Modelo de Seguridad y Privacidad de la Información

Proceso Información, Innovación y Tecnología

Oficina de Seguridad de la Información
Versión 03
Código OD-IIT-0001
Año 2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO: 5
3. CICLO DE OPERACIÓN 6
4. DIAGNÓSTICO 7
4.1 Modelo de Seguridad y Privacidad de la información - MSPI 8
4.2 Sistema de Gestión de Seguridad y Privacidad de la Información (Controles Anexo A de la ISO 27001:2013) – SGSPI 9
4.3 Programa Integral de Gestión de Datos Personales 9
4.4 Gestión de Riesgos de Seguridad de la Información - GRSI 10
5. PLANIFICACIÓN 11
5.1 Contexto 11
5.1.1 Comprensión de la organización y de su contexto 11
5.1.2 Necesidades y expectativas de los interesados 14
a. Requisitos e información general 14
5.1.3 Definición del alcance del MSPI 15
5.2 Liderazgo 16
5.2.1 Liderazgo y Compromiso 16
5.2.2 Política de seguridad y privacidad de la información 17
5.2.3 Roles y responsabilidades 18
5.3 Planificación 18
5.3.1 Identificación de activos de información e infraestructura critica 18
a. Identificación de Activos de Información 18
b. Infraestructura Crítica 19
5.3.2 Valoración de los riesgos de seguridad de la información 19
5.3.3 Plan de tratamiento de los riesgos de seguridad de la información 21
5.4 Soporte 22
5.4.1 Recursos 22
5.4.2 Competencia, toma de conciencia y comunicación 23
6. OPERACIÓN 24
6.1 Planificación e implementación 24

7. EVALUACION DE DESEMPEÑO 26
7.1 Seguimiento, medición, análisis y evaluación 26
7.1.1 Seguimiento 26
7.1.2 Medición 26
7.2 Auditoría Interna 31
7.3 Revisión por la dirección 31
8. MEJORAMIENTO CONTINUO 32
8.1 Mejora 32
9. GLOSARIO: 32
10. CONTROL DE CAMBIOS 33

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

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):

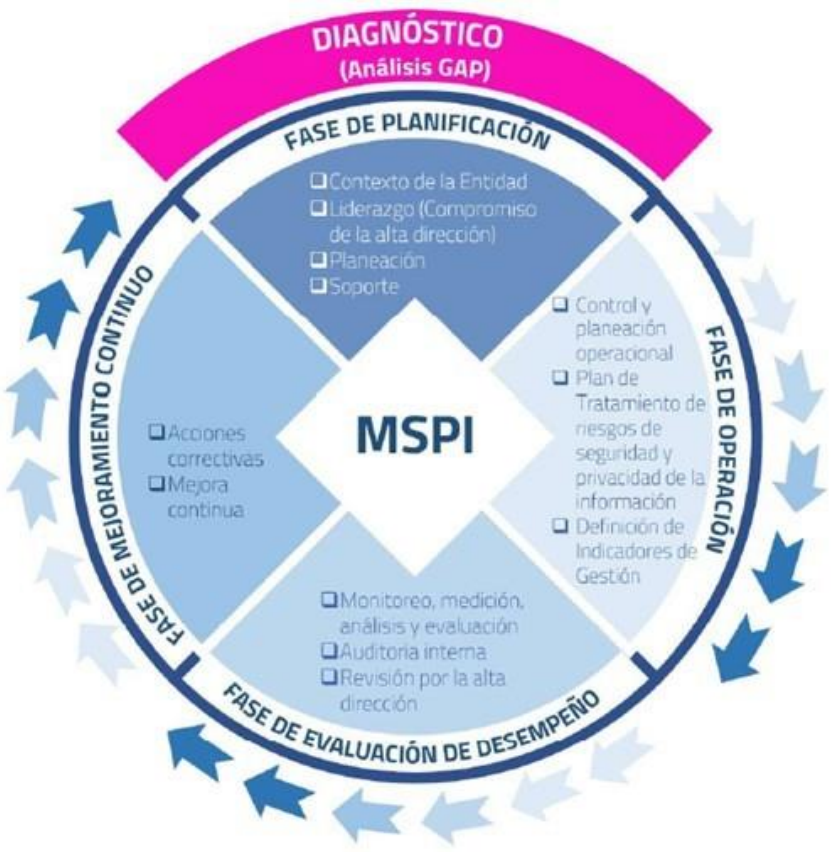


Figura 1 - Ciclo Modelo de Seguridad y Privacidad de la Información (Tomado MSPI - Min Tic V4)

Con el propósito de avanzar en la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información, la DIAN a través del Programa de Apoyo a la Modernización de la DIAN, financiado con recursos del Contrato de Préstamo BID 5148/OC-CO, ha otorgado en el año 2022, el contrato No. 92872-055-2022 al APCA Ernst & Young SAS, Mancera S.C. y EY Addvalue Asesores Cia con el

[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

siguiente objeto, “Realizar actividades de implementación, mantenimiento, administración, fortalecimiento y seguimiento al Sistema de Gestión de Seguridad y Privacidad de la información (SGSPI) de la Entidad”.

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, así como del Programa Integral de Gestión de Datos Personales y de la Gestión de Riesgos de Seguridad de la Información. En el periodo del 7 de febrero al 24 de Marzo de 2023, se desarrolló la evaluación del nivel de madurez del Modelo de Seguridad y Privacidad de la Información - **MSPI**, del Sistema de Gestión de Seguridad y Privacidad de la Información - **SGSPI**, del Programa Integral de Gestión de Datos Personales - **PIGDP** y de la Gestión de Riesgos de Seguridad de la Información – **GRSI** para el año 2023; 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:

