PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2026

ENFOQUES:

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
SEGURIDAD DIGITAL
GESTIÓN DE RIESGOS E INCIDENTES

DEPARTAMENTO ADMINISTRATIVO
DIRECCIÓN NACIONAL DE INTELIGENCIA

"INTELIGENCIA PARA LA PAZ"

DICIEMBRE 2023

1. INTRODUCCIÓN

La Dirección Nacional de Inteligencia - DNI, es una Entidad pública de carácter técnico, pensada y creada a partir de las mejores prácticas de buen gobierno, que tiene por misión producir inteligencia estratégica y contrainteligencia de Estado, desde una perspectiva civil, con el objetivo de identificar oportunidades, riesgos y amenazas que afecten la seguridad nacional.

La DNI desarrolla un proceso especializado de planeamiento; búsqueda y recolección; procesamiento y análisis; y, difusión de información, denominado ciclo de inteligencia, cuyos resultados generan conocimiento, contexto y entendimiento de riesgos y amenazas, para la toma de decisiones del Alto Gobierno.

El Modelo de Seguridad y Privacidad de la Información - MSPI, es reconocido por la institución como un componente esencial para garantizar el principio de reserva legal que regula las actividades de inteligencia y contrainteligencia, y la información que se genera en cada una ellas. Contar con el MSPI, le permite a la institución, a través de la implementación de diversos controles, asegurar eficientemente la información, los procesos, los sistemas, los servicios, la infraestructura tecnológica, y la infraestructura critica, evitando la interrupción de las actividades institucionales.

Por lo anterior, la DNI formula el Plan de Seguridad y Privacidad de la Información (PSPI) 2023 - 2026, el cual incluye y articula los lineamientos del Modelo de Seguridad y Privacidad de la Información; la estrategia de seguridad digital; los lineamientos para el tratamiento de riesgos de seguridad y privacidad de la información; así como, los lineamientos para la gestión de incidentes de seguridad digital.

El plan se implementará acorde con las normas legales, reglamentarias y metodológicas expedidas por el Gobierno Nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones; las normas legales que rigen el desarrollo de actividades de inteligencia y contrainteligencia; los estándares internacionales implementados como buenas prácticas dentro del Sistema Integrado de Gestión Institucional, como lo es la NTC-ISO 27001; y, las necesidades de fortalecimiento y crecimiento institucional, sobre la materia.

Con la implementación del PSPI, se busca fortalecer las medidas técnicas, metodológicas, administrativas y de talento humano, para gestionar de manera eficaz, eficiente y efectiva los activos de información, la infraestructura crítica y los riesgos e incidentes de seguridad y privacidad de la información, garantizando la continuidad de las actividades institucionales, enmarcadas en una gestión por procesos.

Contenido

2. MARCO DE REFERENCIA

2.1. Marco Institucional

La DNI fue creada mediante Decreto Ley 4179 de 2011, como un organismo civil de seguridad que desarrolla actividades de inteligencia estratégica y contrainteligencia.

Tiene como objeto, desarrollar actividades de inteligencia estratégica y contrainteligencia para proteger los derechos y libertades de los ciudadanos y de las personas residentes en Colombia, prevenir y contrarrestar amenazas internas o externas contra la vigencia del régimen democrático, el orden constitucional y legal, la seguridad y defensa nacional, así como cumplir con los requerimientos que en materia de inteligencia le hagan el Presidente de la República y el Alto Gobierno para el logro de los fines esenciales del estado, de conformidad con la ley.
En la Tabla 1, se señalan las normas legales vigentes que regulan las funciones desarrolladas por la Entidad:

Norma	Objeto
Decreto 4179 de 2011	Por el cual se crea un Departamento Administrativo y se establece su objetivo, funciones y estructura.
Ley Estatutaria 1621 de 2013	Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones.
Decreto 1070 de 2015	Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa, y se compila, entre otros, el Decreto Reglamentario 857 de 2014, por medio del cual se expiden normas para fortalecer el marco legal que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".
Decreto 1377 de 2017	Por el cual se adiciona un artículo al Capítulo 5 del Título 5 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, en lo relacionado con las comisiones al exterior.
Decreto 338 de 2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital, y se dictan otras disposiciones.

Tabla 1 – Normatividad que regula las actividades de la DNI

2.2. Seguridad y Privacidad de la Información

El Gobierno Nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones, ha dispuesto para las entidades de la administración pública, diferentes normas legales, manuales y guías, que orientan y facilitan la implementación de la política de Gobierno Digital y específicamente el Modelo de Seguridad y Privacidad de la Información.

