Modelo de Seguridad y Privacidad de la Información

Proceso Información, Innovación y Tecnología

Oficina de Seguridad de la Información
Versión 004
Código OD-IIT-0001
Año 2025

El contenido de este documento corresponde a Información Pública

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento brinda el marco de referencia y explica cómo la Unidad Administrativa Especial de la Dirección de Impuestos y Aduanas Nacionales UAE-DIAN, (en adelante DIAN) adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en armonía con la política de gobierno digital, los lineamientos fijados por MinTIC, el Departamento Administrativo de la Función Pública y la norma técnica NTC ISO/IEC 27001:2022.

El Modelo del MSPI muestra los lineamientos y orienta la implementación del **Sistema de Gestión de Seguridad y Privacidad de la Información** (SGSPI), la integración con el Programa Integral de Protección de Datos Personales y la Gestión de Riesgos de Seguridad de la Información de la DIAN, su armonización con otros sistemas de gestión de la entidad tales como el Sistema Gestión de Calidad, el Sistema de Gestión Documental y el Sistema de Gestión de Riesgos, entre otros.

Para llevar a cabo la implementación del MSPI se debe contar con el Plan de Seguridad y Privacidad de la Información que se actualizará y publicará anualmente de conformidad con el Decreto 612 de 2018. Este plan contempla las actividades y productos específicos a desarrollar, basados en el ciclo PHVA de acuerdo con los lineamientos expuestos en el presente modelo.

En cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y los lineamientos emitidos por la Superintendencia de Industria y Comercio, el presente modelo contempla la generación de un Programa Integral de Protección de Datos Personales para aspectos específicos del programa y los demás controles se integrarán y desarrollarán en el Manual de Políticas y Lineamientos del Seguridad de la Información[1] y el Manual para la Protección de Datos Personales.[2]

[1] MN-IIT-0072 Manual de Políticas Lineamientos de Seguridad de la Información
[2] MN-IIT-0062 Manual para la Protección Datos Personales.

2. OBJETIVO:

Definir el Modelo de Seguridad y privacidad de la Información MSPI en la DIAN para facilitar la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información SGSPI, basados en el ciclo PHVA (Planear, Hacer, Verificar y Actuar) y de acuerdo con la norma NTC ISO/IEC 27001:2022[3], así como, los demás requerimientos legales, normativos, técnicos y reglamentarios.

3. CICLO DE OPERACIÓN

El Modelo MSPI de la DIAN toma como referencia el ciclo definido en el Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y Comunicaciones en su Versión 4[4], el cual está basado en el ciclo PHVA conforme al estándar internacional ISO/IEC 27001:2022 (Planificación, Implementación, Evaluación de Desempeño y Mejora Continua):

[3] Instituto Colombiano de Normas Técnicas y Certificación. Norma técnica colombiana NTC-ISO/IEC 27001:2022

[4] Ministerio de Tecnologías de la Información y las Comunicaciones. Documento Maestro del Modelo de Seguridad y Privacidad de la Información. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Figura 1 - Ciclo Modelo de Seguridad y Privacidad de la Información (Tomado MSPI - Min Tic V4)

4. DIAGNÓSTICO

La DIAN ha realizado valoraciones de los controles del Anexo A y del Sistema de Gestión de Seguridad y Privacidad de la Información conforme al MSPI y al ciclo de PHVA establecido, del Programa Integral de Gestión de Datos Personales y de la Gestión de Riesgos de Seguridad de la Información. En el 2023, se desarrolló la evaluación del nivel de madurez del Modelo de Seguridad y Privacidad de la Información - **MSPI**, el Sistema de Gestión de Seguridad y Privacidad de la Información - **SGSPI**, el Programa Integral de Gestión de Datos Personales - **PIGDP** y la Gestión de Riesgos de Seguridad de la Información – **GRSI**; lo anterior teniendo en cuenta los objetivos de negocio, los roles y las responsabilidades, los procesos y procedimientos, la documentación interna consultada en la Diannet, la estructura organizacional y demás actividades relacionadas que fueron socializadas durante las entrevistas ejecutadas. El procedimiento para la realización de la evaluación fue el siguiente:

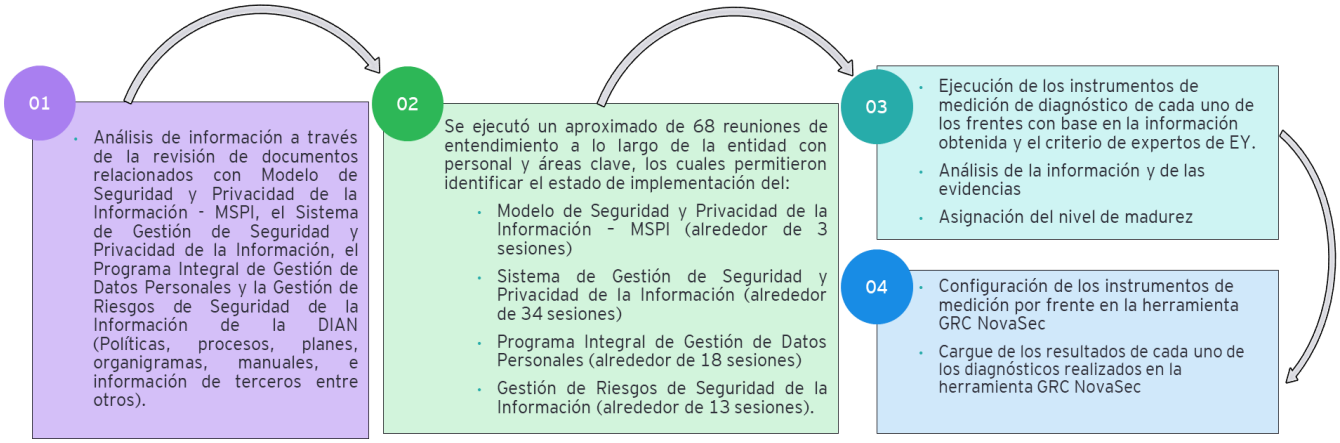

Figura 2: Fases del Diagnóstico

De manera adicional el Diagnóstico se llevó a cabo en tres fases principales:

Fase	Fase 1	Fase 2	Fase 3
	Levantamiento de Información	Ejecución de entrevistas	Análisis de la información y generación de infome de resultados
Resumen de las actividades clave	1. Identificar información vigente que describa el modelo a evaluar.	1. FIltrar las preguntas para que correspondan con la entrevista específica a realizar.	1. Analisis de la información obtenida durante las entrevistas.
	1.a). Entrega de la información solicitada.	2. Hacer el recorrido de las preguntas del diagnóstico correspondientes a cada entrevistado.	1.a Entrega de la informacion pendiente de las entrevistas.
	2. Entendimiento documental de cada instrumento.	3. Solicitar la evidencia documentada cuando la pregunta del cuestionario lo solicite.	2. Consolidación de la información.
	3. Identificación de personas que atenderán las entrevistas.	4. Solicitar información adicional en caso de que el consultor lo defina necesario según las respuestas dadas por el entrevistado.	3. Asignación final de la valoración de madurez a las preguntas del cuestionario.
	4. Definición del plan de entrevistas.	5. Asignación preliminar de la valoración de madurez a las preguntas del cuestionario según las respuestas dadas.	4. Realizar recomendaciones.
	5. Programación de las entrevistas acorde al plan de entrevistas definido.	6. Envío de correo con la información solicitada que no se haya entregado durante la entrevista.	5. Documentación del informe de resultados del diagnóstico.
		7. Documentar las entrevistas.	

Figura 3: Metodología para la ejecución del Diagnóstico

Para la evaluación se establecieron las escalas relacionadas a continuación considerando los siguientes niveles de madurez definidos por el MinTic.

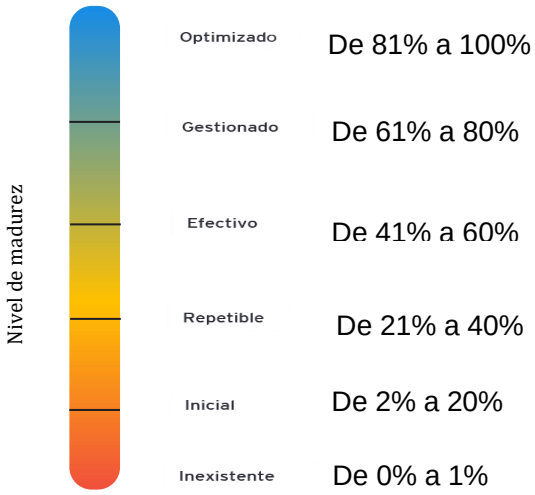

Figura 4: Valores de la escala de medición

A continuación, se presentan los resultados obtenidos de la medición realizada.