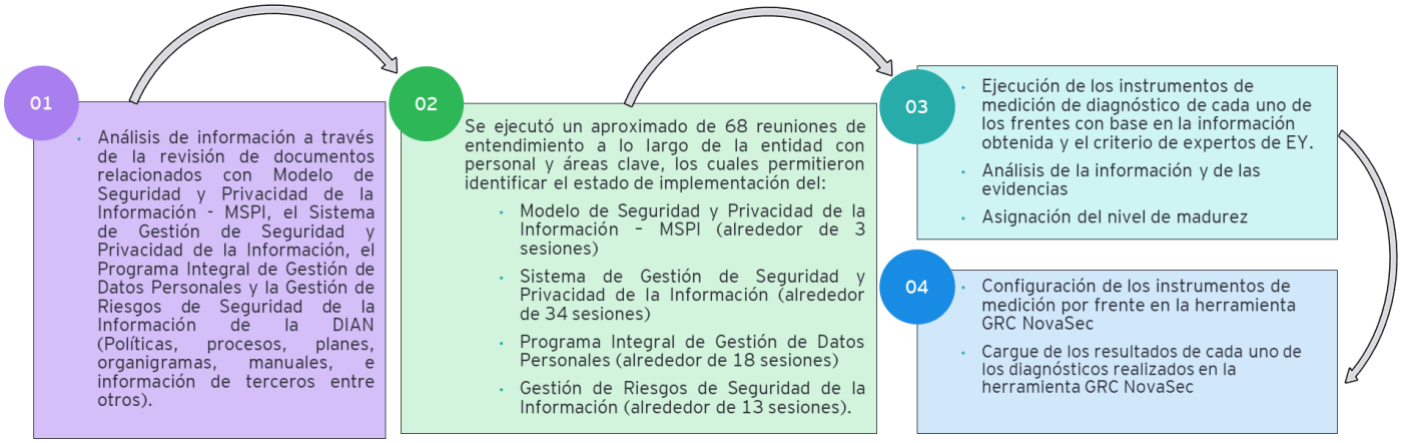


Figura 2: El Diagnóstico fue realizado entre el 7 de febrero y el 24 de marzo de 2023

De manera adicional se implementó la siguiente metodología para la ejecución del Diagnóstico, la cual se dividió 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 propuesta por EY para la ejecución del Diagnóstico

La evaluación se desarrolló con una escala establecida y aprobada de manera independiente para el MSPI, SGSPI, GRSI y PIGDP. Esta escala de medición se realizó considerando los siguientes niveles de madurez, los cuales se alinearon a lo establecido por el MinTic.

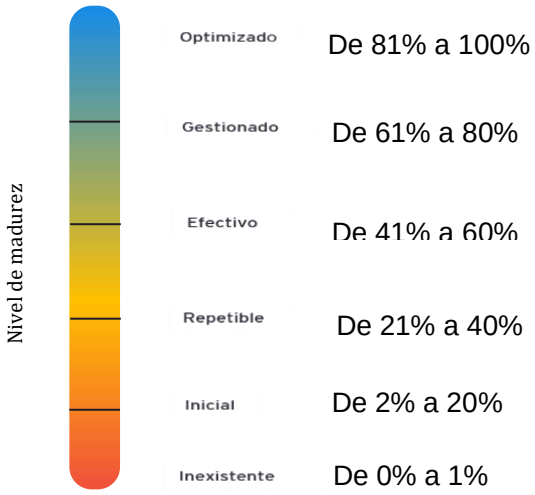


Figura 4: Valores de la escala de medición

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 27001:2013) – SGSPI

Los resultados del Diagnóstico del SGSI 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 incluye un análisis de cada uno de los factores claves que contempla:

- Político:

EXTERNO	INTERNO
POLÍTICO: Los cambios de gobierno y las políticas públicas en países con los que Colombia tiene fuertes lazos comerciales. Estos cambios pueden afectar la legislación y regulación en materia de comercio exterior y aduanas, lo que, a su vez, podría tener un impacto en las operaciones y responsabilidades de la DIAN. Por ejemplo, si un país socio cambia su política comercial y establece nuevos aranceles o regulaciones más estrictas, la DIAN tendría que adaptarse a estos cambios y ajustar sus procesos y procedimientos internos para asegurar el cumplimiento de las nuevas normas y mantener el flujo comercial.	**POLÍTICO:** El direccionamiento estratégico y el liderazgo dentro de la DIAN, lo cual, implica cómo la institución establece sus objetivos, directrices y modelos operativos para cumplir con su misión, además de la eficacia del liderazgo en la implementación de dichos objetivos. La capacidad de la DIAN para coordinar y articular internamente sus funciones, roles y responsabilidades, así como promover el trabajo en equipo y la rendición de cuentas, puede afectar su eficiencia y éxito en la gestión aduanera, tributaria y cambiaria en Colombia.

- Económico:

EXTERNO	INTERNO
ECONÓMICO: La disponibilidad de capital y el acceso a los mercados financieros internacionales pueden influir en la capacidad de las empresas colombianas para financiar sus operaciones de importación y exportación, así como en la atracción de inversión extranjera directa en el país. Por ejemplo, si los mercados financieros internacionales experimentan turbulencias o si las condiciones crediticias se endurecen, las empresas colombianas podrían enfrentar dificultades para obtener financiamiento, lo que afectaría el volumen de comercio y, en última instancia, las operaciones de la DIAN, como pueden ser establecer normas y regulaciones para un comercio justo y sostenible por el país.	**ECONÓMICO:** El presupuesto de funcionamiento de la entidad, el cual, determina la capacidad de la DIAN para llevar a cabo sus funciones, invertir en infraestructura y mejorar su capacidad instalada. Un presupuesto limitado podría afectar la eficiencia y cumplimiento de las operaciones aduaneras, tributarias y cambiarias, mientras que un aumento en el presupuesto podría permitir la modernización de varios procesos, la contratación de personal adicional y la mejora de la infraestructura y tecnología, lo que optimizaría el desempeño general de la entidad.

- Social:

EXTERNO	INTERNO
SOCIAL: La situación de seguridad y la percepción del orden público pueden influir en la confianza de los inversionistas extranjeros y en la disposición de las empresas locales e internacionales para realizar operaciones de comercio en Colombia. Un entorno de orden público inestable puede generar mayores desafíos para la DIAN en términos de brindar seguridad en las operaciones aduaneras y la integridad de las cadenas de suministro. También es importante que la DIAN comprenda las diferentes culturas presentes en Colombia y en los países con los que comercia, para poder establecer relaciones de confianza y respeto mutuo. Teniendo en cuenta sus características demográficas y así adaptarse a las necesidades y oportunidades que se presentan en estas. Así mismo, la responsabilidad social al establecer y supervisar las normas y reglamentaciones relacionadas con el comercio, para asegurarse de que se respeten los derechos humanos, laborales y ambientales.	**SOCIAL:** La calidad y competencia del personal en la DIAN son cruciales para cumplir con la eficiencia y eficacia de las operaciones aduaneras y tributarias. Así mismo, son importantes los valores y principios de la DIAN debido a que estos pueden ser usados como guías para la toma de decisiones del personal, asegurando así la ética y profesionalismo al realizar sus actividades. Además, un clima y un entorno laboral positivo, seguro y saludable, pueden mejorar la satisfacción y retención del personal, reduciendo los riesgos de accidentes laborales y enfermedades, lo que a su vez afecta la capacidad de la entidad para cumplir con sus objetivos en tiempo y mantener altos niveles de rendimiento.

