 de 2021 "Por la cual se modifica la Resolución 2710 de 2017, por la cual se establecen lineamientos para la adopción del protocolo IPv6"

Resolución 1519 del 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”

Resolución 00500 de marzo 10 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”

Decreto 338 de 2022: “"Por el cual se adiciona el Titulo 21 al a parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”

Decreto 767 del 16 de mayo de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"'

4. Política de Seguridad y Privacidad de la Información

La Dirección General de la Corporación para el Desarrollo Sostenible del Urabá –CORPOURABA-, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información –SGSI- buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra Corporación y las políticas de Calidad y del SGSST.

Para CORPOURABA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

El contenido de esta política aplica a la Corporación según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, entes de control y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de CORPOURABA
- Garantizar la continuidad de la corporación frente a incidentes.

CORPOURABA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Corporación, y a los requerimientos regulatorios.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de CORPOURABA:

• CORPOURABA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

• CORPOURABA protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

• CORPOURABA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• CORPOURABA protegerá su información de las amenazas originadas por parte del personal.

• CORPOURABA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• CORPOURABA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• CORPOURABA implementará control de acceso a la información, sistemas y recursos de red.

• CORPOURABA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• CORPOURABA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• CORPOURABA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• CORPOURABA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

5.1 Análisis de brecha MSIP

Apoyados en la herramienta "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" [4] se obtuvieron en el último seguimiento en el mes de junio de 2021, los siguientes resultados de análisis de brecha sobre la efectividad de los controles:

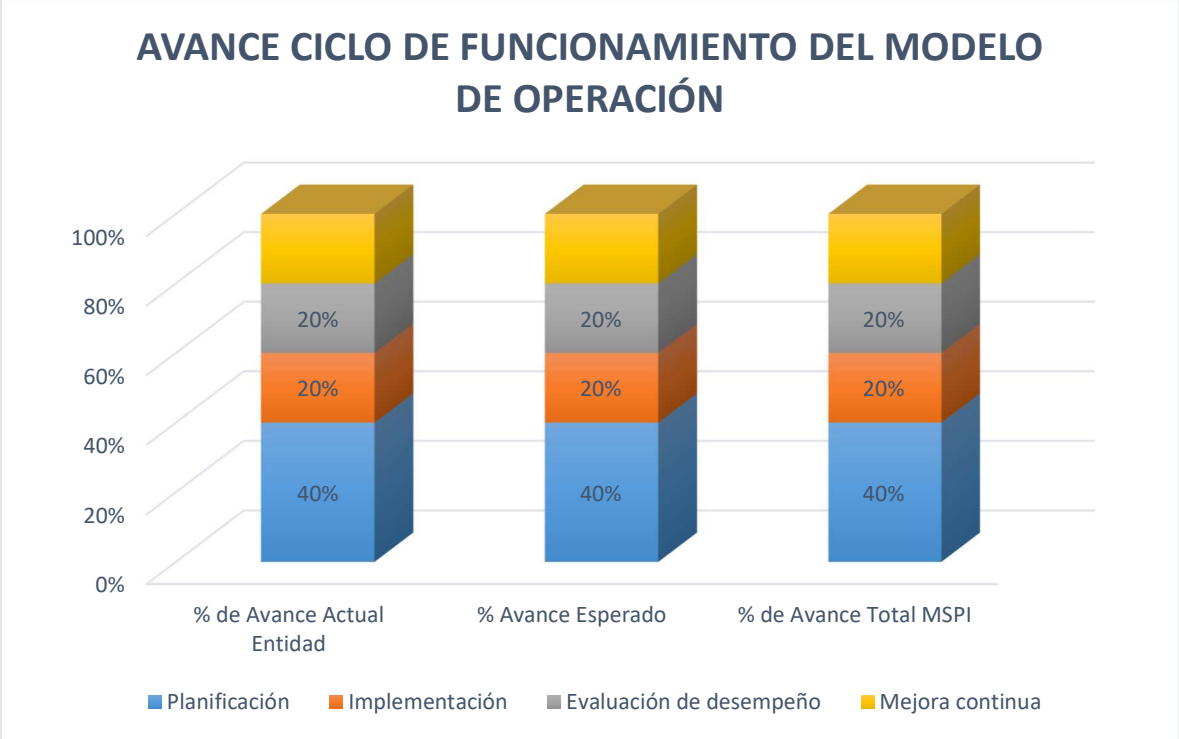
No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	90	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	90	90	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	90	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	81	80	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	85	85	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	90	80	**OPTIMIZADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	85	85	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	82	80	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	84	80	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	83	80	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	90	80	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	80	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	90	80	**OPTIMIZADO**
A.18	CUMPLIMIENTO	82,5	80	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**88**	**83**	**OPTIMIZADO**