4.1 Modelo de Seguridad y Privacidad de la información - MSPI

Los resultados del Diagnóstico del MSPI realizado se presentan en la siguiente tabla:

NIVEL DE CUMPLIMIENTO MSPI	
FASE	ACTUAL
PLANIFICACIÓN	36%
OPERACIÓN	20%
EVALUACIÓN DE DESEMPEÑO	29%
MEJORA CONTINUA	10%

Tabla 1: Resultados MSPI, 2023

El resultado general de la medición obtenida sobre el MSPI correspondió a un promedio del 24% de cumplimiento, de acuerdo con la escala establecida para el MSPI.

4.2 Sistema de Gestión de Seguridad y Privacidad de la Información (Controles Anexo A de la ISO 27001:2022) – SGSPI

Los resultados del Diagnóstico del SGSPI el cual incluye los controles del Anexo A de la norma ISO27:001:2022 realizado se presentan en la siguiente tabla:

NIVEL DE CUMPLIMIENTO SGSPI	
DOMINIO	ACTUAL
CONTROLES ORGANIZACIONALES	35%
CONTROLES DE PERSONAS	50%
CONTROLES FÍSICOS	53%
CONTROLES TECNOLÓGICOS	43%
CONTROLES ADICIONALES	40%

Tabla 2: Resultados Anexo A ISO 27001:2022, 2023

El resultado general de la medición obtenida sobre el SGSPI correspondió a un promedio del 44% de cumplimiento, de acuerdo con la escala establecida para el SGSPI.

4.3 Programa Integral de Gestión de Datos Personales

Los resultados del Diagnóstico del PIGDP realizado se presentan en la siguiente tabla:

NIVEL DE CUMPLIMIENTO DATOS PERSONALES	
DOMINIO	ACTUAL
PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	81%
TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	40%
INFORMACIÓN MÍNIMA DE LOS TITULARES PERSONALES	50%
SUMINISTRO DE LA INFORMACIÓN PERSONAL	67%
ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	61%
POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	77%
AVISO DE PRIVACIDAD	58%
REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD	0%
GESTIÓN DE ENCARGADOS DEL TRATAMIENTO	29%
TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL	100%
TRANSFERENCIA O CESIÓN Y TRANSMISIÓN NACIONAL	56%
RESPONSABILIDAD DEMOSTRADA	38%
REGISTRO NACIONAL DE BASES DE DATOS	64%
AUTORIZACIÓN	63%
DATOS PRIVADOS, SEMIPRIVADOS	38%
SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES	0%
FORMACIÓN Y EDUCACIÓN	38%
EVALUACIÓN Y REVISIÓN CONTINUA	50%
RETENCIÓN Y ELIMINACIÓN DEL DATO PERSONAL	60%
DATOS RECOLECTADOS ANTES DE LA EXPEDICIÓN DEL DECRETO 1377 de 2013 (27 de junio de 2013)	0%

Tabla 3: Resultados PIGDP, 2023

El resultado general de la medición obtenida sobre el PIGDP correspondió a un promedio del 46% de cumplimiento, de acuerdo con la escala establecida para el PIGDP.

4.4 Gestión de Riesgos de Seguridad de la Información - GRSI

Los resultados del Diagnóstico de la GRSI realizado se presentan en la siguiente tabla:

NIVEL DE CUMPLIMIENTO RIESGOS (31000 Y DAFP)	
DOMINIO	ACTUAL
FASE DE PLANIFICACIÓN	***28%***
PLAN DE MEJORAMIENTO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	27%
NECESIDADES Y EXPECTATIVAS DE LOS INTERESADOS (INTERNO)	25%
NECESIDADES Y EXPECTATIVAS DE LOS INTERESADOS (EXTERNO)	25%
ALCANCE	20%
LIDERAZGO Y COMPROMISO	24%
POLÍTICAS	20%
ROLES Y RESPONSABILIDADES	30%
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRITICA	60%
IDENTIFICACIÓN DE LOS RIESGOS INHERENTES DE SEGURIDAD DE LA INFORMACIÓN	32%
IDENTIFICACIÓN DEL NIVEL DE CONFIANZA PARA LA AUTENTICACIÓN DIGITAL	20%
VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	52%
DECLARACIÓN DE APLICABILIDAD	24%
PLAN DE TRATAMIENTO DE RIESGOS	27%
IDENTIFICACIÓN Y EVALUACIÓN DE CONTROLES EXISTENTES	32%
GESTIÓN DE RIESGOS DE SEGURIDAD DE LA CADENA DE SUMINISTRO Y DE TERCEROS	1%
RECURSOS	28%
FASE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	***17%***
PLAN DE IMPLEMENTACIÓN DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	20%
EVALUACIÓN DE RIESGOS DE SEGURIDAD DIGITAL PARA LAS ÁREAS RESPONSABLES	20%
EVALUACIÓN DE RIESGOS DE SEGURIDAD DIGITAL PARA LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN-OSI	20%
EVALUACIÓN DE LA IMPLEMENTACIÓN DE LOS CONTROLES EN LAS ÁREAS	11%
EVALUACIÓN DE LA REVISIÓN DE LA IMPLEMENTACIÓN DE LOS CONTROLES POR PARTE DE LA OSI	11%
IMPLEMENTACIÓN DE LOS PLANES PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	20%
FASE DE MONITOREO Y REVISIÓN	***12%***
PRIMERA LÍNEA DE DEFENSA (DUEÑOS DE LOS RIESGOS)	20%
SEGUNDA LÍNEA DE DEFENSA (RESPONSABLES DE LA GESTIÓN DE RIESGOS (OSI))	7%
TERCERA LÍNEA DE DEFENSA (CONTROL INTERNO))	20%
REGISTRO Y REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ÁREAS DE LA ENTIDAD)	1%
REGISTRO Y REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (OSI)	20%
AUDITORÍA EXTERNA DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	1%
AUDITORÍA INTERNA DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	20%
REPORTE DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN A AUTORIDADES O ENTIDADES ESPECIALES	1%
REVISIÓN POR LA DIRECCIÓN DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	20%
MEDICIÓN DEL DESEMPEÑO	1%
FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	***5%***
MEJORA CONTINUA	5%

Tabla 4: Resultados GRSI, 2023

El resultado general de la medición obtenida sobre la GRSI correspondió a un promedio del 15% de cumplimiento, de acuerdo con la escala establecida para la GRSI.

5. PLANIFICACIÓN

5.1 Contexto

5.1.1 Comprensión de la organización y de su contexto

El contexto interno y externo de la entidad se elaboró teniendo como base el método descriptivo PESTEL, el cual se visualiza en el listado maestro de documentos, denominado Análisis PESTEL[5] , el cual incluye un análisis de cada uno de los factores claves.

Para elaborar este contexto se tuvo en cuenta la normatividad aplicable, la cual se relaciona en el Documento con la Normatividad del análisis PESTEL V1_0[6]

5.1.2 Necesidades y expectativas de los interesados

Para obtener el cumplimiento y las oportunidades (necesidades y expectativas) de las partes interesadas internas o externas que están relacionadas con el SGSPI de la DIAN y que pueden influir directamente en la operación de este, se tuvieron en cuenta las siguientes entradas relevantes:

- Comprensión de la organización y de su contexto
- Aspectos de Planeación institucional[7]
- Plan Nacional de Desarrollo
- Política de Gobierno Digital
- Entrevistas con los líderes de áreas/procesos de la entidad
- Listado de entidades de orden nacional o territorial que se relacionan directamente en el cumplimiento misional de la entidad
- Listado de proveedores de la entidad
- Grupos de Partes Interesadas
- Normatividad que le aplique a la entidad y de conformidad con la implementación del MSPI y el SGSPI.

a. Requisitos e información general

Se tuvieron en cuenta los siguientes requisitos relevantes para el desarrollo y análisis de las expectativas de las partes interesadas:

- El Plan Nacional de Desarrollo 2022-2026, en su numeral 8 “Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas”

[5] Documento con el análisis PESTEL.pdf. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI
[6] Ver análisis PESTEL V1_0.pdf. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI
[7] Planeación y Evaluación Institucional.
https://www.dian.gov.co/dian/entidad/Paginas/PlaneacionEvaluacionInstitucional.aspx#:~:text=Planeaci%C3%B3n%20Institucional,y%20los%20proyectos%20de%20inversi%C3%B3n.

relaciona las expectativas del actual gobierno frente al desarrollo de la seguridad digital para el periodo 2022-2026.