- Tecnológico:

EXTERNO	INTERNO
TECNOLÓGICO: Los avances en tecnología y el acceso a sistemas de información externos, pueden influir en la capacidad de Colombia para mantenerse competitiva en el comercio internacional y en el desarrollo de soluciones digitales para los servicios públicos. Por ejemplo, si otros países adoptan tecnologías actuales para agilizar sus operaciones aduaneras y mejorar la seguridad, Colombia también deberá invertir en tecnologías similares para mantenerse al día y seguir cumpliendo con la eficiencia en sus operaciones aduaneras, tributarias y cambiarias.	**TECNOLÓGICO:** La DIAN debe confirmar que sus sistemas de información estén en línea con los avances tecnológicos actuales y futuros, y que sean capaces de manejar grandes volúmenes de datos de manera segura y eficiente. También es crucial confirmar la interoperabilidad entre los sistemas de información de la DIAN y otros organismos gubernamentales relevantes como pueden ser MinTIC, para facilitar la colaboración y el intercambio de información. La inversión en tecnología y la capacitación del personal en el uso de herramientas tecnológicas avanzadas también son importantes para asegurar la eficiencia y la eficacia de las operaciones de la DIAN.

- Ecológico

EXTERNO	INTERNO
ECOLÓGICO: La DIAN deberá colaborar estrechamente con otras entidades gubernamentales y organizaciones internacionales para cumplir de manera efectiva con la implementación de regulaciones ambientales en el comercio internacional. Debe tener en cuenta las políticas y cambios normativos necesarios para contrarrestar las consecuencias de eventos como riesgos naturales y promover políticas propias para contribuir a la gestión sostenible de los recursos naturales.	**ECOLÓGICO:** La DIAN debe implementar prácticas de gestión ambiental y control operacional, como la gestión de residuos y el consumo responsable de recursos. Además, la entidad debe confirmar el cumplimiento de los requisitos legales ambientales, tanto a nivel nacional como internacional. Al adoptar una gestión ambiental sólida, la DIAN puede reducir su impacto ecológico y contribuir a un comercio más sostenible en Colombia.

- Legal:

EXTERNO	INTERNO
LEGAL: La relación de la DIAN con otras entidades públicas, privadas y ONG's a nivel nacional e internacional, pueden afectar el marco legal y regulatorio en el que opera la DIAN, así como su capacidad para colaborar en la implementación y el cumplimiento de políticas y normativas en materia de aduanas y tributación. Por ejemplo, la DIAN podría necesitar trabajar en conjunto con organizaciones internacionales y otras agencias gubernamentales para asegurar el cumplimiento de acuerdos comerciales, regulaciones de importación y exportación, la prevención del contrabando y la evasión fiscal.	**LEGAL:** La relación con otras dependencias, terceros y contribuyentes dentro de la propia institución y en el ámbito nacional, puede afectar la capacidad de la DIAN para establecer relaciones efectivas y transparentes con sus dependencias internas, así como con empresas, contribuyentes y otras partes interesadas, es crucial para lograr un buen funcionamiento y el cumplimiento de las leyes y regulaciones en materia aduanera y tributaria. La DIAN debe asegurar que sus procesos internos y externos estén alineados con las leyes aplicables y promover una comunicación clara y oportuna con todas las partes involucradas.

El detalle del contexto interno y externo de la DIAN y la normativa relacionada, se encuentran desarrollados en el documento Análisis PESTEL[5].

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.xlsx[6]

[5] Documento con el Análisis PESTEL.docx
[6] Documento con la Normatividad del análisis PESTEL V1_0.xlsx

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 implementación 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” 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 objetivo y el alcance del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN, incluida en el documento **OD-IIT-0001 Modelo de Seguridad y Privacidad de la Información**, 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 4 de 2021**, para determinar dentro de estas definiciones las partes interesadas que afecten el desarrollo del Modelo de Seguridad y Privacidad de la Información MSPI-DIAN.

[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.

- 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 puede ser consultada en los documentos asociados a: **Planes e Identificación de las necesidades y expectativas de las partes interesadas[8].**

5.1.3 Definición del alcance del MSPI

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

- Modelo de procesos[9]
- Modelo organizacional[10]
- Servicios tecnológicos de acuerdo con la identificación de activos de información
- Arquitectura Digital[11]
- Presupuesto disponible para implementación
- 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 los 8 macroprocesos enmarcados en los procesos Estratégicos, Misionales, Habilitantes y de Aseguramiento, tanto en el nivel central como en el nivel seccional de la UAE – DIAN, teniendo en cuenta el ciclo de vida de la información en el desarrollo de su misión institucional y cumplimiento de sus objetivos estratégicos., Así mismo, aplica a todos los usuarios internos y externos de la UAE- DIAN (servidores públicos, funcionarios vinculados a la planta

[8] Planes e Identificación de las necesidades y expectativas de las partes interesadas.docx
[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
[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] Documento con el análisis PESTEL.docx
[14] Planes e Identificación de las necesidades y expectativas de las partes interesadas.docx

permanente y provisional, contratistas, consultores, pasantes, proveedores de bienes, entidades del estado, entes de control) y otros terceros que desempeñen alguna actividad en las instalaciones de la UAE - DIAN o a nombre de esta y de acuerdo con el contexto definido.

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

5.2 Liderazgo

5.2.1 Liderazgo y Compromiso

De acuerdo con lo definido en el Comité Institucional de Gestión y Desempeño (resolución **000021 del 28 de enero de 2022),** la DIAN adopta el Modelo Integrado de Planeación y Gestión MIPG y se establece que a la Oficina de Seguridad de la Información - OSI le corresponde asegurar la implementación en línea con lo estipulado en el artículo 17, **numeral 6. "**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 la Estrategia de Gobierno en Línea, 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 el de Seguridad y Privacidad de la Información, la DIAN creó la Oficina de Seguridad de la Información - OSI mediante Decreto 2183 del 23 de diciembre de 2017 asignando las funciones correspondientes y haciendo parte del Comité Institucional Estratégico. De esta forma, también se da cumplimiento a lo establecido en la Política de Gobierno Digital, 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.