[4] INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD. Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2017

Gracias a este análisis de brecha se identificó que estamos a 2 punto porcentuales de la meta global para el año 2025.

En cuanto al análisis de brecha para el avance del PHVA se tiene:

Año	AVANCE PHVA			
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado	% de Avance Total MSPI
2015	Planificación	40%	40%	40%
2016	Implementación	20%	20%	20%
2017	Evaluación de desempeño	20%	20%	20%
2018	Mejora continua	20%	20%	20%
TOTAL				100%



Se ha identificado que cumplimos la meta del plan.

En cuanto a la madurez del MSPI se tiene que se ha alcanzado el nivel optimizado y para este plan se propone mantener este nivel.

5.1 Análisis de brecha Transición de IPv4 a IPv6.

Se presenta plan acorde con los nuevos lineamientos del gobierno para cumplir a mediados de 2022.

En el año 2022 se realizaron los ajustes de equipos críticos, tales como switches, continuamos ajustando el diagnóstico y se realizan cotizaciones para la implementación de las otras etapas, las cuales se programan para ejecutar en 2023.

5.1 Gestión de Información

GOBIERNO DE TI	DE LA INFORMACI	CONTROL DE ACCESOS	USUARIOS
			Ciudadanía-MADS-Gobierno Nacional — Entidades Públicas Privadas – Persona Natural –Comunidades Étnicas – Asociaciones de Usuarios – Comunidad en general –Entes territoriales – Rama judicial - Entes de Control – Cooperación Internacional – Gremios.
		PRESENTACIÓN	ACCESO A LA INFORMACIÓN
			Consulta en Línea trámites en CITA y PQRDS– PÁGINA WEB – Boletines y Comunicados – Reportes – Estadísticas – Datos Abiertos – Espacio Vital
		MAC	Bodegas de Datos Agrupados

			Directorio Activo – TERANAS – Servidores dedicados			
		CONTINUIDAD DEL NEGOCIO	CALIDAD DE DATOS			
			Parámetros Geodatabases	Módulo de Metadatos - Geográficos - Documental - Alfanuméricos	Datos Maestros -información de usuarios	Estándares
		COMUNICACIÓN	EXTRACCIÓN, TRASFORMACIÓN Y CARGA DE BASES DE DATOS			
			Gestión de Calidad de Datos Formato, completitud, codificación estandarizada			
		COMUNICACIÓN Y OPERACIONES	SERVICIOS DE INTEROPERABILIDAD (GEL-XML (MIN TIC) / OGC-ICDE))			
			Servicios Intercambio de Negocio ←	→ Catálogo de Servicios ←	→ ESB – Bus de servicios de Conectividad y Orquestaciones Complejas	
		PROCESO	CERTIFICACIÓN DE OPERACIONES ESTADÍSTICAS Y/O REGISTROS ADMINISTRATIVOS			
			Lenguaje Común de Intercambio – Mapas de Intercambio -- Calidad de Datos -- Estandarización con modelos de dominios sectoriales – Directorio de Componentes -- Expediente Electrónico			
		Y AMBIE	EXTRACCIÓN TRANSFORMACIÓN Y CARGA			
			MADS	ASOCARS	ANLA	DANE
		LICENCIO	SISTEMAS DE INFORMACIÓN			
			CITA – SISF – SINAP – INTRANET – GEOVISOR – SISTEMA DE INFORMACIÓN GEOGRÁFICO			
		POLÍTICA	GOBIERNO DIGITAL	MARCO DE REFERENCIA ARQUITECTURA DE TI	MODELO DE GESTIÓN IT4+	SEGURIDAD DE LA INFORMACIÓN	INTEROPERABILIDAD