- El Análisis PESTEL (Político, Económico, Social, Tecnológico, Ecológico, Legal) como base de la identificación del Contexto Interno y Externo realizado para la DIAN, para determinar si las partes identificadas en este análisis afectan directa e indirecta al Modelo de Seguridad y Privacidad de la Información bajo la responsabilidad de la Oficina de Seguridad de la Información - OSI.
- La información relacionada con el alcance del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN, se encuentra en el numeral 5.1.3, los cuales están alineados con el logro de los objetivos estratégicos de la DIAN.
- La Política de gobierno digital emitida por el Departamento de Planeación Nacional, a través del **Modelo Integrado de Planeación y Gestión MIPG versión 6 de 2024** para determinar dentro de estas definiciones las partes interesadas que afecten el desarrollo del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN.
- La información incluida en la Planeación estratégica DIAN, la cual brinda lineamientos sobre los compromisos, programas y proyectos que se deben desarrollar para el logro de los objetivos estratégicos de la DIAN. Esto es relevante para la Oficina de Seguridad de la Información - OSI para determinar las partes interesadas relacionadas con esta planeación y con el desarrollo del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN.
- Las entrevistas con los responsables de la Oficina de Seguridad de la Información - OSI, para determinar si se cuenta con la identificación de los principales actores que afecten el desarrollo del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN.
- Se realizó el análisis de la reglamentación, normatividad y legislación aplicable a los procedimientos de la Oficina de Seguridad de la Información - OSI como responsable del MSPI-DIAN.
- La norma técnica ISO/IEC 27001: 2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.
- La documentación relacionada con la identificación de las necesidades y expectativas de las partes interesadas de la DIAN[8]**.**

5.1.3 Definición del alcance del MSPI

Para determinar los límites del MSPI y la aplicabilidad del SGSPI en el marco del modelo de operación por proceso de la DIAN, se tuvo en cuenta:

- Modelo de procesos[9]
- Modelo organizacional[10]

[8] Planes e Identificación de las necesidades y expectativas de las partes interesadas.pdf. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI

[9] Mapa de Procesos. https://diancolombia.sharepoint.com/sites/diannetpruebas/procesos/Paginas/Mapa-de-Procesos.aspx

[10] Organigrama. https://www.dian.gov.co/dian/entidad/Organigramanuevo/Org_DIAN_2021.pdf

- Servicios tecnológicos de acuerdo con la identificación de activos de información
- Arquitectura Digital[11]
- Listado de las sedes físicas donde opera la Entidad[12]
- La comprensión de la organización y de su contexto[13]
- La necesidades y expectativas de los interesados[14]

Así las cosas, el MSPI cobija siete (7) procesos enmarcados en las perspectivas Financiera, Servicio al cliente, Misional y de apoyo, tanto a nivel central como a nivel seccional.

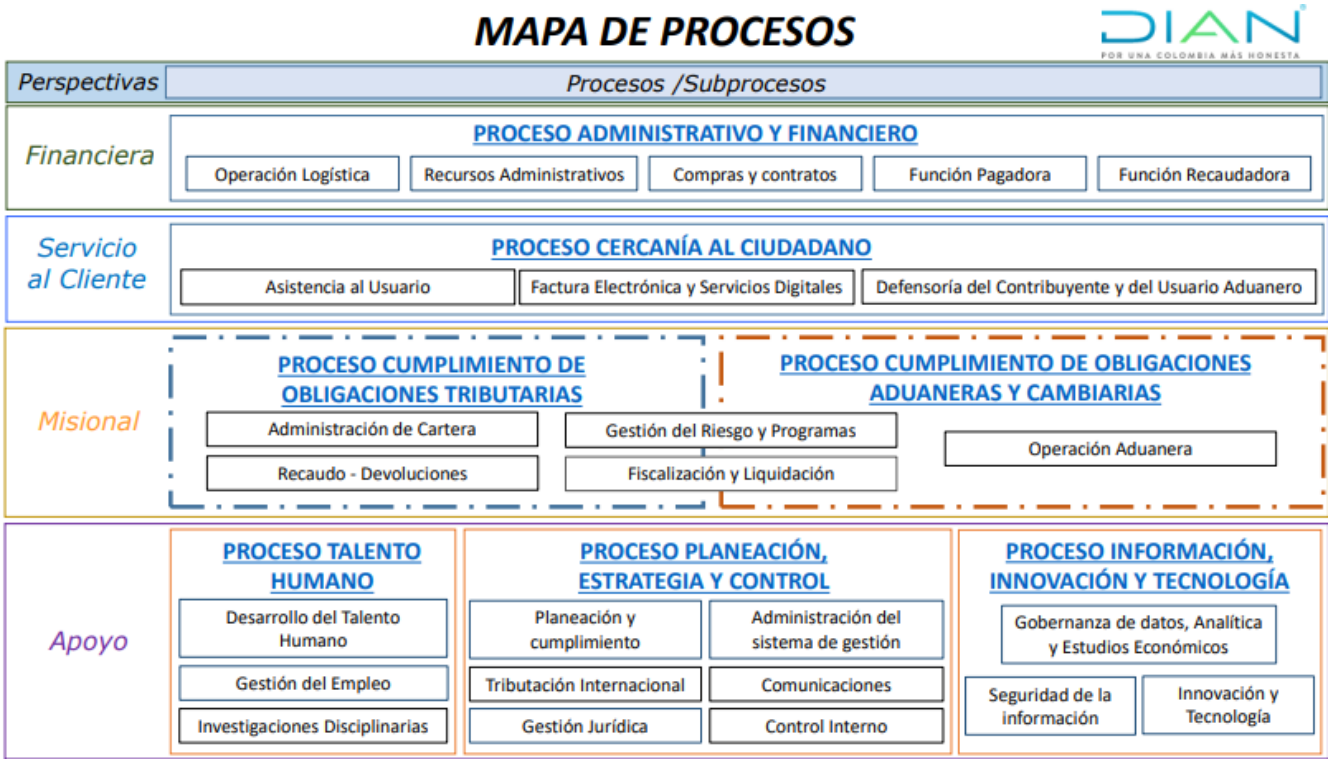

Figura 5 – Mapa de procesos DIAN

La base del alcance surge a partir de la identificación de la totalidad de los activos de información de la entidad.

[11] PR-IIT-0456 Gestión de Arquitectura Digital
[12] DIAN. 2023. Puntos de Contacto y Directorio Telefónico. https://www.dian.gov.co/atencionciudadano/contactenos/Paginas/puntosdecontacto.asp
[13] Ver Análisis PESTEL.pdf. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI
[14] Ver Planes e Identificación de las necesidades y expectativas de las partes interesadas.pdf. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI

5.2 Liderazgo

5.2.1 Liderazgo y Compromiso

De acuerdo con lo definido mediante la resolución DIAN No 000021 del 20 de enero de 2022, la DIAN adopta el Modelo Integrado de Planeación y Gestión MIPG (**artículo 1**), se crea el Comité Institucional de Gestión y Desempeño (**artículo 15**) y en el Comité se establece que a la Oficina de Seguridad de la Información - OSI le corresponde asegurar la implementación a la que se refiere el **numeral 6**, **articulo 17**, de la citada resolución "...Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información..."[15]

Conforme con lo establecido en el Libro 2, Parte 2, Titulo 9, Capitulo 1, Sección 2 del Decreto 1078 de 2015, donde se define como uno de los componentes de la Estrategia de Gobierno en Línea, la Seguridad y Privacidad de la Información y por ello la DIAN creó la Oficina de Seguridad de la Información - OSI mediante Decreto 2183 del 23 de diciembre de 2017 asignando las funciones correspondientes, la cual hace parte del Comité Institucional Estratégico. Dando cumplimiento también de esta forma a lo establecido en el Decreto 767 de 2022, Capítulo 1 Política de Gobierno Digital, Sección 2 Elementos de la Política de Gobierno Digital, Artículo 2.2.9.1.2.1. Estructura, 3.2. Seguridad y Privacidad de la Información.

La DIAN articula el cumplimiento de los objetivos de Seguridad de la Información a través de la:

- Adopción del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI, conforme a la resolución (en trámite).
- Declaración de la política de Seguridad y Privacidad de la Información de la UAE – DIAN.
- Declaración de la política para la gestión de riesgos de seguridad de la información incorporada en la Política General de Riesgos de la entidad.
- Adopción dentro de sus procedimientos y procesos de la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas*, *versión 6 de 2022*, y el *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, versión 4 de 2021,* como referencia del gobierno colombiano para la gestión de la seguridad de la información.
- Ejecución del plan de sensibilización de seguridad de la información, cuyos resultados son presentados ante el Comité Institucional Estratégico.
- Ejecución del monitoreo y seguimiento definidos en los diferentes procedimientos.
- Revisión de los Indicadores de Seguridad de la Información de acuerdo con la periodicidad establecida en la hoja de vida, identificando desviaciones que generen acciones de tratamiento y/o mejoramiento.

[15] DIAN. 28 enero 2022. Resolución Número 000021
https://www.dian.gov.co/normatividad/Normatividad/Resoluci%C3%B3n%20000021%20de%2028-01-2022.pdf

5.2.2 Política de seguridad y privacidad de la información

Ante el Comité Institucional Estratégico de la DIAN realizado el 3 de diciembre de 2024 fue aprobada la actualización de la Política de Seguridad y Privacidad de la Información[16] como parte de su compromiso y apoyo en el diseño e implementación del Modelo de Seguridad y Privacidad de la Información para garantizar la gestión de estos aspectos en la entidad, lo cual quedó registrado en el acta No. 03 de la misma fecha. En dicha Política de Seguridad y Privacidad de la Información se incluyen 11 objetivos con los cuales se busca asegurar la implementación de esta política en la DIAN.