Como parte de la gestión estratégica de la entidad se estableció el objetivo de "Transformación Tecnológica", el cual incluye como uno de los objetivos de contribución, el siguiente: "Diseñar e implementar el plan de seguridad de la información"; por lo cual la UAE – DIAN para asegurar la dirección estratégica y la implementación de la Política de Seguridad y Privacidad de la información, define los objetivos de Seguridad y Privacidad de la Información los cuales pueden ser consultados en la Política General de Seguridad y Privacidad de la Información de la entidad[16].

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

- La adopción de los controles establecidos en el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI, el cual se basa en el Anexo A de la norma ISO 27001:2022. Así como en la adopción de los controles adicionales necesarios que demuestren efectividad y eficacia en la disminución de la probabilidad y el impacto de riesgos identificados.
- La declaración de la política para la gestión de riesgos de seguridad de la información incorporada en la Política General de Riesgos de la entidad.
- La 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*

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

[16] DIAN. 30 de noviembre de 2022. 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

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.

- Comunicando la importancia de su gestión a toda la entidad a través del plan anual de sensibilización y cultura y el logro de sus objetivos y con la presentación de resultados ante el Comité Institucional de Gestión y Desempeño. El plan de sensibilización se relaciona en el documento de la Estrategia de Gestión del Cambio SGSPI y el documento con el Diseño y Plan con las campañas de sensibilización y concientización.
- Confirmando que se cumplan los resultados previstos a través de los monitoreos y seguimientos definidos en sus procedimientos.
- Revisando periódicamente el desarrollo de su gestión e identificando desviaciones que impidan su desarrollo a través de los indicadores de gestión definidos por la Oficina de Seguridad de la Información - OSI en la documentación asociada con Indicadores de Seguridad de la Información.

5.2.2 Política de seguridad y privacidad de la información

Mediante el Comité Institucional Estratégico de la DIAN realizado el 17 de agosto de 2023, fue aprobada la actualización de la Política de Seguridad y Privacidad de la Información[17] 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 del Comité Institucional Estratégico que se llevó a cabo el 17 de agosto de 2023. 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. Clasificación de la información
3. Transferencia de información
4. Control de acceso
5. Seguridad de la información en las relaciones con los proveedores
6. Seguridad de la información para el uso de servicios en la nube
7. Derechos de propiedad intelectual
8. Protección de registros
9. Privacidad y protección de la información de identificación personal (PII)
10. Trabajo a distancia
11. Escritorio despejado y pantalla despejada
12. Gestión de vulnerabilidades técnicas
13. Gestión de la configuración
14. Copia de seguridad de la información
15. Inicio sesión

Así mismo, la alta dirección de la DIAN estableció la política para la administración de riesgos de seguridad de la información, la cual se alinea con las políticas para la gestión de riesgos de la entidad.

[17] Ibid.

Esta política confirma el compromiso de la alta dirección para la gestión de riesgos de seguridad de la información y define sus niveles de responsabilidad, los mecanismos para su comunicación, su objetivo, alcance y todos los elementos que apoyen su desarrollo[18].

5.2.3 Roles y responsabilidades

En el año 2020, luego de la restructuración de la DIAN mediante el **Decreto 1742 de 2020**[19] se asignan las funciones a la Oficina de Seguridad de la Información - OSI, vigentes a la fecha y se establece el Comité Institucional Estratégico -CIE en el Capítulo 6, Artículo 77, donde se define como una de sus funciones 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.

En cuanto a la matriz de roles y responsabilidades 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, corresponde a las Direcciones Seccionales y la tercera corresponde a la Matriz de Roles y Responsabilidades de la Oficina de Seguridad de la Información – OSI en la cual se encuentran los roles asociados a los dominios del SGSPI frente a las funciones de la OSI. Esta matriz se encuentra en el Listado Maestro de Documentos de la entidad, denominada Matriz de Roles y Responsabilidades en Seguridad [20]

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 el GRC de Novasec que es 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 2022, en la DIAN se encuentran asignados 128 enlaces de seguridad y privacidad de la información a nivel nacional.

[18] Política de Gestión de Riesgos de Seguridad de la Información

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

[20] Matriz de Roles y Responsabilidades en Seguridad

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 Servicios Tecnológicos:
  - Inventario y caracterización de servicios tecnológicos
- Dominio de Sistema de Información:
  - Inventario y caracterización de sistemas de información
  - Inventario de servicios web publicados
- Dominio de Información:
  - Inventario y caracterización de bases de datos
  - Directorio de datos abiertos de la entidad
  - Directorio de sistemas de información

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.[21]

5.3.2 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, es por ello por lo que considera como importante:

- 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

[21] Anexo Definiciones y Siglas de Seguridad de la Información

- 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.

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 5: 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[22]. 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 2020 de MINTIC[23].

[22] 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

[23] 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

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.

Cabe destacar que las definiciones de los roles y sus responsabilidades tienen 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 Aplicabilidad[24], estos controles 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* y que en el momento de la valoración se escogió como opción de Tratamiento, "*Reducir/mitigar*".

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

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.**

[24] Declaración de Aplicabilidad

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"[25], se ha conformado la Oficina de Seguridad de la Información - OSI con funciones definidas en el **Decreto DIAN 1742 de 2020, Art. 10**[26], a esta oficina pertenecen 17 funcionarios distribuidos de la siguiente manera:

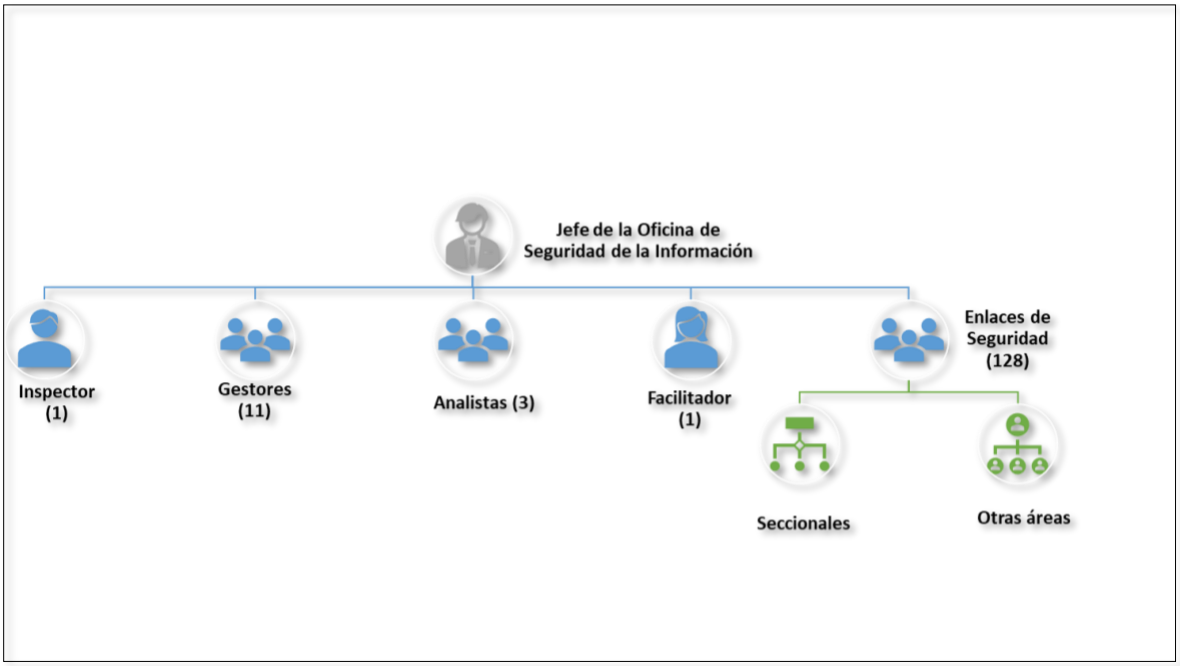


Figura 6: Estructura Oficina de Seguridad de la Información Mayo, 2023

La información relacionada con los recursos de personal, funciones y competencias de la Oficina de Seguridad de la Información – OSI puede ser consultada en el Manual de Funciones de la entidad y en la Matriz de Roles y Responsabilidades de la Oficina de Seguridad de la Información

Se considera que la DIAN ha invertido recursos para el fortalecimiento de la Seguridad y Privacidad en la entidad, teniendo en cuenta las implementaciones que se desarrollarán durante 2023 y parte del 2024 a través de la Consultoría contratada para "Realizar actividades de implementación,

25 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
26 DIAN. 22 de diciembre de 2020. Decreto 1742 de 2020. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=153986

mantenimiento, administración, fortalecimiento y seguimiento al Sistema de Gestión de Seguridad y Privacidad de la información (SGSPI) de la DIAN".

5.4.2 Competencia, toma de conciencia y comunicación

La DIAN confirma que cuenta con funcionarios capacitados para la gestión del 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 y que estos poseen la formación, educación y experiencia necesaria para su implementación.

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 anual de sensibilización y cultura, 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 en el mes de septiembre
- 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 definida para el Programa de Apoyo a la Modernización de la DIAN.
- **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 encuentra definida en los documentos **Estrategia gestión del cambio SGSPI**[27], **y Planeación y diseño de las campañas de sensibilización**[28]

6. OPERACIÓN

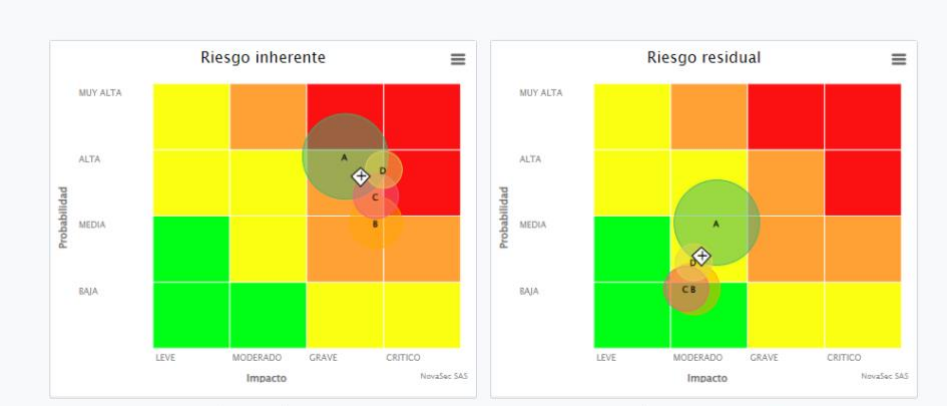
6.1 Planificación e implementación

Durante los años 2021 y 2022, se realizó la gestión de riesgos de seguridad de la información en las siguientes dependencias:

- Oficina de Seguridad de la Información
- Subdirección de Información y Analítica
- Subdirección Centro de Trazabilidad Aduanera
- Subdirección de Estudios Económicos
- Subdirección de Análisis de Riesgos y Programas

Producto de dicha gestión, se obtuvo el perfil general de riesgos de seguridad de la información para las dependencias mencionadas, el cual se visualiza a continuación:

[27] Estrategia gestión del cambio SGSPI
[28] Planeación y diseño de las campañas de sensibilización



	Proceso	Riesgos	Riesgo inherente					Riesgo residual				
			Impacto	Valor	Probabilidad	Valor	Perfil	Impacto	Valor	Probabilidad	Valor	Perfil
◈	Perfil consolidado [Promedio]	163	GRAVE	2.7	ALTA	2.6	IMPORTANTE	MODERADO	1.4	MEDIA	1.4	MODERADO
A	Seguridad de la información (Nuevo)	71	GRAVE	2.5	ALTA	2.9	IMPORTANTE	MODERADO	1.6	MEDIA	1.9	MODERADO
B	Gestión del riesgo y programas (Nuevo)	38	GRAVE	2.9	MEDIA	1.9	IMPORTANTE	MODERADO	1.3	BAJA	0.9	ACEPTABLE
C	Gobernanza de datos, Analítica y Estudios Económicos (Nuevo)	31	GRAVE	2.9	ALTA	2.3	IMPORTANTE	MODERADO	1.2	BAJA	0.9	ACEPTABLE
D	Operación aduanera (Nuevo)	23	GRAVE	3	ALTA	2.7	IMPORTANTE	MODERADO	1.3	MEDIA	1.3	MODERADO

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 o IMPORTANTE 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 publicados en el repositorio de SharePoint de la OSI[29]

Adicionalmente según lo definido en el instructivo **CT-IIT-0132 gestión de riesgos de seguridad de la información** y el documento **MN-IIT-0075 - Manual de usuario para la gestión de riesgos de seguridad de la información**, los planes de Tratamiento se deben cargar en la herramienta GRC NovaSec, en el módulo de Riesgos, en cada uno de los controles y riesgos sobre los cuales se definió el plan de mejora.

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 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. Así mismo 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**.