En la Tabla 2, se señalan las normas legales vigentes emitidas por el Gobierno Nacional en materia de seguridad y privacidad de la información:

Norma	Objeto
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho al Acceso a la Información Pública Nacional, y se dictan otras disposiciones.
Decreto 1078 de 2015	Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, y se compila, entre otros, los Decretos: i) 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital; y, ii) lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1083 de 2015	Por el cual se expide el Decreto Único Reglamentario del Sector Función Pública, y se compila, entre otros, los Decretos: 1499 de 2017: Sistema de Gestión establecido en el Artículo 133 de la Ley 1753 de 2015; 612 de 2018: Integración de los planes institucionales y estratégicos al plan de acción.
Decreto 1080 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Cultura, y se dictan disposiciones en materia de gestión documental para todas las Entidades del Estado.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital, y se adopta el modelo de seguridad y privacidad, como habilitador de la política de Gobierno Digital.
CONPES 3995 de 2020	Política nacional de confianza y seguridad digital.

Tabla 2 – Normatividad en materia del MSPI

En la Tabla 3, se señalan las guías generales expedidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, en materia de seguridad y privacidad de la información:

Documento	Objeto
Manual de Gobierno Digital	Define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados, en relación con la Política de Gobierno Digital.
Modelo de Seguridad y Privacidad de la Información	Define los lineamientos para la implementación de un sistema de gestión de seguridad y privacidad de la información y seguridad digital, basado en el ciclo PHVA, así como los requerimientos legales, técnicos, normativos reglamentarios y de funcionamiento.
Autodiagnóstico Modelo de Seguridad y Privacidad de la Información	Instrumento de valoración que permite a las entidades públicas identificar el nivel de implementación del modelo de seguridad y privacidad de la información, y establecer la línea base para mejorar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información.
Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.	Establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la Entidad, en el marco de riesgos de gestión, corrupción y seguridad digital.

Tabla 3 – Guías generales en materia del MSPI

En la Tabla 4, se señalan los estándares internacionales adoptados y en proceso de implementación por parte de la Entidad sobre la materia, como parte de la mejora continua y buenas prácticas dentro del Sistema Integrado de Gestión Institucional:

Documento	Objeto
ISO 27001 – Sistema de Gestión de Seguridad de la Información.	Estándar internacional que contiene los requisitos para la implementación de un sistema de gestión de seguridad de la información.
ISO 27001 - Anexo A	Documento normativo que sirve como guía para implementar los controles de seguridad de la información específicos de la ISO 27001.
ISO 22301 - Continuidad y disponibilidad de los servicios.	Estándar internacional que contiene los requisitos para la implementación de una gestión de continuidad del negocio, como proceso holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades.

Tabla 4 – Buenas prácticas en materia de seguridad de la información

2.3. Lineamientos Plan Estratégico Sectorial / Institucional

Partiendo de las funciones dadas a la Dirección Nacional de Inteligencia a través del Decreto 4179 de 2011; la legislación aplicable para el desarrollo de actividades de inteligencia y contrainteligencia, los compromisos como Estado frente a los Objetivos de Desarrollo Sostenible, y los propósitos del Plan Nacional de Desarrollo 2022-2026, "Colombia potencia mundial de la vida", en este documento se define el direccionamiento estratégico que regirá la gestión durante el periodo 2023-2026, como una guía orientadora en el accionar institucional.

En la imagen 1, se presentan los objetivos y estrategias definidas.

Imagen 1. Objetivos y estrategias - Plan Estratégico Sectorial / Institucional 2023 - 2026

Para el desarrollo de los propósitos institucionales, se han definido como principales activos las personas, la información, las instalaciones, los sistemas de información y las comunicaciones.

Con los avances tecnológicos y el uso masivo de las tecnologías de la información y las comunicaciones (TIC), se creará y desarrollará un modelo de seguridad digital integral, con el propósito de asegurar la información de inteligencia estratégica y contrainteligencia, enmarcado en la Ley de Inteligencia 1621 de 2013.

Se fortalecerán los sistemas de información y se mantendrán canales efectivos de comunicación y difusión, por medio de los cuales, la información que se genere, desde cualquier área, llegue a sus destinatarios de forma asertiva, sin distorsiones y que así mismo, sea gestionada desde sus orígenes.

Con el fin de mitigar el riesgo en las posibles pérdidas, fugas o alteraciones de información reservada, se fortalecerá y mantendrá el sistema de gestión de seguridad de la información, implementando buenas prácticas y estándares reconocidos a nivel nacional e internacional, así como controles efectivos y el fortalecimiento de la cultura de seguridad de la información.