Así mismo, la DIAN cuenta con el **MN-IIT-0072 - Manual de Políticas y Lineamientos de Seguridad de la Información** el cual contiene las siguientes políticas específicas:

1. Políticas de seguridad de la información
2. Restricción de acceso de la información
3. Autenticación segura
4. Control de acceso
5. Copia de seguridad
6. Derechos de acceso
7. Enmascaramiento de datos

La DIAN estableció la Política para la administración de riesgo[17] dentro de la cual contiene los riesgos de seguridad de la información y por ello la Oficina de Seguridad de la Información - OSI emitió la cartilla CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información como metodología para la gestión de dichos riesgos en la entidad.

5.2.3 Roles y responsabilidades

Por medio del **Decreto 1742 de 2020**[18] se establece el Comité Institucional Estratégico - CIE el cual cumple las funciones de órgano asesor para el desarrollo de los objetivos y funciones de la DIAN de acuerdo con lo establecido en el Capítulo 6, Artículo 77, que para el caso que nos ocupa, aplican las siguientes:

- **Numeral 6.** Aprobar las Políticas de Gestión de la Entidad y, entre otras, la política de seguridad de la información, la política archivística y/o de gestión documental y la política de gestión del talento humano.
- **Numeral 8.** Decidir sobre los asuntos de carácter estratégico directivo que el Director General, los Directores de Gestión o el Jefe de la Oficina de Seguridad de la Información - OSI, o quien haga sus veces, presenten al Comité Institucional Estratégico -CIE y que no correspondan a los asuntos ordinarios propios de su cargo.

[16] DIAN 3 de diciembre de 2024. Política de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales (DIAN).
https://www.dian.gov.co/Documents/POLITICA_GENERAL_DE_SEGURIDAD_Y_PRIVACIDAD_DE_LA_INFORMACION.pdf

[17] Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN Versión 2 - 03 de octubre de 2023

[18] DIAN. 22 de diciembre de 2020. Decreto 1742 de 2020.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=153986

Así mismo, el mencionado decreto asigna 10 funciones a la Oficina de Seguridad de la Información - OSI a la fecha, que enmarca la gestión de seguridad de la información en la Entidad basado en la normatividad vigente.

En cuanto a la matriz de roles y responsabilidades[19] de las áreas de la DIAN frente al Sistema de gestión de seguridad y privacidad de la Información, esta se encuentra dividida en tres grandes grupos: la primera corresponde al nivel central, incluyendo la alta dirección, direcciones de gestión, subdirecciones y oficinas, la segunda, correspondiente a las Direcciones seccionales y la tercera corresponde a la matriz de roles y responsabilidades de la Oficina de seguridad de la oficina – OSI en la cual se encuentran los roles asociados a los dominios del SGSPI frente a las funciones de la OSI.

5.3 Planificación

5.3.1 Identificación de activos de información e infraestructura critica

a. Identificación de Activos de Información

La identificación de activos de información en la DIAN se realiza a través de lo definido en el procedimiento **PR-IIT-0366 - Gestión de Activos de Información** y la cartilla **CT-IIT-0079 - Cartilla para la gestión de activos de información**.

La identificación, creación, actualización, modificación, supresión o inactivación de un activo de información se realiza desde la solución tecnológica dispuesta por la DIAN para tal fin. En este orden de ideas, en todas las Direcciones de Gestión, Oficinas y Direcciones Seccionales, se cuenta con un servidor público que asumen el rol de "enlace de seguridad y privacidad de la información" quien, consecuentemente, tendrá la facultad de crear o actualizar cualquier información relacionada con los activos de información de su dependencia. Hasta noviembre de 2024, en la DIAN se encuentran asignados 109 enlaces de seguridad y privacidad de la información a nivel local y nacional.

Adicionalmente, para la gestión de activos de información se tienen definidas políticas y lineamientos incorporados en el documento **MN-IIT-0072 - Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información**.

La identificación de activos de información también debe tener en cuenta los aspectos definidos en la Arquitectura Empresarial de la entidad, principalmente lo relacionado con:

- Dominio de Sistema de Información:
  - Inventario y caracterización de sistemas de información[20]
- Dominio de Información:
  - Directorio de datos abiertos de la entidad[21]

[19] MATRIZ RACI - ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN V1. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI

[20] Si requiere información adicional, favor comunicarse con DGIT – Subdirección de Soluciones y Desarrollo

[21] https://www.dian.gov.co/atencionciudadano/Paginas/Transparencia.aspx#collapse10

b. Infraestructura Crítica

En la etapa de "identificación" del activo de información, el responsable de la gestión de activos define el tipo de activo de información, de acuerdo con lo descrito en el documento **CT-IIT-0079 - Cartilla para la gestión de activos de información**. En esta sección se identifica el tipo de activo en donde, entre otras cosas, se tiene la opción de "*Infraestructura Crítica Cibernética"*, para aquellos activos que cumplan con las características de este tipo de infraestructura. Ver definición en Anexo de Definiciones y Siglas de Seguridad de la Información.

Adicionalmente, en la etapa de "valoración" de la Gestión de activos de información de acuerdo con lo descrito en el numeral 4.2.4 Información adicional (Pestaña de información complementaria valoración del activo de información) del documento **CT-IIT-0079 - Cartilla para la gestión de activos de información**, el responsable de la valoración del activo determina si este es un Ciber Activo y/o Ciber Activo Crítico de TI. Ver definiciones en el documento de Definiciones y Siglas de Seguridad de la Información.[22]

5.3.2 Identificación y valoración de los riesgos de seguridad de la información

La DIAN reconoce la importancia de realizar análisis previos al desarrollo de la metodología para la gestión de riesgos de seguridad de la información que le permita identificar información relevante que pueda afectar su desarrollo, siendo esta la que se lista a continuación:

- Contexto Interno y Externo.
- Identificación de las necesidades y expectativas de las partes interesadas.
- Alcance del Modelo de Seguridad y Privacidad de la Información MSPI de la DIAN.
- Alcance de la gestión de riesgos de seguridad de la información.
- Alineación con las políticas de gestión de riesgos de la entidad y la gestión de riesgos de seguridad de la información.
- Los roles y responsabilidades
- Los recursos para la gestión de riesgos de seguridad de la información.
- La alineación con los objetivos de la entidad y los objetivos de los procesos.
- Los factores generadores de riesgos de seguridad de la información.

A su vez, la DIAN cuenta con un Marco para la Gestión de Riesgos y una Política que facilita la integración de riesgos en todas sus actividades y define las disposiciones para su identificación, análisis, valoración, tratamiento y monitoreo. Además, se describe la metodología establecida en la cartilla CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información y se alinea con los procedimientos **PR-PEC-0242 - Planificación de la gestión de riesgos** y **PR-PEC-0243 - Implementación, monitoreo y mejoramiento de la gestión de riesgos** de la Coordinación de Riesgos y Procesos.

La DIAN dispone de una metodología para la Gestión de Riesgos de Seguridad de la Información la cual contempla dentro de su desarrollo la gestión de riesgos de protección de datos personales, de ciberseguridad, de analítica de datos y todos aquellos que afecten el desarrollo del MSPI de la DIAN.

[22] Anexo Definiciones y Siglas de Seguridad de la Información. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI

La gestión de riesgos de seguridad de la información es realizada por los servidores públicos expertos en los procesos o subprocesos con el acompañamiento de la Oficina de Seguridad de la Información - OSI.

El siguiente diagrama representa de manera general las diferentes fases que integran la metodología para la gestión de riesgos de seguridad de la información.

Figura 6 – Diagrama General de la Metodología de Gestión de Riesgos

La metodología establecida para la gestión de los Riesgos de Seguridad de la Información está basada y armonizada con los lineamientos consignados en los siguientes documentos:

- Guía para la administración de riesgos y el diseño de controles en entidades públicas[23]. Riesgos de gestión, corrupción y seguridad digital – Versión 6 – noviembre de 2022 del Departamento Administrativo de la Función Pública-DAFP
- (Anexo 4 – DAFP). Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - MNGRSI – Guía riesgos 2021 de MINTIC[24].

La Oficina de Seguridad de la Información - OSI conoce la importancia de identificar los roles y las responsabilidades para la gestión de riesgos de seguridad de la información, es por ello, que define en la cartilla CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información, los participantes y sus responsabilidades. Adicionalmente tiene en cuenta lo establecido en el **decreto 1742 de 2020 en el art 10 numeral 2**. (Funciones oficina seguridad de la información) y se apoya en las definiciones realizadas en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6 de noviembre de 2022.