Durante el año 2023 se espera ampliar la Gestión de Riesgos de Seguridad de la Información a las áreas que contemple el alcance de Sistema de Seguridad y Privacidad de la DIAN; esta gestión se documenta en el **Registro con los resultados de la aplicación de los procedimientos de gestión de riesgos de seguridad**

[29] Planes de Tratamiento de Riesgos. \\diancolombia.sharepoint.com\DocumentacionOSI\PlanesdeTratamientodeRiesgos

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 identifica la necesidad de realizar seguimientos, mediciones, análisis y evaluaciones 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, por lo cual, se han realizado encuestas y evaluaciones a través de la herramienta de GRC Novasec, las cuales no establecen una periodicidad constante. Así mismo, se ha incluido dentro de la cartilla **CT-IIT-0132 - Gestión de riesgos de seguridad de la información** los seguimientos que se consideran necesarios para evidenciar cualquier tipo de desviación que se pueda presentar en la Gestión de los Riesgos de Seguridad de la Información.

Para continuar con la implementación del SGSPI se contempló el fortalecimiento de la Gestión de la Seguridad y Privacidad a través del contrato de Consultoría cuyo objeto corresponde a “Realizar actividades de implementación, mantenimiento, administración, fortalecimiento y seguimiento al Sistema de Gestión de Seguridad y Privacidad de la información (SGSPI) de la DIAN".

7.1.2 Medición

El SGSPI tiene definidos los siguientes indicadores, para medir el cumplimiento de la ejecución de los controles relevantes del sistema:

CONTROL	NOMBRE DEL INDICADOR	FORMULA
5.1.1 Políticas para la seguridad de la información	políticas de seguridad y privacidad de la información	Número de políticas específicas de seguridad y privacidad de la información implementadas/Número total de políticas específicas de seguridad y privacidad de la información por implementar X100
5.1.2. revisión de las políticas de seguridad de la información	Frecuencia de las revisiones de la política de seguridad y privacidad de la información	política de seguridad y privacidad de la información actualizada y aprobada por la alta dirección
6.1.1. Roles y responsabilidades para la seguridad de la información	Roles y responsabilidades	Número de personas desvinculadas con roles activos/Número total de personas desvinculadas en el período x100
7.1.1. Selección e investigación de antecedentes del personal	Protección de datos personales (Autorización tratamiento datos personales)	Número de empleados que firman autorización para el tratamiento de datos personales en la entidad/Total de funcionarios de la entidad X 100
7.1.2. Términos y condiciones del empleo	Compromisos de Confidencialidad para empleados (Compromisos de confidencialidad suscritos por empleados)	Funcionarios que suscribieron compromisos de confidencialidad / Número de funcionarios vinculados a la entidad en un periodo x100
7.2.2 Toma de conciencia, educación y formación en seguridad de la información	Planes de sensibilización, capacitación y comunicaciones, relacionados con Seguridad y Privacidad de la información	Número de actividades de sensibilización y/o capacitaciones realizadas en Seguridad y Privacidad de la información en el período/ Número total de actividades de sensibilización y/o capacitaciones programadas para el período x 100

CONTROL	NOMBRE DEL INDICADOR	FORMULA
		Número de campañas de comunicación en temas de seguridad y privacidad de la información realizadas /Número de campañas de comunicación programadas x 100
7.2.2 Toma de conciencia, educación y formación en seguridad de la información	Formación en Seguridad y privacidad de la Información	Número de funcionarios formados en temas de seguridad y privacidad de la información /Total de funcionarios de la entidad x 100
		Número de personas que aprobaron la evaluación de la capacitación/Número de personas que participaron en la capacitación X 100
7.3.1. Terminación o cambio de responsabilidades del empleo	Cierre de cuentas por funcionarios desvinculados de la entidad	Número de cuentas de usuario canceladas/Total de funcionarios desvinculados en el periodo x100
	Difusión no autorizada de información por desvinculación	Incidentes por difusión de información privilegiada/ funcionarios desvinculados de la entidad por un periodo x 100
8.1.1. Inventario de activos	Identificación de activos críticos	Número de activos críticos identificados por proceso/ Total de activos identificados por proceso x 100
	Actualización del Inventario de Activos de Información	Número de procesos con activos de información actualizados/ Número total de procesos de la entidad x 100
8.2.1. Clasificación de la Información	Clasificación de Activos de Información	Número de activos clasificados por proceso/Total activos identificados por proceso x 100
8.2.1. Clasificación de la Información	Infraestructura Critica cibernética-ICC	Número de activos identificados como Infraestructura Critica Cibernética-ICC por proceso/ Total activos identificados por proceso x100
9.1.2. Acceso a redes y a servicios en red	Creación de usuarios	Cantidad de usuarios activos/cantidad de usuarios asignados en el sistema de información o aplicación x100
		Cuentas de usuario inactivas /total de usuarios asignados por aplicación o servicio informático x100
		Cuentas de usuario que no caducan (superusuarios)/ Total de usuarios asignados x 100
9.2.1. Registro y cancelación del registro de usuarios	Frecuencia Actualización de Contraseñas	Número de contraseñas actualizadas en el periodo/Total contraseñas activas del periodo x 100
	Oportunidad en la eliminación de cuentas	Promedio de tiempo transcurrido entre el retiro del trabajador y la eliminación de la cuenta inferior a una hora
9.2.3. Gestión de derechos de acceso privilegiado	Derechos de Acceso privilegiado	Cantidad de usuarios privilegiados asociados por cada servicio informático /Cantidad de usuarios autorizados por servicio informático x 100
		Número de usuarios privilegiados/Numero de funcionarios y/o contratistas del área de Tecnología de información x 100
10.1. Controles Criptográficos	Controles criptográficos	Cantidad de sistemas que contienen datos confidenciales y/o sensibles con controles criptográficos/ Total de sistemas que contienen datos confidenciales y/o sensibles * 100
	Seguridad de información reservada	Archivos con información cifrada/ archivos con información clasificada como reservada x100%
12.4.1. Registro de eventos	Gestión de Eventos de Seguridad y privacidad de la Información	Número de eventos gestionados/Número de eventos reportados x 100