Además de esto, se garantizarán las herramientas tecnológicas necesarias que permitirán realizar una trazabilidad del estado de la información, desde el momento de su creación, su procesamiento, y su difusión, hasta el momento mismo de su almacenamiento y custodia, garantizando en todo momento su integridad, confiabilidad y disponibilidad.

Se desarrollarán procesos de innovación en la gestión de la información, así como contenidos multimedia para comunicación y difusión de la información, que permitan llegar de forma asertiva a los receptores, innovando de igual manera en el aseguramiento de los mismos productos.

Se adelantarán actividades de depuración de la información almacenada en repositorios diferentes al Sistema de Información de Inteligencia y Contrainteligencia, el cual tiene un tratamiento especial ordenado por la Ley 1621 de 2013.

La DNI, consciente de la importancia del patrimonio documental, como garante del cumplimiento de la función misional de la Entidad, revisará y fortalecerá la gestión documental."[1]

2.4. Roles y Responsabilidades

Las orientaciones e implementación de los lineamientos del Modelo de Seguridad y Privacidad de la Información, en el marco de las Políticas de Gobierno Digital y Seguridad Digital, se realizan bajo un esquema de coordinación y colaboración armónica, a través de los roles y responsabilidades, los cuales vinculan desde la alta dirección, hasta las dependencias específicas de la Entidad e instancias técnicas que lo gestionan, tal como se presenta en la Tabla 5.

Rol	Responsable	Responsabilidad
Líder de las Políticas de Gobierno Digital y Seguridad digital	Ministerio de Tecnologías de la Información y las Comunicaciones	Emitir las normas, manuales, guías y metodologías de seguimiento y evaluación de las Políticas de Gobierno Digital y Seguridad Digital.

[1] Estrategias institucional 2019-2022, versión 2:2019. Disponible en intranet y en la herramienta de apoyo al SIGI

Rol	Responsable	Responsabilidad
Responsable Institucional de las Políticas de Gobierno Digital y Seguridad digital	Director General	Coordinar, hacer seguimiento y verificar la implementación de las Políticas de Gobierno Digital y Seguridad Digital.
Responsable de orientar la implementación de las Políticas de Gobierno Digital y Seguridad Digital	Comité de Gestión y Desempeño. Conformado mediante Resolución 920 de 2017.	Orientar la implementación de las Políticas de Gobierno Digital y Seguridad Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.
Responsable de liderar la implementación de las Políticas de Gobierno Digital y Seguridad Digital	Director de Gestión Institucional a través del Coordinador de Tecnologías de la Información y las Comunicaciones (Arquitectura de TI y servicios ciudadanos digitales) Centro de Protección de Datos (Seguridad y Privacidad de la Información)	Liderar la implementación de las Políticas de Gobierno Digital y Seguridad Digital, con sus respectivos habilitadores: 1. Arquitectura 2. Seguridad y privacidad de la información 3. Servicios ciudadanos digitales.
Responsable del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital.	Jefe del Centro de Protección de Datos	Asegurar la implementación de las políticas del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión y respuesta de los incidentes de seguridad digital

Tabla 5 – Roles y Responsabilidades MSPI

3. DIAGNÓSTICO INSTITUCIONAL

3.1. Antecedentes Institucionales

Desde la vigencia 2014, la institución inició el proceso de implementación de la Norma Técnica ISO 27001, con la finalidad de implementar buenas prácticas que le permitieran tener un sistema de gestión de seguridad de la información robusto y ajustado a las necesidades institucionales. La DNI obtuvo la primera certificación del sistema de gestión de seguridad de la información bajo los requisitos de la Norma ISO 27001: 2013, por parte del Ente certificador Bureau Veritas, en la vigencia 2016; en adelante, anualmente se han recibido las visitas de seguimiento y recertificación, manteniendo vigente el reconocimiento y sirviendo de referencia para otras instituciones del Estado.

Contar con la implementación de la norma técnica citada le ha permitido a la DNI tener grandes avances y resultados frente a los requisitos del Modelo de Seguridad y Privacidad de la Información, actualizado por el Gobierno Nacional en la actual vigencia. La Institución cuenta con diversas políticas, manuales, procedimientos, instructivos, formatos y documentos técnicos de la gestión de activos, riesgos e incidentes, que evidencian la gestión desarrollada en materia de seguridad de la información y seguridad digital.

Así mismo, desde la vigencia 2016, la Entidad viene participando en la implementación de políticas de Estado en materia de seguridad digital. En relación con el CONPES 3854 de 2016 "Seguridad Digital", se desarrollaron acciones que permitieron fortalecer las capacidades institucionales, operativas, administrativas, humanas, de infraestructura física y tecnológica de la DNI, bajo el marco de los principios fundamentales de la política nacional de seguridad digital, finalizando la actividad en la vigencia 2020.