6 ANÁLISIS DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

Acordes con la información contenida en la “Guía No. 7: Guía de gestión de riesgos”[5] y la “Guía para la Administración del Riesgo” del DAFP[6] se realiza anualmente el análisis de riesgo para la seguridad de la información en la Corporación y se realizan los seguimientos al plan de tratamiento de estos riesgos. En formato R-MJ-10.

7 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se relacionan los procedimientos que se encuentran en el Sistema de Gestión Corporativo relacionado con los procedimientos requeridos en la “Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información. [7]”

[5] Guía No. 7: Guía de gestión de riesgos. MINTIC 2016.
[6] Guía para la Administración del Riesgo. DAFP 2017.
[7] Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información. MINTIC 2016.

7.1 Seguridad Del Recurso Humano:

Se encuentra definido en los procedimientos: “P-TH-01 VINCULACIÓN SERVIDORES PUBLICOS” Y “P-TH-08 RETIRO”

7.2 Gestión De Activos:

Se encuentra definido en los procedimientos: “D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN” y “P-RI-01 COMPRAS E INFRAESTRUCTURA”

7.3 Control De Acceso:

Se encuentra definido en el procedimiento: “D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN”

7.4 Criptografía: N/A

Ya que la información que se maneja en la Corporación no se requiere la encriptación de esta.

7.5 Seguridad Física Y Del Entorno:

Se encuentra definido en los procedimientos: “D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN” y las actividades del contrato de soporte y seguridad física y videovigilancia.

7.6 Seguridad De Las Operaciones:

Se encuentra definido en los procedimientos: “D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN”

7.7 Seguridad De Las Comunicaciones:

Se encuentra definido en los procedimientos: “D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN”

7.8 Relaciones Con Los Proveedores:

Se encuentra definido en los procedimientos: “M-RI-02 MANUAL DE CONTRATACIÓN” y “P-RI-04 CONTRATACION”

7.9 Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información:

Se encuentra definido en el PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI.

7.10 Gestión De Incidentes De Seguridad De La Información:

Se tiene programado elaborarlo en 2023 con base en la “Guía para la preparación de las TIC para la continuidad del negocio” del MINTIC, 2010.

7.11 Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio:

Se realiza en el formato “Catálogo de Continuidad y disponibilidad_ejemplos.xlsx” en el año 2021 con base en la “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información” del MINTIC, 2016.