CONTROL	NOMBRE DEL INDICADOR	FORMULA
12.7.1. Controles sobre auditorías de sistemas de información	Auditorías a Sistemas de Información	Número de auditorías de seguridad de la información a sistemas de información realizadas/ total de sistemas de información (TACI: tributario, aduanero, cambiario, internacional)
	Seguimiento a registro de accesos	Acciones de auditoría sobre registro de acceso a sistemas de información /Total Sistemas de información en operación con registro de acceso
13.1.2. Seguridad de los servicios de red (TI)	Seguimiento de los servicios de red	Número de mecanismos de seguridad implementados en la DIAN/Número de mecanismos definidos en la 27001 (firewall, IDS, autenticación, criptografía, conexión segura y procedimientos operativos)
16.1.2. Reporte de eventos de seguridad de la información	Gestión de Eventos de Seguridad de la Información	Número de servidores que reportan eventos de seguridad en el SIEM/ total de servidores de la DIAN
16.1.5 Respuesta a incidentes de seguridad de la información	Gestión de Incidentes de Seguridad de la Información	Número de incidentes gestionados (cerrados)/ Número de incidentes reportados por diferentes fuentes en el trimestre x 100
16.1.5 Respuesta a incidentes de seguridad de la información	Porcentaje de Incidentes de seguridad de la información atendidos oportunamente	Número de incidentes de seguridad atendidos y tratados en un tiempo de atención menor o igual al definido por el modelo de gestión de incidentes/Número de incidentes de seguridad que se presentaron durante el periodo de revisión
	Gestión de Incidentes de Privacidad de la Información	Número de incidentes en el tratamiento de datos personales gestionados / Total incidentes de Datos personales presentados en un periodo.
18.2.2. Cumplimiento con las políticas y normas de seguridad	Porcentaje de implementación de controles	Número de controles Implementados/ Número de controles por implementar de acuerdo con la Declaración de Aplicabilidad x 100

Tabla 5: Indicadores del Sistema de Gestión de Seguridad

De acuerdo con lo definido en el numeral **4. DIAGNÓSTICO** del presente documento, se realizó la medición del 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. Para la medición de cada uno de los frentes se utilizaron criterios establecidos para cada aspecto a evaluar y los valores para la medición se establecen según los siguientes niveles de Madurez

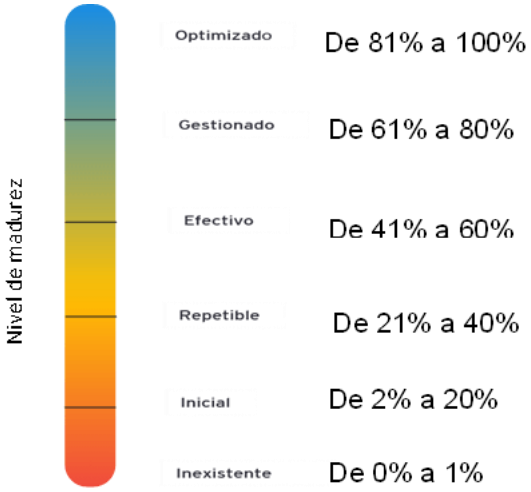


Figura 7: Valores de la escala de medición

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 44% de cumplimiento.

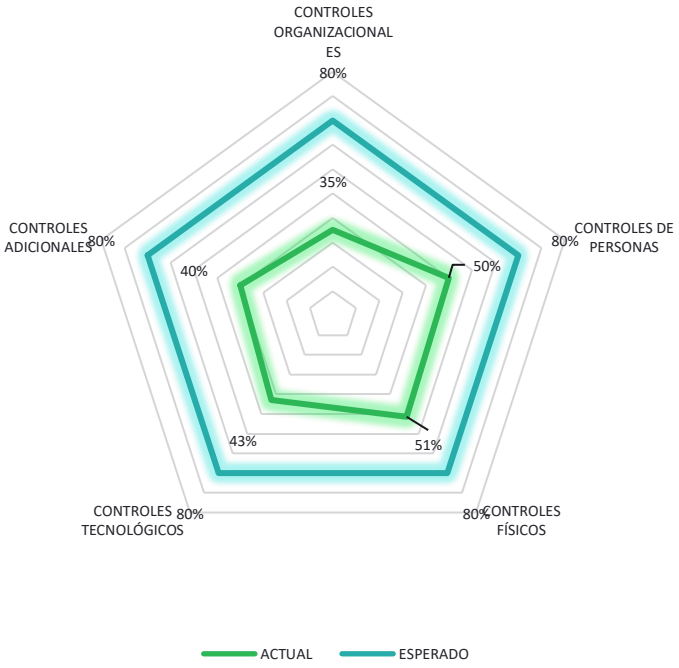


Figura 8: Resultados Evaluación SGSPI, 2023

b. Modelo de Seguridad y Privacidad de la Información - MSPI: La evaluación realizada para el MSPI corresponde a un promedio del 24% de cumplimiento.

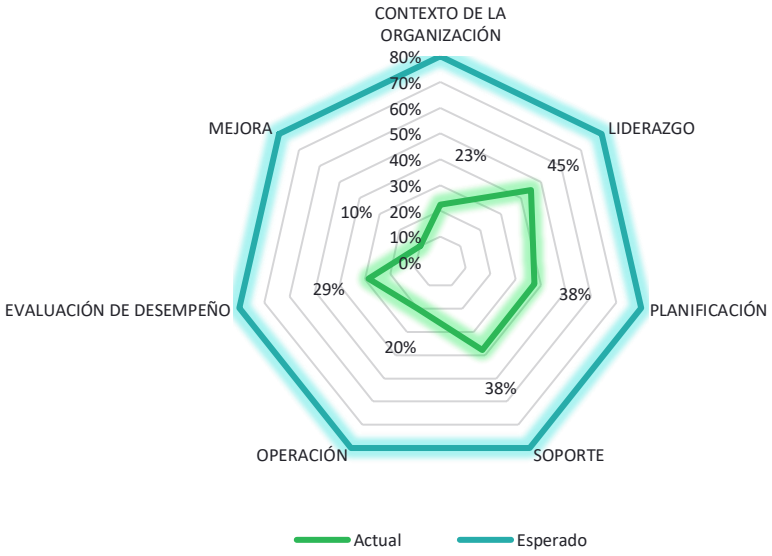


Figura 9: Resultados Evaluación MSPI, 2023

c. Programa Integral de Protección de Datos Personales: La evaluación realizada para el MSPI corresponde a un promedio del 46% de cumplimiento.