Actualmente, la institución participa en el CONPES 3995 de 2020 "Confianza y Seguridad Digital", en el cual se plantea como meta: el diseño, estructuración e implementación del proyecto de implementación del Equipo de Respuesta a Incidentes de Seguridad de Tecnología de la Información CSIRT (Computer Security Incident Response Team) del Sector Inteligencia, con el fin de que contribuya en la protección de la seguridad digital nacional, aportando con informes sobre las ciber amenazas que pueden afectar el correcto funcionamiento de la infraestructura crítica digital del país.

De otra parte, la Entidad ha definido directrices, políticas y controles para implementar los diferentes lineamientos establecidos en la Ley 1621 de 2013, específicamente en lo relacionado con la reserva de la información y la protección de datos y archivos de inteligencia y contrainteligencia. Para ello, anualmente se desarrolla un plan de trabajo con acciones que permiten garantizar la privacidad

de la información y la garantía de los derechos humanos, en desarrollo de las actividades de inteligencia y contrainteligencia, a través de los procesos de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia.

3.2. Políticas Institucionales

La institución ha definido políticas y lineamientos mediante los cuales ha avanzado en la implementación del MSPI, la seguridad digital, la gestión de riesgos de seguridad de la información y la gestión de incidentes de seguridad digital, así:

Seguridad y privacidad de la información y seguridad digital

A través del Manual [redacted] – [1] Seguridad de la Información, la institución ha establecido las políticas del Sistema de Gestión de Seguridad de la Información, tanto física como digital, con un alcance a todos los procesos, servidores públicos, contratistas y terceras partes, que deban tener acceso a la información de la Entidad.

La política principal busca consolidar una cultura de seguridad de la información, bajo los principios de confidencialidad, integridad y disponibilidad, y de esa forma disminuir los niveles de riesgo de la información y de los sistemas y redes que la soportan, a través de la gestión integral del riesgo, el cumplimiento del marco legal, las mejores prácticas y la mejora continua.

A partir de estas directrices, se especifican políticas de: teletrabajo, seguridad del recurso humano; gestión de activos; control de acceso; criptografía; seguridad física y del entorno; seguridad en las operaciones; seguridad en las comunicaciones; adquisición, desarrollo y mantenimiento de sistemas; relación con los proveedores; gestión de incidentes de seguridad de la información; aspectos de seguridad de la información de la gestión para la continuidad del negocio; y, política de cumplimiento, las cuales en detalle se encuentran definidas en el manual citado.

Gestión de riesgos de seguridad de la información

A través del Manual [redacted] -[2] Sistema Integrado de Gestión Institucional, y el procedimiento [redacted] -[3] Gestión Integral del Riesgo, la Entidad ha establecido la política integral para la gestión de riesgos, comprometiéndose a valorar, tratar, monitorear y comunicar los riesgos asociados con los procesos, y a emprender acciones de control sobre los eventos que puedan afectar la gestión, el logro de los objetivos institucionales, y los posibles hechos generadores de corrupción.

La gestión de riesgos surte las etapas de establecimiento del contexto, identificación, análisis, evaluación y tratamiento del riesgo, en un ambiente de comunicación, monitoreo, revisión y seguimiento constante.

La identificación de los riesgos de seguridad de la información se realiza a partir de los activos institucionales, los cuales son identificados y clasificados, para posteriormente proceder con la identificación de los riesgos de perdida de la confidencialidad, integridad y disponibilidad. Para cada riesgo se asocia el grupo de activos del proceso, y conjuntamente, se analizan las posibles amenazas y vulnerabilidades que podrían causar su materialización. La metodología específica para la identificación, análisis, evaluación y tratamiento, se encuentra descrita en el instructivo [redacted] -4 Metodología para la administración del riesgo, la cual se encuentra armonizada con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, y el Departamento Administrativo de la Función Pública.

Gestión de incidentes de seguridad digital

A través del procedimiento [redacted] – 5 Gestión de eventos e incidentes de seguridad de la información e informática, se adoptaron las políticas para identificar aquellas situaciones catalogadas como eventos e incidentes, y para tomar las acciones necesarias oportunamente, minimizando la posibilidad de materialización de riesgos de seguridad de la información o interrupción de los servicios.

Todos los servidores públicos, contratistas y terceras partes que tienen acceso a la información institucional, son responsables de aplicar las diferentes políticas del sistema de gestión de seguridad de la información, para mitigar la generación de eventos e incidentes.