7.12 Plan de sensibilización y apropiación del MSPI para toda la entidad.

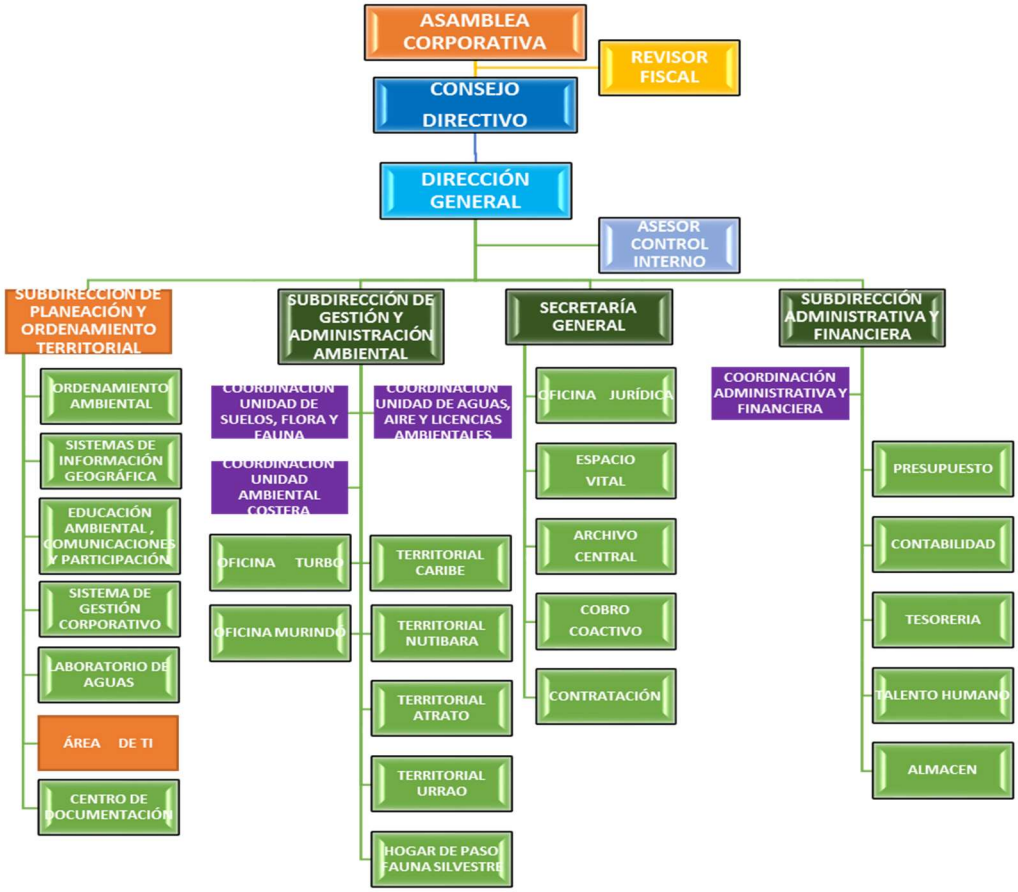
En el “P-TH-03 FORMACIÓN, CAPACITACIÓN Y BIENESTAR” se programarán las actividades relacionadas con la seguridad de la información.

8 ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Gobierno de SI

Basados en la “Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información” desarrollado por MINTIC y el organigrama de la Corporación se define el siguiente de SI.

Organigrama Corporativo



Organigrama de SI

8.2. Responsable de Seguridad de la Información:

En la Corporación se define como responsable de Seguridad de la Información (oficial de seguridad de la información) al subdirector de Planeación y Ordenamiento Territorial.

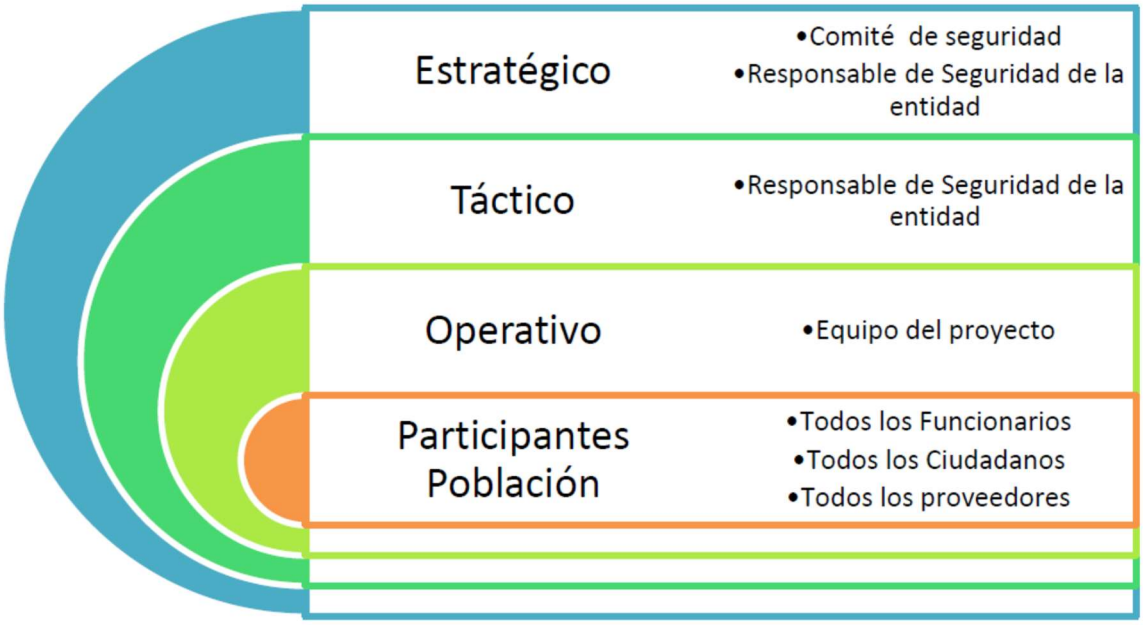
Por recomendación de la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" se desarrollaran proyectos de TI y SI, para lo cual la dirección del proyecto está en manos del responsable de SI.