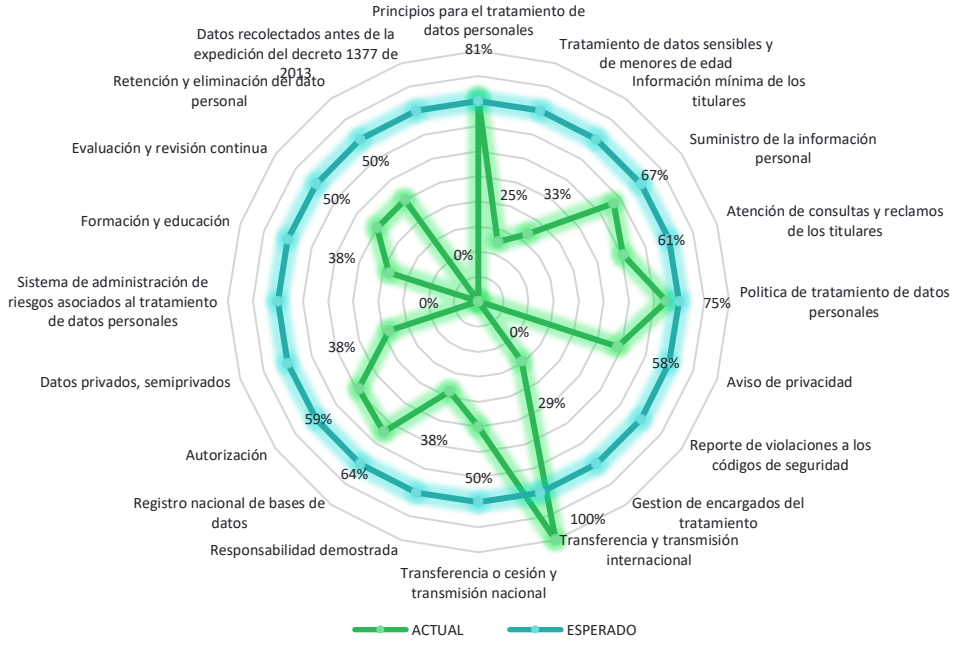


Figura 10: Resultados Evaluación PIGDP, 2023

d. **Gestión de Riesgos de Seguridad de la Información:** La evaluación realizada para GRSI corresponde a un promedio del 15% de cumplimiento.

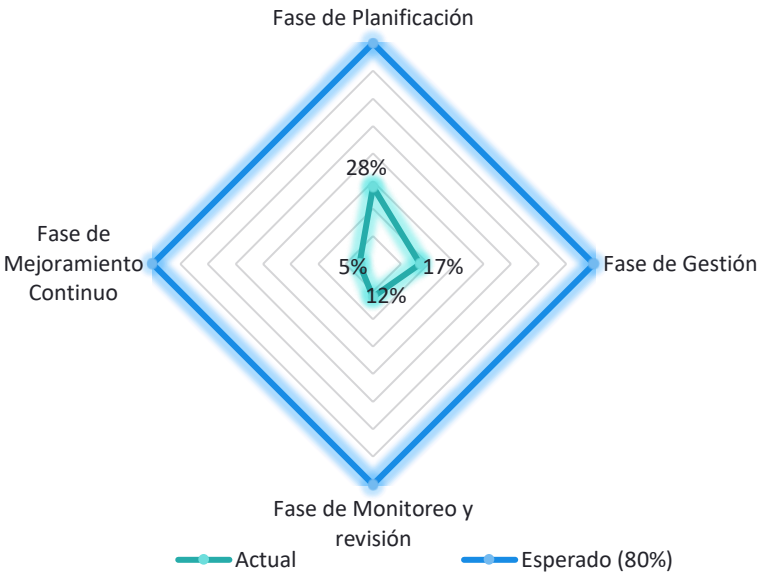


Figura 11: Resultados Evaluación GRSI, 2023

De igual manera se realizarán valoraciones reales (controles actuales y nuevos implementados) y valoraciones proyectadas teniendo en cuenta la implementación de futuros nuevos controles.

La documentación relacionada con la Medición de Indicadores del Sistema de Gestión de Seguridad y Privacidad de la de la DIAN se encuentra en el documento de Indicadores de Seguridad de la Información[30]

7.2 Auditoría Interna

Una vez concluido el contrato No. 92872-055-2022 asignado al APCA Ernst & Young SAS, Mancera S.C. y EY Addvalue Asesores Cia., se proyecta gestionar la ejecución de una Auditoría externa al Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), durante el 2025 una vez el SGSPI lleve aproximadamente un año de mejoramiento en su implementación.

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 de Gestión y Desempeño, en cumplimiento de la resolución 000021 del 28 de enero de 2022, ***artículo 17 "****Funciones del Comité, …"* ***numeral 1.*** "*Aprobar y hacer seguimiento, por lo menos*

[30] Indicadores de Seguridad de la Información

una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión -MIPG". De acuerdo con lo anterior el Jefe de la Oficina de Seguridad de la Información - OSI presenta los temas más relevantes relacionados con la Seguridad y Privacidad de la Información en la entidad, al Comité Institucional Estratégico, según se establezca previamente acerca de los temas a tratar en este y la criticidad que se identifique en cada uno de los aspectos asociados.

8. MEJORAMIENTO CONTINUO

8.1 Mejora

Conforme a los resultados obtenidos en **7.1 Seguimiento, medición, análisis y evaluación**, se debe realizar las acciones correspondientes para satisfacer el objetivo del control y llegar al nivel de cumplimiento gestionado según la escala de valoración de los controles de seguridad definida, se debe realizar seguimiento a las acciones para el cierre de brechas propuestas.

Para continuar con la implementación del SGSPI se contrató la Consultoría contratada para "Realizar actividades de implementación, mantenimiento, administración, fortalecimiento y seguimiento al Sistema de Gestión de Seguridad y Privacidad de la información (SGSPI) de la DIAN"."

9. GLOSARIO:

El glosario correspondiente al presente documento puede ser consultado en el **Anexo** Definiciones y Siglas de Seguridad de la Información[31]

[31] 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.	No Aplica
2	30/09/2021	14/9/2023	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.	No Aplica
3	15/9/2023		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 Se eliminan los siguientes anexos de la versión 2: No.1, No.2, No.3, No.4, No.5 y No.6.	Esta versión corresponde a Información Pública

Elaboró:	Fanny Constanza Hernández Arias **Elaboración técnica**	Gestor IV	Oficina de Seguridad de la Información
	Tito Alejandro Menjura Murcia **Elaboración metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales

Revisó:	Hugo Alcides Pérez Pinilla	Jefe (E)	Oficina de Seguridad de la Información
Aprobó:	Hugo Alcides Pérez Pinilla	Jefe (E)	Oficina de Seguridad de la Información

ANEXO No.1 Definiciones y siglas

ANEXO No.7 Protocolo para el manejo de correos falsos