En caso de presentarse una novedad, evento o incidente, dentro del citado procedimiento se describen los pasos que se deben seguir, iniciando con la identificación y comunicación; clasificación de acuerdo con el nivel de criticidad; recolección de la información asociada al evento o incidente; estimación de tiempo de atención y solución del caso; retroalimentación, aprendizaje y mejora sobre lo ocurrido.

Gráfico 1. Modelo de operación por gestiones de seguridad y privacidad de la información, seguridad digital y continuidad de la operación

3.3. Resultados Diagnóstico MSPI

Con el fin de conocer el estado actual en el que se encuentra la implementación de la seguridad y privacidad de la información en la Entidad, durante el segundo trimestre de la vigencia 2021 se aplicó el "Instrumento de evaluación del MSPI", mediante el cual se pudieron identificar los controles implementados, y aquellos que requieren ser fortalecidos, siendo un insumo para la elaboración del plan de seguridad y privacidad de la información, con enfoque de seguridad y privacidad, seguridad digital y gestión de riesgos e incidentes.

El ejercicio inició con la creación de la mesa técnica de MSPI, conformada por seis (6) servidores públicos, que representan las diferentes dependencias de la Entidad, la cual tiene como propósito apoyar la adopción de los lineamientos del MSPI, la guía de riesgos, el procedimiento de gestión de incidentes, la estrategia de seguridad digital, y, concluir con la propuesta del Plan de Seguridad y Privacidad de la Información.

Este ejercicio interdisciplinario, permitió realizar un análisis integral sobre el estado actual de la implementación del MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad

digital, definiendo el nivel de madurez, y aportando al diseño de estrategias para el fortalecimiento institucional sobre la materia.

Resultados Instrumento de evaluación del MSPI

El diligenciamiento de la herramienta permitió obtener una calificación para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control establecidos en las hojas nombradas como "ADMINISTRATIVAS y TÉCNICAS" dentro de la Herramienta Instrumento MSPI.

El resultado obtenido para la evaluación del estado actual nos refleja los controles según el Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital que ha establecido MinTIC para las entidades públicas del orden nacional, así como el avance del ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Con el diligenciamiento de la herramienta MSPI, se obtuvieron los siguientes resultados:

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	93	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	94	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	92	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	100	100	**OPTIMIZADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	100	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	100	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	99	100	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**

A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	94	100	**OPTIMIZADO**
A.18	CUMPLIMIENTO	94	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**97**	**100**	**OPTIMIZADO**

Tabla 6. Calificación de dominios de acuerdo con los controles asociados

Se ve la necesidad de fortalecer los dominios donde la calificación fue inferior a 100 con el fin de hacer más efectivo el Modelo de Seguridad y Privacidad de la Información - MSPI, la gestión de riesgos de seguridad de la Información y la gestión de incidentes de seguridad digital, lo cual se tiene en cuenta en el desarrollo de las estrategias.

En el Gráfico 2, se muestra el resultado del análisis de brecha y el avance del PHVA frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #ñ8) del Modelo de Seguridad de Privacidad de la Información, los cuales se construyen automáticamente al diligenciar el Instrumento de Evaluación del MSPI, así:

Gráfico 2. Brecha anexo a ISO27001:2013

De otra parte, en el Gráfico 3, se presenta el avance del MSPI desde el punto de vista del ciclo PHVA y el comparativo con los plazos establecidos en la política de Gobierno Digital, para la vigencia 2023:

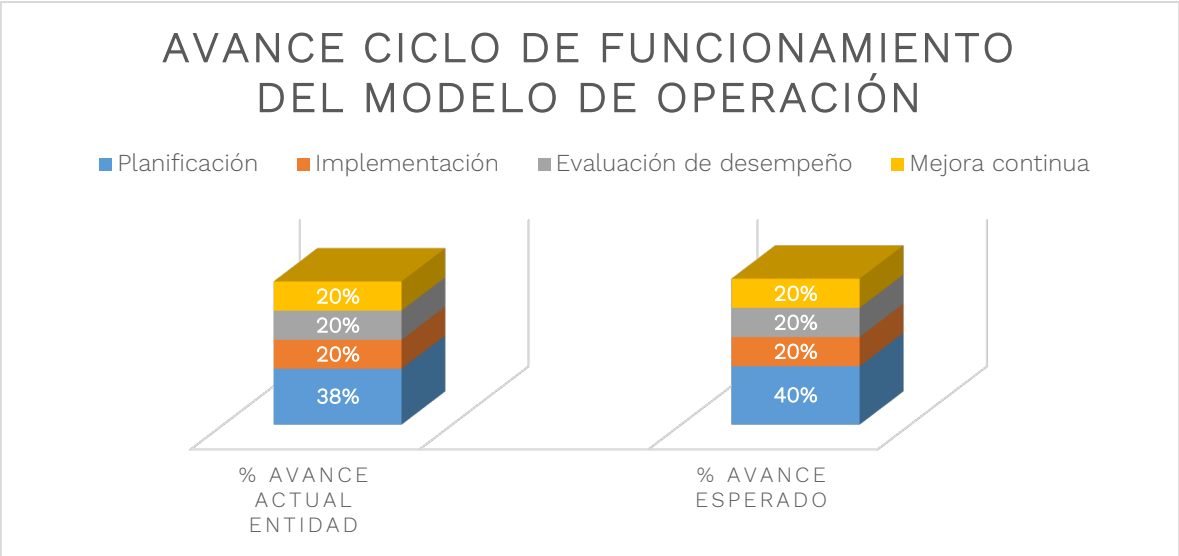
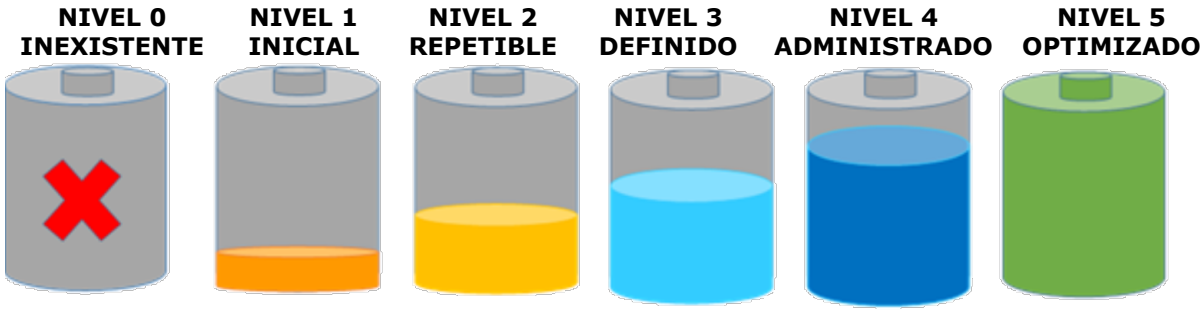


Gráfico 3. Avance MSPI acorde con ciclo PHVA

De acuerdo con la medición del nivel de madurez del Sistema de Gestión de Seguridad de la Información - SGSI, realizada con base en los requisitos de la Norma ISO 27001: 2013 y los lineamientos dados por el Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la información, y el procedimiento para la gestión de los incidentes de seguridad digital, con corte a diciembre de 2023, el sistema se encuentra en un Nivel 5 “Optimizado”, lo cual indica que se reconocen las necesidades en materia de seguridad de la información, se tienen documentados los manuales, procedimientos e instructivos del proceso de seguridad de la información, se realizan ejercicios de diagnóstico, planificación, implementación y evaluación del desempeño, y se implementan acciones de mejora continua.



Inexistente	Inicial	Repetible	Definido	Administrado	Optimizado
Desconoce o no tiene en cuenta el tema de seguridad de la información.	Reconoce que tiene problemas de seguridad y que estos necesitan ser resueltos.	Tiene procedimientos no formales de Seguridad.	En este nivel se realizan las fases de diagnóstico planificación e implementación.	Ha realizado las fases de evaluación de desempeño y mejora continua.	Encuentra en la seguridad de la información un valor agregado para la Entidad.

Optimizado

En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.

Se utilizan indicadores de efectividad para establecer si la Entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

La Entidad genera tráfico en IPv6.

Gráfico 4. Nivel de madurez MSPI

De otra parte, acorde con el análisis de los resultados de la medición de gestión y desempeño institucional de la vigencia 2022, adelantada por el Departamento Administrativo de la Función Púbica, a través del Formulario Único de Reporte y Avance de Gestión – FURAG, instrumento de medición del Modelo Integrado de Planeación y Gestión - MIPG, la política de seguridad digital se encuentra en un nivel de implementación del 98,1; y la política de gobierno digital en 79. [2]

El "Instrumento de evaluación del MSPI" también permitió determinar cómo se encuentra la Entidad frente a las mejores prácticas en ciberseguridad definidas por

[2] Informe análisis resultados FURAG 2022

el NIST, determinando un diagnóstico frente a los lineamientos de la política de Ciberseguridad y Ciberdefensa, definidos en el documento CONPES 3701 de 2011, el CONPES 3854 de 2016 y el CONPES 3595 de 2020, como se muestra en el Gráfico 5:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
ETIQUETAS FILA	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	94	100
DETECTAR	96	100
RESPONDER	98	100
RECUPERAR	80	100
PROTEGER	97	100