La gestión de riesgos de seguridad de la información cuenta con una herramienta tecnológica de apoyo que incluye la gestión de Gobierno, Riesgo y Cumplimiento - GRC NovaSec (en adelante GRC), en esta herramienta se desarrollan cada una de las etapas para la gestión de los riesgos de seguridad de la información, de acuerdo con lo descrito en el documento **MN-IIT-0075 - Manual de usuario para la gestión de riesgos de seguridad de la información**.

La gestión de riesgos de seguridad de la información incluye dentro de su análisis, la declaración de aplicabilidad de los controles asociados al Anexo A de la Norma ISO 27001:2022. Ver Declaración de

[23] Departamento Administrativo de la Función Pública. Noviembre de 2022. Guía para la administración del riesgo y el diseño de controles en entidades públicas.
https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a-70c6-dd15-68f5-6cd2ea2a8707?t=1677003002032

[24] Departamento Administrativo de la Función Pública. Octubre de 2021. Manual Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237907_maestro_mspi.pdf

Aplicabilidad[25], los cuales ayudan a mitigar la materialización de los riesgos de seguridad de la información.

5.3.3 Plan de tratamiento de los riesgos de seguridad de la información

El plan de tratamiento de riesgos está sincronizado con lo definido por la alta dirección de la DIAN en cuanto a sus *niveles de riesgos, el apetito de riesgo, la tolerancia al riesgo y la capacidad del riesgo*.

La Oficina de Seguridad de la Información – OSI identifica su responsabilidad frente al acompañamiento que se debe brindar a la gestión de los planes de tratamiento de riesgos de seguridad de la información, la cual se encuentra detallada en la cartilla CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información.

En el plan de tratamiento de riesgos de la DIAN se definen las acciones para gestionar los riesgos residuales ubicados en las zonas de riesgo *inaceptable, importante y moderado*. Para los riesgos que se encuentran por fuera del apetito de riesgo y no cuenten con un plan de tratamiento, se debe aplicar el protocolo “aceptación de riesgos” definido en la cartilla de gestión de riesgos de seguridad de información - CT-IIT-0132.

Los riesgos residuales que quedan ubicados en estas zonas indican que los controles definidos no son suficientes y/o no son efectivos. Si los controles no son suficientes, es necesario identificar nuevos controles y para los que no son efectivos, mejorarlos, de manera que permitan mitigar el riesgo llevándolo, a las zonas de riesgo ACEPTABLE de manera gradual a través de la mejora continua.

La DIAN cuenta con un plan de implementación de los controles que incluye la información de todos los planes de tratamiento, sus actividades, las fechas y sus responsables, los cuales, están enfocados en definir nuevos controles o mejorar el diseño y/o implementación de los controles existentes. Los planes de tratamiento de riesgos quedan registrados en la herramienta GRC y se pueden verificar a través de la opción de reportes de la herramienta GRC, como se describe en el **MN-IIT-0075 - Manual de Usuario para la Gestión de Riesgos de Seguridad de la Información - GRC NovaSec.**

[25] Declaración de Aplicabilidad. Para profundizar en el tema, solicitarlo a la Oficina de Seguridad de la Información - OSI

5.4 Soporte

5.4.1 Recursos

La DIAN ha designado y proporcionado recursos humanos y económicos necesarios para adoptar el Modelo de Seguridad y Privacidad de la Información el cual incluye la gestión de riesgos de seguridad de la información y protección de datos personales, cómo parte del compromiso y liderazgo de la alta dirección; en este sentido y en cumplimiento de la **resolución 000021 del 28 de enero de 2022**, **artículo 17.** "Funciones del Comité…", en el **numeral 6.** "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información"[26], se ha conformado la Oficina de Seguridad de la Información - OSI con funciones definidas en el **Decreto DIAN 1742 de 2020, Art. 10**[27], a esta oficina pertenecen 30 funcionarios distribuidos de la siguiente manera:

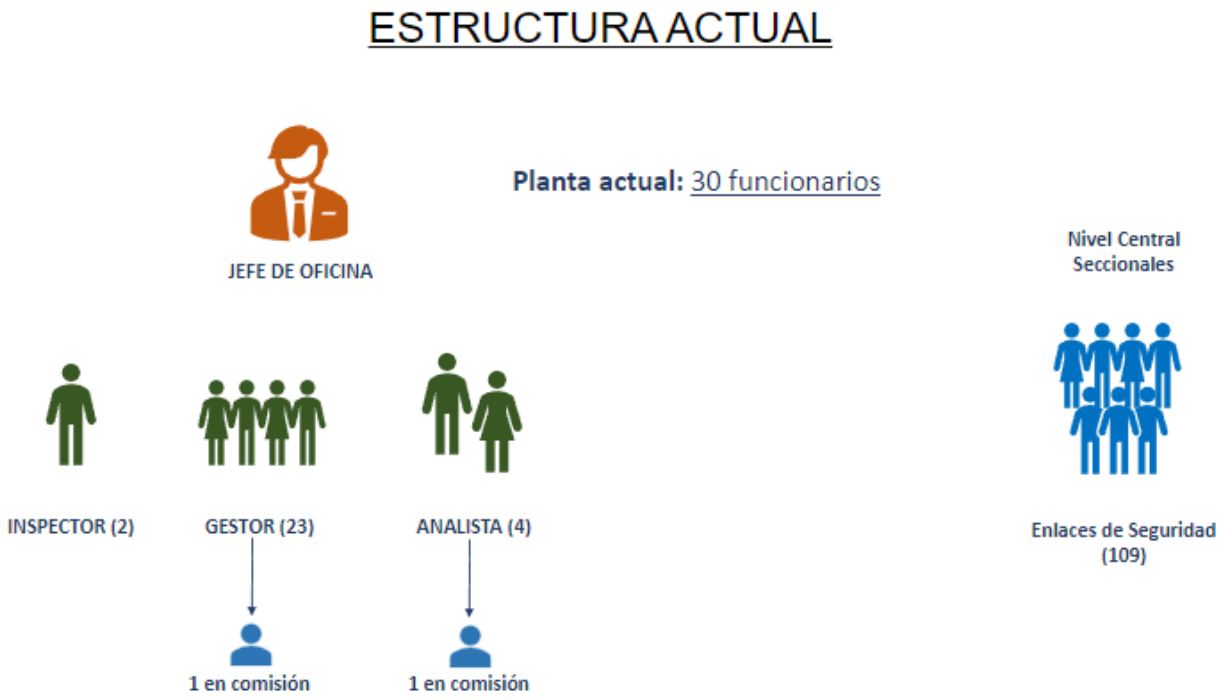

Figura 7: Estructura Oficina de Seguridad de la Información Noviembre 2024

5.4.2 Competencia, toma de conciencia y comunicación

La DIAN ha impartido capacitación a sus funcionarios de la Oficina de Seguridad de la Información (OSI) con respecto a los conocimientos básicos del Modelo de Seguridad y Privacidad de la

26 Resolución DIAN 021 del 28 de enero de 2022, Art. 17, ítem 6, publicada en https://www.dian.gov.co/normatividad/Normatividad/Resoluci%C3%B3n%20000021%20de%2028-01-2022.pdf
27 DIAN. 22 de diciembre de 2020. Decreto 1742 de 2020. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=153986

Información, del Sistema de gestión de Seguridad y Privacidad de la Información, al igual de la gestión de riesgos de seguridad de la información y protección de datos personales y por ello poseen la formación y la educación necesaria para su operación.

Para sensibilizar a los funcionarios, contratistas y demás grupos de interés respecto al Sistema de Gestión de Seguridad y Privacidad de la Información, la entidad cuenta con:

- Un plan de sensibilización de seguridad de la información, mediante el cual se diseñan y construyen piezas comunicativas, sobre temas de interés en seguridad y privacidad de la información, las cuales, son divulgadas periódicamente a través de los diferentes canales oficiales de comunicación de la entidad.
- Un módulo de Protección de datos personales, dentro del curso de Reinducción gestionado a través de la Escuela de la DIAN.
- Talleres de sensibilización en materia de seguridad y privacidad de la información.
- Curso de seguridad de la información a través de la escuela de la DIAN, programa PIC.
- Módulo de seguridad de la información en el curso de teletrabajo
- Desarrollo de la Semana seguridad con cobertura nacional con periodicidad anual.
- Campañas de comunicaciones vía correo electrónico, Conexión (teams) y pagina web.
- Sensibilización relacionada con Asuntos Disciplinarios en la inducción general, la cual también abarca las implicaciones del no cumplimiento a los establecido en las políticas de Seguridad y Privacidad de la información.
- Capacitaciones relacionadas con la gestión de riesgos de seguridad de la información.