8.3 Equipo del Proyecto:

En la corporación se ha tercerizado la prestación de los servicios de TI, tales como soporte técnico, página web, Aplicativos como CITA, Adhoc y SINAP, etc. Cada contrato tiene definido un coordinador y un supervisor, los cuales conforman el equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

A continuación se presenta un modelo (adoptado de la "Guía No 4…") de los miembros del equipo de seguridad y privacidad de la información. Las funciones del comité de seguridad las asume el Comité Interinstitucional de Desarrollo Administrativo.



9 SEGUIMIENTO Y REVISIÓN DEL MSPI

• Procedimientos de seguimiento, revisión y otros controles

Ver “D-RI-02: PRACTICAS DE ADMINISTRACIÓN Y SEGURIDAD INFORMÁTICA – PROTOCOLO PARA SEGURIDAD”

• Emprender revisiones regulares de la eficacia del MSPI

Ver “D-RI-02: PRACTICAS DE ADMINISTRACIÓN Y SEGURIDAD INFORMÁTICA – PROTOCOLO PARA SEGURIDAD”

• Realizar auditorías internas del MSPI

Ver “P-MJ-09: AUDITORIAS INTERNAS”

• Emprender una revisión del MSPI, realizada por la dirección

Ver “P-DI-02: REVISIÓN POR LA DIRECCIÓN”

• Actualizar los planes de seguridad

Ver “P-DI-03 MODELO INTEGRADO DE PLANEACION Y GESTIÓN”

• Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del MSPI.

Ver “P-MJ-11 ADMINISTRACIÓN DEL RIESGO”

• Revisar las valoraciones de los riesgos a intervalos planificados,

Ver “P-MJ-11 ADMINISTRACIÓN DEL RIESGO”

• Medir la eficacia de los controles

Ver indicadores del SGC.

• Implementar las mejoras identificadas en el MSPI

Ver “P-MJ-08 ACCIONES PARA EL MEJORAMIENTO”

• Emprender las acciones correctivas y preventivas adecuadas,

Ver “P-MJ-08 ACCIONES PARA EL MEJORAMIENTO”

• Comunicar las acciones y mejoras a todas las partes interesadas,

Ver “P-MJ-08 ACCIONES PARA EL MEJORAMIENTO”

• Asegurar que las mejoras logran los objetivos previstos.

Ver “P-MJ-08 ACCIONES PARA EL MEJORAMIENTO”

• Los registros exigidos por la norma ISO 27001 y el MSPI, ej. Un libro de visitantes, informes de auditoría y formatos de autorización de acceso diligenciados.

Se programarán para el primer año de la vigencia, 2022.