Tabla 7. Modelo Ciberseguridad NIST

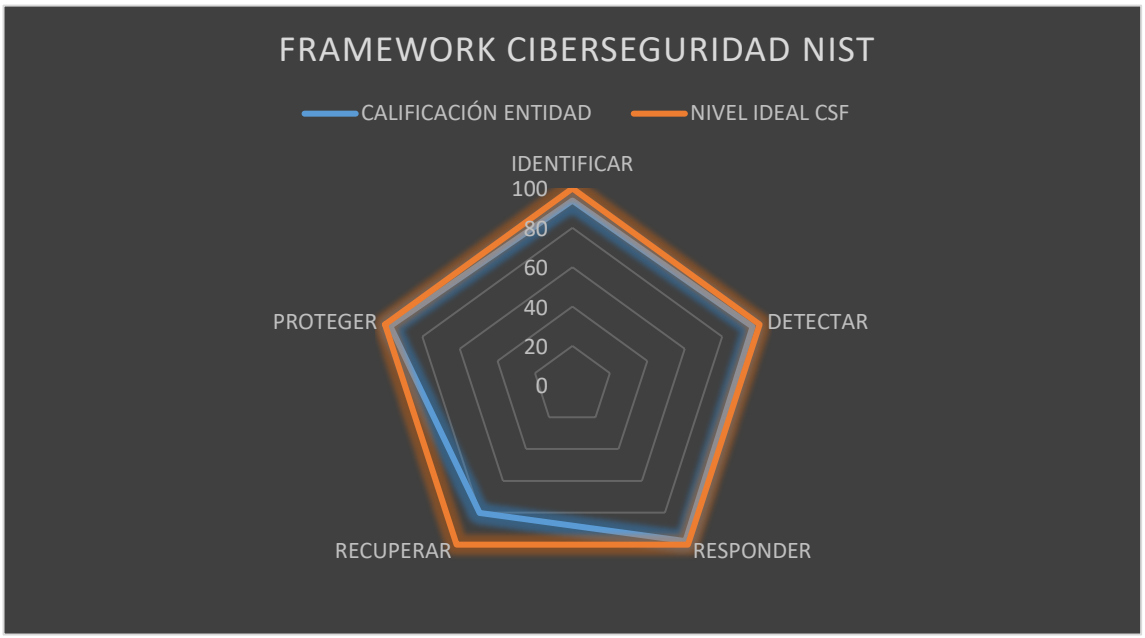


Gráfico 5. Diagnóstico en Ciberseguridad

Del resultado obtenido se definen dos aspectos a fortalecer, así:

[redacted]

[redacted]

- [redacted]

[redacted]. -6

En el Anexo 1, se presentan los resultados específicos relacionados con el diagnóstico realizado a los lineamientos en materia de privacidad de la información.

4. ORIENTACIONES ESTRATÉGICAS EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y GESTIÓN DE RIESGOS E INCIDENTES

Teniendo en cuenta que la DNI ha priorizado el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para el desarrollo de las actividades institucionales, como se evidencia en la arquitectura empresarial de TI, y que esto conlleva a estar expuestos a sufrir incidentes de seguridad digital, pudiéndose afectar el ejercicio de las funciones, la Entidad establece el Plan de Seguridad y Privacidad de la Información 2023-2026, el cual contempla las estrategias para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la gestión de la seguridad digital, la gestión de riesgos de seguridad y privacidad de la Información, y el procedimiento para la gestión de los incidentes de seguridad digital, como herramientas que impulsan el fortalecimiento de las capacidades para evitar la interrupción de las actividades institucionales, y garantizar la continuidad de las mismas.

Las orientaciones estratégicas se basan en el desarrollo de una cultura de carácter preventivo, de manera que, con estudios y análisis de contexto, se planeen, implementen, evalúen y mejoren las acciones necesarias para entregar productos de inteligencia y contrainteligencia de confianza, protegiendo la información, los procesos, los sistemas, los servicios, la infraestructura tecnológica y la infraestructura critica, a través de la gestión oportuna y efectiva de los riesgos e incidentes.

4.1. Objetivos

Objetivo General

Preservar y proteger la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudió de la información que se genera en los diferentes procesos de la Entidad, independientemente del medio en el que se encuentren (físicos y digitales), propendiendo por la continuidad de las operaciones, dando cumplimiento a los requisitos legales y reglamentarios, promoviendo el alto

desempeño y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información.