De acuerdo con el **MN-IIT-0072 - Manual de Políticas y Lineamientos de Seguridad de la Información** la Subdirección Escuela de Impuestos y Aduanas (SEIA) debe establecer los mecanismos o controles necesarios en sus procedimientos para que los programas de inducción, reinducción, capacitación y sensibilización incluyan y evalúen temas de seguridad y privacidad de la información, y la Oficina de Seguridad de la Información - OSI debe promover una cultura de uso seguro de la información y del ciberespacio para los usuarios internos de la entidad; mediante la ejecución periódica de campañas, programas de concientización y/o sensibilización acerca de los riesgos de ciberseguridad, ciber amenazas, políticas de seguridad y acciones a seguir en caso de presentarse incidentes de seguridad de la información.

La estrategia de Sensibilización y Comunicación de Seguridad y Privacidad de la Información se compone principalmente de las siguientes actividades:

- **Definir la Audiencia**: la correcta definición de la audiencia permitirá al equipo diseñar mecanismos de comunicación y sensibilización eficientes según las necesidades y características de estos, una comunicación asertiva y personalizada facilitará la adaptación y apropiación de las audiencias a nuevos cambios y procesos.
- **Establecer los objetivos de la sensibilización**: se deben definir los objetivos generales de comunicación para la DIAN que permitan la entrega y recepción de los mensajes de manera oportuna y directa.
- **Determinar mensajes, frecuencia y canales de transmisión**: Las comunicaciones serán definidas y planeadas de forma que las audiencias puedan tener la información necesaria y el involucramiento adecuado, facilitando que se logren los niveles de apropiación. Los canales de comunicación internos establecidos por la DIAN son los siguientes:
    - La Diannet

  - Conexión a través de Microsfot Teams
  - Link AL DÍA
  - Link FLASH
  - Link DIRECTIVO
  - Link SECCIONAL
  - Mailing
  - Corresponsales
- **Ejecución del plan de comunicación interna:** construcción de contenidos y piezas de comunicación, además de la entrega de los mensajes a comunicar definidos en conjunto con la dependencia encargada de la DIAN para tal fin y alineados con la estrategia de comunicación de la Entidad.
- **Disposición del personal idóneo (**Capacidades y competencias**):** Disponer del personal capacitado para el desarrollo de las actividades, brindando claridad, eficiencia y manejo de las temáticas relacionadas con el sistema de gestión de Seguridad y Privacidad de la información y el MSPI

La documentación relacionada con la Sensibilización y Concientización en temas asociados a la Gestión de la Seguridad y Privacidad de la Información en la DIAN se definen previamente con la dependencia de comunicaciones.

6. OPERACIÓN

6.1 Planificación e implementación

Durante los años 2023 y 2024, se realizó la gestión de riesgos de seguridad de la información conforme al mapa de procesos indicado en la Figura 5.

Producto de dicha gestión, se obtuvo el perfil general de riesgos de seguridad de la información para los procesos de la DIAN, el cual se visualiza a continuación:

Figura 8 – Perfil de Riesgos (Nov. 2022)

Adicionalmente y aplicando lo descrito en la sección **5.3.3 Plan de tratamiento de los riesgos de seguridad de la información**, se identificaron aquellos controles inefectivos o efectivos con oportunidad de mejora para los riesgos ubicados en las zonas INACEPTABLE, IMPORTANTE o MODERADO y se definieron los planes de tratamiento y nuevos controles para la reducir el riesgo identificado.

Los planes de tratamiento y controles definidos se encuentran registrados en la herramienta GRC, Modulo Riesgos, donde cada proceso refleja el plan necesario para llevar los riegos al estado ACEPTABLE[28]

La Oficina de Seguridad de la Información – OSI a través del líder de riesgos de seguridad de la información y con el apoyo del líder de protección de datos personales es responsable de definir, actualizar, aprobar, publicar y socializar la metodología de gestión de riesgos de seguridad de la

[28] Planes de Tratamiento de Riesgos. https://grc.dian.gov.co/novasecMS/autenticacion.php

información definida para la DIAN (Teniendo en cuenta el decreto 1742 art 10 numeral 2. Funciones oficina seguridad de la información) y de apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. Asimismo, debe informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información, a través de los protocolos definidos en el documento PR-PEC-0242 planificación de la gestión de riesgos.

7. EVALUACION DE DESEMPEÑO

7.1 Seguimiento, medición, análisis y evaluación

7.1.1 Seguimiento

La DIAN a través de la Oficina de Seguridad de la Información – OSI realizo en el 2024 mediciones y evaluaciones periódicas tanto al Sistema de Gestión de Seguridad y Privacidad de Seguridad de la Información, así como al Modelo de Seguridad y Privacidad, al Programa Integral de Protección de Datos Personales y a la Gestión de Riesgos de Seguridad de la Información.

Para ello se definieron los siguientes indicadores de gestión:

Nombre del Indicador/Control	Objetivo	Formula	Calculo Fórmula	Peridiciocidad
1. Gestión de accesos	Identificar la cantidad de cuentas de usuarios no autorizados dentro del servidor del domino.	Número de usuarios activos en el DA/ número de usuarios en la planta y contratos de la DIAN x 100	(1- ((Variable 1 + Variable 2) / Variable 3)))*100	Semestral
2. Derechos de Acceso privilegiado	Identificar que todos los usuarios privilegiados de bases de datos creados en el periodo estén autorizados por el mecanismo definido.	Cantidad de usuarios con accesos privilegiados en las bases de datos/Cantidad de usuarios privilegiados autorizados en Aranda x 100	(Variable 1/ Variable 2)* 100	Semestral
3. Compromiso de Confidencialidad para empleados (Compromisos de confidencialidad suscritos por servidores públicos)	Identifica la cantidad de servidores públicos que suscribieron el acuerdo de confidencialidad de la DIAN.	Servidores públicos que suscribieron el compromiso de confidencialidad / Número de servidores públicos vinculados a la entidad x100	(Variable 1/ Variable 2)* 100	Anual
4. Compromiso de Confidencialidad para contratistas (Compromisos de confidencialidad suscritos por contratistas (personas naturales y personas jurídicas))	Identificar la cantidad de contratistas que suscribieron el acuerdo de confidencialidad de la DIAN.	Contratistas (personas naturales y personas jurídicas) que suscribieron el compromiso de confidencialidad / Número de contatistas (personas naturales y personas jurídicas) vinculados a la entidad en un periodo x100	(Variable 1/ Variable 2)* 100	Anual
5. Responsabilidades posteriores a la desvinculación de los servidores públicos	Identificar una muestra sobre le total de servidores públicos desvinculados para validar que cuenten con el acta de entrega de cargo firmada.	Número de actas de entrega de cargo firmadas/número de servidores públicos desvinculados x100	(Variable 1/ Variable 2)* 100	Semestral
7. Porcentaje de implementación de controles	Identificar el porcentaje de controles de seguridad implementados en la entidad, establecidos en la declaración de aplicabilidad.	Número de controles implementados que se encuentran efectivos/ Número de controles de la Declaración de Aplicabilidad x 100	(Variable 1/ Variable 2)* 100	Anual
9. Gestión de Incidentes de Seguridad de la Información	Identificar la cantidad de incidentes de seguridad de la información gestionados por la entidad.	Número de incidentes de Seguridad de la Información gestionados (cerrados)/ Número de incidentes de Seguridad de la Información reportados por diferentes fuentes x 100	(Variable 1/ Variable 2)* 100	Semestral
11. Gestión de Incidentes de Privacidad de la Información	Identificar y gestionar la cantidad de incidentes de seguridad de la información que afectaron el tratamiento de datos personales de la entidad.	Número de incidentes que afectaron el tratamiento de datos personales/ Total incidentes de seguridad de la información reportados	(Variable 1/ Variable 2)* 100	Semestral
12. Gestión de vulnerabilidades	Identificar la cantidad de vulnerabilidades remediadas por la entidad.	Número de vulnerabilidades altas y muy altas remediadas por la DGIT/número de vulnerabilidades altas y muy altas identificadas en las pruebas del verificar por parte de la OSI	(Variable 1/ Variable 2)* 100	Anual
13. Gestión de procesos disciplinarios asociados a Seguridad y Privacidad de la Información	Identificar el cumplimiento de los procesos disciplinarios asociados a seguridad y privacidad de la información.	Número de procesos disciplinarios asociados a Seguridad y Privacidad de la información gestionados	(Variable 1 / (Variable 2 - Variable 3 - Variable 4)) * 100	Anual
14. Sistema de Gestión de Seguridad de la Información	Identificar el cumplimiento del Plan Anual de Seguridad y Privacidad de la Información.	Número de actividades del Plan de Seguridad y Privacidad de la Información finalizadas/Número total de actividades del Plan de Seguridad y Privacidad de la Información X 100	(Variable 1/ Variable 2)* 100	Anual
15. Auditorias y/o consultorías de revisión al Sistemas de Gestión	Identificar el cumplimiento de la planificación de la ejecución de auditorías y/o consultorías de revisión al SGSPI definido por la entidad.	Número de auditorías y/o revisiones realizadas al SGSPI/ Número de auditorías y/o revisiones planeadas al SGSPI	(Variable 1/ Variable 2)* 100	Anual
16. Programa Integral de Gestión de Datos Personales	Identificar el cumplimiento del Programa Integral de Gestión de Datos Personales definido por la entidad.	Número de actividades principales ejecutadas/ número de actividades principales programadas X100	(Variable 1/ Variable 2)* 100	Semestral
17. Gestión de activos críticos	Identificar los activos críticos de la entidad que cuentan con gestión de riesgos	Número de activos críticos identificados por proceso/ Total de activos identificados por proceso x 100	(Variable 1/ Variable 2)* 100	Anual
18. Control de acceso físico	Identificar el cumplimiento de los criterios relacionados con el control de acceso físico.	Total de criterios cumplidos relacionados con control de acceso físico dentro del formato de verificación física/ total de criterios relacionados con control de acceso físico X100	((Variable 1 / Variable 2) / Variable 3)*100	Anual
19. Efectividad de las medidas de tratamiento implementadas	Identificar el nivel de cumplimiento de los planes de acción definidos para la mitigación de los riesgos, identificados en la gestión de riesgos de seguridad de la información.	Número de medidas de tratamiento ejecutadas/Total de medidas de tratamiento definidas	(Variable 1/ Variable 2)* 100	Semestral
20. Efectividad en la Gestión de Riesgos	Identificar la proporción de riesgos residuales ubicados en zonas importante y/o inaceptables frente al total de los riesgos residuales en la entidad.	Número de riesgos ubicados en zona importante y/o inaceptable/Total de riesgos residuales de seguridad identificados para la entidad	(Variable 1/ Variable 2)* 100	Anual
21. Alcance del sistema de gestión riesgos de seguridad de la información	Identificar el nivel de implementación de la gestión de riesgos de seguridad de la información en la entidad.	Número de dependencias con la gestión de riesgos de seguridad de la información implementada/Total de dependencias de la DIAN	(Variable 1/ Variable 2)* 100	Anual
22. Planes de sensibilización y concientización, relacionados con Seguridad y Privacidad de la información	Identificar el cumplimiento del plan de sensibilización y concientización de Seguridad y Privacidad de la información	Número de actividades de sensibilización y/o capacitación realizadas en Seguridad y Privacidad de la Información/ Número total de actividades de sensibilización y/o capacitación programadas x 100	(Variable 1/ Variable 2)* 100	Anual
23. Formación en Seguridad y Privacidad de la Información	Identificar la cantidad de usuarios que aprueban la formación de seguridad y privacidad de la información en la DIAN.	Número de personas que aprobaron la evaluación de la formación de Seguridad y Privacidad/Número de personas que participaron en la formación de Seguridad y Privacidad X 100	(Variable 1/ Variable 2)* 100	Anual
24.Disponibilidad de servicios	Identificar la cantidad de sistemas de información críticos que poseen planes de contingencia probados.	Sistemas de información críticos con planes de contingencia probados/ Sistemas de información críticos de la entidad	(Variable 1/ Variable 2)* 100	Anual
25.Seguridad en Proyecto de TI	Establecer la cantidad de proyectos tecnológicos en las cuales se tiene elaborada la matriz de riesgos y controles de seguridad de la información.	Proyectos tecnológicos con controles de seguridad identificados / Proyectos tecnológicos en curso durante determinado periodo	(Variable 1/ Variable 2)* 100	Anual
26.Gestion de monitoreo de Seguridad de la Información	Identificar la cantidad de fuentes e infraestructura que reportan eventos de seguridad en el SIEM.	Número de fuentes e infraestructura que reportan eventos de seguridad en el SIEM/ total de infraestructura de la DIAN	(Variable 1/ Variable 2)* 100	Anual