Adicionalmente se ejecutar procedimientos de seguimiento, revisión y otros controles para;

- Detectar rápidamente errores en los resultados del procesamiento
- Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
- Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
- Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

10 PLANIFICACIÓN DE ACTIVIDADES DEL MSPI

De acuerdo a los objetivos del MSPI se tienen las siguientes actividades:

Componente	Actividades	2022	2023	2024	2025
1. FASE DE PLANIFICACIÓN	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas
	1.2. Revisión Procedimientos de Seguridad de la Información.	Crear Procedimientos acorde con ISO 27001	Actualizar Procedimientos	Actualizar Procedimientos	Actualizar Procedimientos
	1.3. Roles y Responsabilidades de Seguridad	Definir y aprobar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades
	1.4. Identificación, documentación y aprobación de activos de información.	Documentar y aprobar activos de información	Actualizar activos de información	Actualizar activos de información	Actualizar activos de información
	1.5. Identificación, Valoración Y Tratamiento de Riesgos.	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos
	1.6. Capacitación y sensibilización	Diseñar y aprobar programas y planes para los funcionarios sobre conciencia y comunicación de las políticas	Funcionarios toman conciencia de la seguridad y privacidad de la información.	Ejecutar planes de toma de conciencia, comunicación y divulgación.	Ejecutar planes de toma de conciencia, comunicación y divulgación.
	1.7. Implementar el Modelo de Seguridad y Privacidad de la Información	Alcanzar nivel de Madurez Optimizado	Mantener Nivel de Madurez Optimizado	Mantener Nivel de Madurez Optimizado	Mantener Nivel de Madurez Optimizado
2. FASE DE IMPLEMENTACIÓN	2.1. Planificación y Control Operacional	Definir documentación para el control operacional	Aprobar la documentación	Ajustar de la documentación	Ajustar de la documentación
	2.2. Implementación del plan de tratamiento de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos
	2.3. Indicadores De Gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión
	2.4. Plan de Transición de IPv4 a IPv6	Implementar y realizar seguimiento plan de transición			

Componente	Actividades	2022	2023	2024	2025
3. FASE DE EVALUACIÓN DE DESEMPEÑO	3.1. Plan de revisión y seguimiento a la implementación del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI
	3.2. Plan de Ejecución de Auditorias	Planear y ejecutar auditorías internas al MSPI	Planear y ejecutar auditorías internas al MSPI	Planear y ejecutar auditorías internas al MSPI	Planear y ejecutar auditorías internas al MSPI
4. FASE DE MEJORA CONTINUA	4.1. Plan de mejora continua	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	Documentar el seguimiento al plan de mejoramiento.	Documentar el seguimiento al plan de mejoramiento.	Documentar el seguimiento al plan de mejoramiento.	Documentar el seguimiento al plan de mejoramiento.
	4.3 Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan
5. MODELO DE MADUREZ	5.1. Autodiagnóstico nivel de madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.2. Identificación del nivel madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.3. Análisis de brecha	Realizar Análisis	Realizar Análisis	Realizar Análisis	Realizar Análisis
6. PRIVACIDAD DE LA INFORMACIÓN	6.1. Contar con una herramienta de análisis sobre impacto en la privacidad	N/A	Realizar la herramienta de análisis sobre impacto en la privacidad	Ajustar la herramienta	Ajustar la herramienta
	6.2. Descripción de los flujos de información	N/A	Documentar procesos	Revisar procesos documentados	Revisar procesos documentados
	6.3. Identificar los riesgos de privacidad	N/A	Elaborar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad

Componente	Actividades	2022	2023	2024	2025
7. ADOPCIÓN DEL PROTOCOLO IPv6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	Verificar y actualizar el plan	Verificar y actualizar el plan		
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	Programar Implementación el plan	Implementar el plan		
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.		Realizar pruebas y adquirir dominio IPv6		

Con base en estas actividades se elaborarán los indicadores y un tablero de control para el seguimiento de estos indicadores.