Figura 9 – Indicadores SGSPI (Nov. 2024)

7.1.2 Medición

Los resultados y soportes de la medición de los indicadores se encuentran registrados en GRC, en el módulo Cumplimiento.[29]

De acuerdo con la medición después del ejercicio realizado entre el año 2023 y 2024, el estado actual del Modelo de Seguridad y Privacidad de la Información - MSPI, el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, el Programa Integral de Gestión de Datos Personales - PIGDP y la Gestión de Riesgos de Seguridad de la Información – GRSI, es:

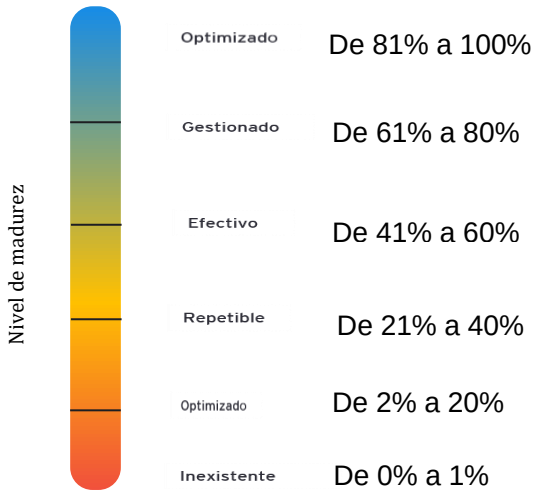

Figura 10 – niveles de madurez (Nov. 2024)

a. **Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI:** La evaluación realizada para los controles del Anexo A de la norma ISO 27001:2022 corresponden a un promedio del 82,3% de cumplimiento.

[29] https://grc.dian.gov.co/novasecMS/autenticacion.php

Figura 11: Resultados Evaluación SGSPI, 2024

b. **Modelo de Seguridad y Privacidad de la Información - MSPI:** La evaluación realizada para el MSPI corresponde a un promedio del 94,4% de cumplimiento.

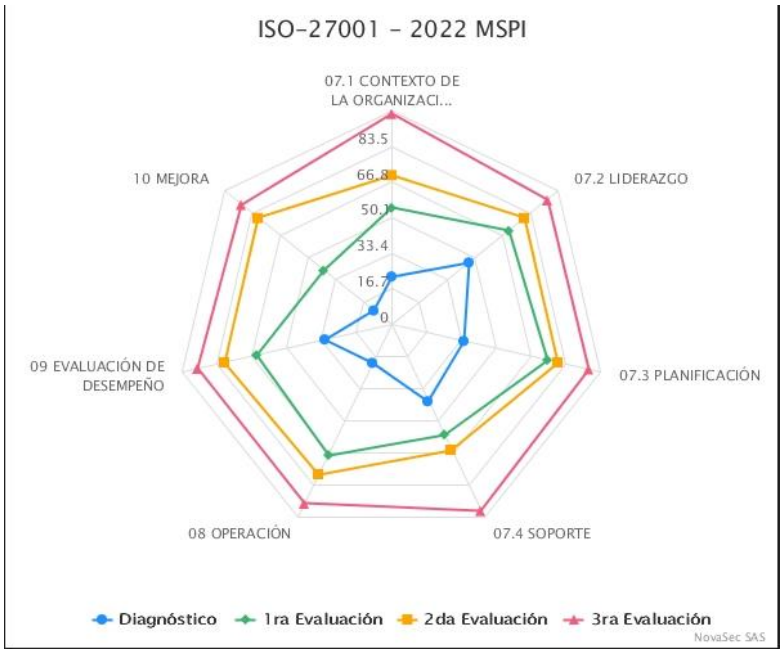

Figura 12: Resultados Evaluación MSPI, 2024

c. **Programa Integral de Protección de Datos Personales:** La evaluación realizada para el MSPI corresponde a un promedio del 94,8% de cumplimiento.

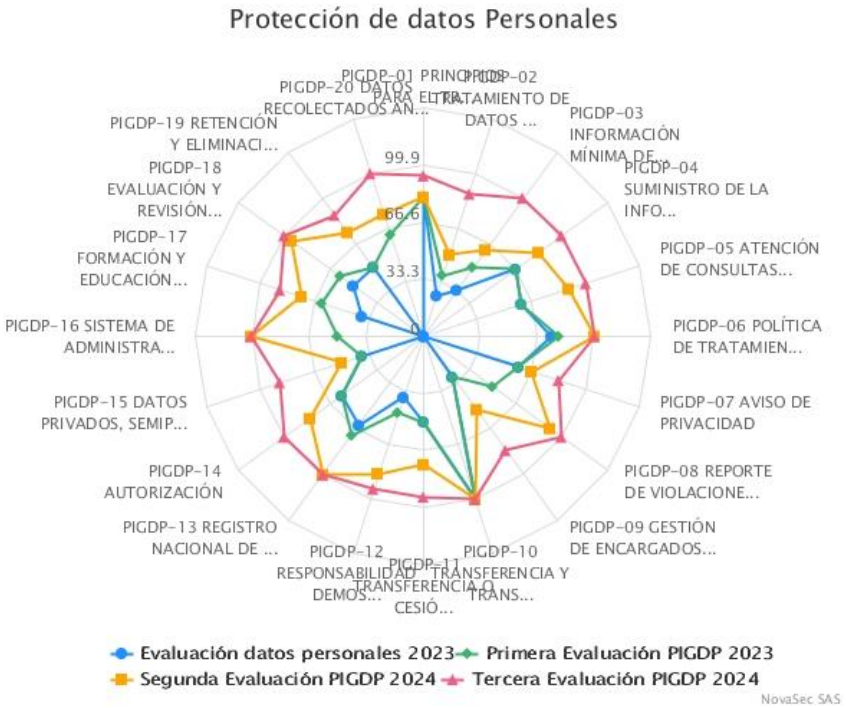

Figura 13: Resultados Evaluación PIGDP, 2024

d. Gestión de Riesgos de Seguridad de la Información: La evaluación realizada para GRSI corresponde a un promedio del 91,2% de cumplimiento.

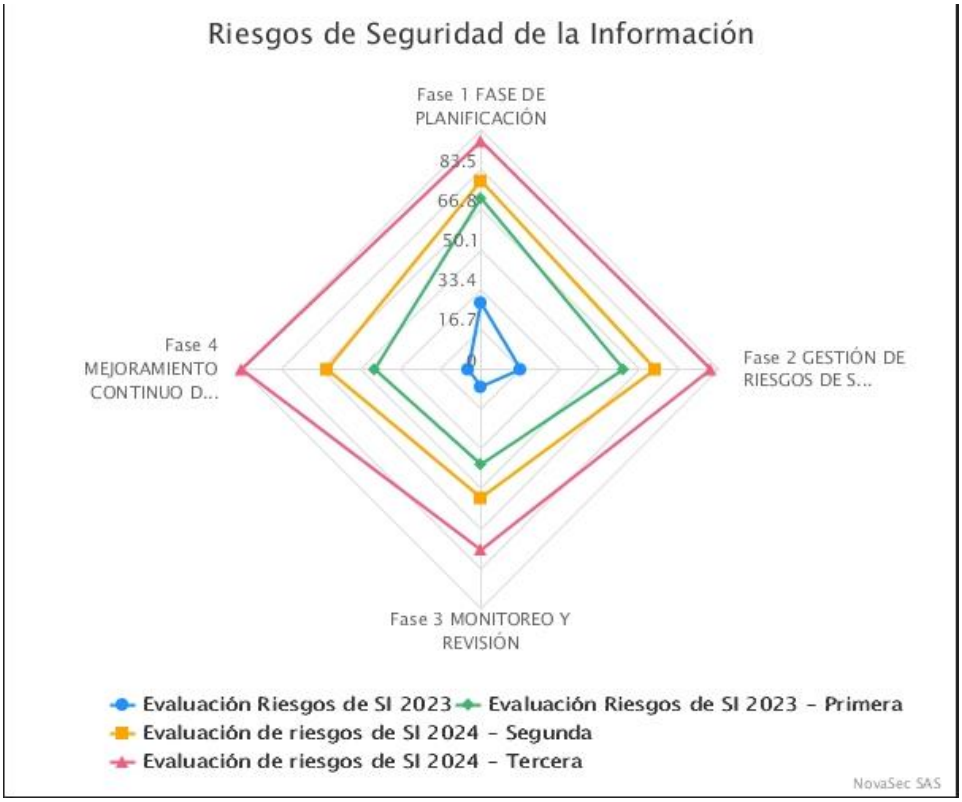

Figura 5: Resultados Evaluación GRSI, 2024

7.2 Auditoría Interna

Durante el último trimestre del 2023, se realizó una consultoría documental al MSPI para el periodo del 1 enero 2022 al 30 junio del 2023 a través de la Oficina de Control Interno y los hallazgos y recomendaciones lo encuentran en el informe AB 2023_11[30]

7.3 Revisión por la dirección

Los temas de seguridad y privacidad de la información, la política y los Indicadores del Sistema de Gestión de Seguridad y Privacidad de la Información, son tratados y aprobados en el Comité Institucional Estratégico, en cumplimiento del decreto 1742 del 2020, ***artículo 77 "****El Comité Institucional Estratégico -CIE será un órgano asesor para el desarrollo de los objetivos y funciones de la DIAN, en cuanto a las funciones propias relacionadas con los asuntos estratégicos de la Entidad. Las funciones del Comité Institucional Estratégico -CIE serán las siguientes:",* ***numeral 6.*** "*Aprobar las Políticas de Gestión de la Entidad, entre otras, la política de seguridad de la información, la política*

[30] INFORME GAB 2023 011.pdf

archivística y/o de gestión documental y la política de gestión del talento humano". De acuerdo con lo anterior, la política de Seguridad de la Información fue aprobada mediante el acta No. 2 de agosto del 2023.
Adicionalmente en el Comité Institucional de Gestión y Desempeño de fecha 17 de agosto de 2023, mediante acta N" 2 se presentaron el Modelo de Seguridad y Privacidad de la Información MSPI, seguridad de la Información, Sistema de Seguridad de la Información y el programa Integral de Gestión de Datos Personales.

En desarrollo del comité Institucional de Gestión y Desempeño del día 13 de diciembre de 2023, mediante acta N° 04, se presentó Matriz de Roles y Responsabilidades, SGSPI y el resultado de la gestión de Riesgos de Seguridad y Privacidad realizada durante el año.

De la misma manera, el 30 de enero de 2024 en el Comité Institucional de Gestión y Desempeño dentro del Acta N°1 se aprobó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, y el Plan de Seguridad y Privacidad de la información.

8. MEJORAMIENTO CONTINUO

8.1 Mejora

Conforme a los resultados obtenidos en **7.1 Seguimiento, medición, análisis y evaluación y 7.2 Auditoría interna**, se debe realizar las acciones correspondientes para satisfacer el objetivo del control y llegar a 80 puntos o superior según la escala de valoración de los controles de seguridad definida. Esta información se ve reflejada en la herramienta GRC, modulo planes[31]

Posterior al cierre de las acciones de mejora enunciadas anteriormente se procede a repetir el ciclo desde **5.3.2 Valoración de los riesgos de seguridad de la información**.

9. GLOSARIO:

El glosario correspondiente al presente documento puede ser consultado en el Anexo Definiciones y Siglas de Seguridad de la Información[32]

[31] Plan de riesgos 2024 y Plan de Seguridad y Privacidad de la Información 2024.
[32] Anexo Definiciones y Siglas de Seguridad de la Información.docx.

10. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
1	13/07/2020	29/09/2021	Versión inicial.	
2	30/09/2021	14/09/2023	Versión 2, que reemplaza lo establecido en la versión 1. Se generaron ajustes en el documento, relacionados con el nombre del proceso de acuerdo con la nueva estructura de procesos establecida en el considerando de la Resolución 060 del 11 de junio del 2020 y el código alfanumérico en la(s) pagina(s) 11, 13, 17, 35 y 43. Se ajustaron las dependencias de acuerdo con la nueva estructura establecida en el Decreto 1742 del 22 de diciembre de 2020 y en la Resolución 00070 del 09 de agosto de 2021. En el numeral 1.2.9.3 Estimación del riesgo de seguridad digital (página 28) se elimina el instructivo relacionado (IN-IC-0059 Metodología para la ejecución del procedimiento de implementación de gestión de riesgos), debido a que dicho documento no hace parte del actual listado maestro de documentos. Cabe aclarar, que el contenido técnico de los documentos no presenta cambios respecto a la versión anterior. Por lo tanto, cualquier consulta respecto a los contenidos técnicos de los mismos debe efectuarse a los elaboradores técnicos y revisores de la versión anterior.	
3	15/09/2023	19/02/2025	Versión 3, que reemplaza lo establecido en la versión 2. Se actualizó el documento alineando los capítulos al MSPI versión 4 emitido el 22/02/2021 por el Ministerio de Tecnologías de la Información y las Comunicaciones y la gestión realizada durante el último año por la Oficina de Seguridad de la Información de la DIAN	Esta versión corresponde a Información Pública.
4	20/02/2025		Versión 4, que reemplaza lo establecido en la versión 3. Se reviso y se actualizó el documento ajustando el estado actual del MSPI, SGSPI, GRSI, PIDP y Política de seguridad de la información.	Esta versión corresponde a Información Pública.

Elaboró:	Yeinny Andrea Bolivar L. Edgar Fernando Aviles G. **Elaboración Técnica**	Analista III Gestor III	Oficina de Seguridad de la Información
	Tito Alejandro Menjura M. Ricardo Estefan Bareño B **Elaboración metodológica**	Gestor II Gestor II	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Carlos Javier Ibañez S.	Gestor II	Oficina de Seguridad de la Información
Aprobó:	Hugo Alcides Pérez P.	Jefe Oficina de Seguridad de la Información	Oficina de Seguridad de la Información