10.1 Proyección de presupuesto área de SI

Presupuesto por líneas de acción

Componente	Actividades	Recurso Humano	Recurso económico o tecnológico
1. FASE DE PLANIFICACIÓN	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información	X	
	1.2. Revisión Procedimientos de Seguridad de la Información.	X	
	1.3. Roles y Responsabilidades de Seguridad	X	X
	1.4. Identificación, documentación y aprobación de activos de información.	X	
	1.5. Identificación, Valoración Y Tratamiento de Riesgos.	X	
	1.6. Capacitación y sensibilización	X	X

Componente	Actividades	Recurso Humano	Recurso económico o tecnológico
	1.7. Implementar el Modelo de Seguridad y Privacidad de la Información	X	X
2. FASE DE IMPLEMENTACIÓN	2.1. Planificación y Control Operacional	X	
	2.2. Implementación del plan de tratamiento de riesgos	X	X
	2.3. Indicadores De Gestión	X	
	2.4. Plan de Transición de IPv4 a IPv6	X	
3. FASE DE EVALUACIÓN DE DESEMPEÑO	3.1. Plan de revisión y seguimiento a la implementación del MSPI	X	X
	3.2. Plan de Ejecución de Auditorias	X	
4. FASE DE MEJORA CONTINUA	4.1. Plan de mejora continua	X	X
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	X	
	4.3 Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.	X	
5. MODELO DE MADUREZ	5.1. Autodiagnóstico nivel de madurez	X	
	5.2. Identificación del nivel madurez	X	
	5.3. Análisis de brecha	X	
6. PRIVACIDAD DE LA INFORMACIÓN	6.1. Contar con una herramienta de análisis sobre impacto en la privacidad	X	X
	6.2. Descripción de los flujos de información	X	
	6.3. Identificar los riesgos de privacidad	X	
7. ADOPCIÓN DEL PROTOCOLO IPv6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	X	X
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	X	X
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.	X	X

11. Plan de Comunicaciones del PESI

Para alcanzar el logro de los objetivos de este plan, las actividades se encaminan a lograr una nivelación de funcionarios y usuarios por medio de tres ejes fundamentales:

- Formación.
- Acceso a la tecnología.
- Procesos institucionales acordes.

Para lograr este punto, se consideraron las siguientes acciones:

Incluir en el plan de capacitación programas de capacitación, entrenamiento y sensibilización a la incorporación de Sistemas de Información, en temas relacionados con:

- Administración De Contraseñas
- Uso Y Manejo De Inventario
- Malware y sus diferentes tipos
- Software Permitido/Prohibido En La Entidad
- Políticas Organizacionales Relacionadas Con Seguridad De La Información
- Uso De Dispositivos De La Entidad Fuera De Las Instalaciones
- Uso De Correo Electrónico E Identificación De Correos Sospechosos
- Seguridad En El Puesto De Trabajo
- Uso Apropiado De Internet
- Temas de control de acceso a los sistemas (privilegios, separación de roles)
- Política De Escritorio Limpio
- Ingeniería Social
- Sanciones Por Incumplimiento De Las Políticas
- Gestión De Incidentes (Como reportar, que puedo reportar)
- Spam
- "Shoulder Surfing" Backups Y Recuperación
- Cambios En Los Sistemas
- Amenazas Y Vulnerabilidades Comunes
- Roles Y Responsabilidades En La Entidad

11.1. Alcance

La oferta de productos definida en este ítem corresponde a una serie de productos relacionados con la preparación de las personas que se encuentran relacionadas de manera directa e indirecta con el soporte que debe darse a funcionarios, decisores y usuarios en materia de SI.

11.2. Red de formadores de formadores

Con el fin de disminuir esfuerzos – y costos – se propone construir una red de formadores de formadores que permitan el establecimiento y difusión de los siguientes temas:

- Redes de conocimiento.
- Círculos de conocimiento.
- Gestión del conocimiento.
- Pedagogía para no pedagogos.
- Modelos educativos.
- Diseño de contenidos para entornos virtuales.

Control de cambios

En la revisión del 20-01-2022 se realizaron los siguientes ajustes.

- Actualización de la normatividad.
- Ajustes a Organigrama de TI para incluir seguridad de la información.
- Ajustes en el plan de auditorías limitándolo a auditorías internas del MSPI.
- Ajuste al nivel de madurez esperado en el MSPI, ya que en 2022 se alcanzó el nivel Optimizado.