Objetivos específicos

i. Fortalecer y sostener el Modelo de Seguridad y Privacidad de la Información – MSPI, y la seguridad digital, con base en las normas legales y buenas prácticas internacionales, como elemento esencial para el desarrollo de las actividades de inteligencia estratégica y contrainteligencia.

ii. Gestionar los riesgos de seguridad y privacidad de la información, de acuerdo con el contexto y necesidades institucionales, para prevenir afectaciones en el desarrollo de las actividades propias.

iii. Gestionar los incidentes de seguridad digital que se presenten sobre los activos de información.

4.2. Estrategias

A partir de los objetivos establecidos, los cuales se alinean con el Plan Estratégico Institucional 2023-2026, a continuación, se relacionan las estrategias mediante las cuales se materializarán los objetivos específicos, que a su vez contribuyen al cumplimiento del objetivo general.

Teniendo en cuenta que la seguridad digital es un elemento transversal a toda la gestión del sistema de seguridad y privacidad de la información, la cual busca preservar la confidencialidad, integridad y disponibilidad de la información que se encuentra en medios digitales, en el desarrollo de las diferentes estrategias estarán implícitas las acciones que permiten fortalecer la seguridad digital.

Lo anterior, acorde con la Resolución 500 de 2021, la cual señala que la estrategia de seguridad digital debe incorporarse en la implementación del MSPI, la gestión de riesgos de seguridad y privacidad de la información, y la gestión de incidentes de seguridad digital.

Objetivo	Estrategia
Fortalecer y sostener el Modelo de Seguridad y Privacidad de la Información – MSPI, y la seguridad digital, con base en las normas legales y	Integrar en las políticas, manuales, procedimientos, instructivos, formatos, roles y responsabilidades, los lineamientos en materia de privacidad de la información y seguridad digital, que sean necesarios para la implementación del MSPI.

Objetivo	Estrategia
buenas prácticas internacionales, como elemento esencial para el desarrollo de las actividades de inteligencia estratégica y contrainteligencia.	Establecer e implementar estrategias que permitan promover una cultura en materia de seguridad y privacidad de la información y seguridad digital, concientizando tanto al interior como a las partes interesadas relevantes.
	Gestionar y mantener el sistema de gestión de seguridad y privacidad de la información, y la seguridad digital, a través de la aplicación de herramientas de evaluación que permitan evidenciar el nivel de madurez, así como el cumplimiento de requisitos de buenas prácticas implementadas.
	Diagnosticar las capacidades institucionales en materia de seguridad y privacidad de la información, así como de seguridad digital, para identificar oportunidades de fortalecimiento.
Gestionar los riesgos de seguridad y privacidad de la información, de acuerdo con el contexto y necesidades Institucionales, para prevenir afectaciones en el desarrollo de las actividades institucionales.	Identificar los activos de información e infraestructura critica, con base en los lineamientos dados por el Gobierno Nacional en materia de privacidad de la información y seguridad digital.
	Realizar la gestión integral de riesgos de seguridad y privacidad de la información, y seguridad digital (plan de tratamiento) acorde con el procedimiento institucional establecido.
	Monitorear de manera permanente la efectividad de los controles establecidos para los riesgos de seguridad y privacidad de la información, y seguridad digital.
Gestionar la prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje de los incidentes de seguridad digital que se presenten sobre los activos de información.	Desarrollar acciones para prevenir, proteger y detectar eventos e incidentes de seguridad y privacidad de la información y seguridad digital.
	Desarrollar acciones para la respuesta, comunicación, recuperación y aprendizaje de los incidentes de seguridad y privacidad de la información y seguridad digital.

Tabla 8 – Objetivos y estrategias PSPI

5. PROGRAMACIÓN, SEGUIMIENTO Y EVALUACIÓN

5.1. Programación de gestión

De acuerdo con el Decreto 612 de 2018, incorporado en el Decreto 1083 de 2015, el Plan de Seguridad y Privacidad de la Información 2023-2026, establecido por la Entidad, y que orienta la gestión en materia de seguridad y privacidad, seguridad digital, y gestión de riesgos e incidentes, será incorporado al Plan Integrado Anual, y publicado acorde con los lineamientos de los mencionados Decretos.

La incorporación se realiza a través de cronogramas de trabajo que detallan las actividades, tareas, responsables y fechas de ejecución, y desarrollan los objetivos, estrategias y acciones del modelo de seguridad y privacidad de la información y a su vez aportan al cumplimiento de las normas legales en la materia, las políticas de Gobierno Digital y Seguridad Digital, la misión, visión y objetivos estratégicos institucionales.

El Centro de Protección de Datos, con el acompañamiento de la mesa técnica de seguridad y privacidad de la información, realizará la revisión y actualización del Plan de Seguridad y Privacidad de la Información de manera anual, a razón de los cambios que puedan surgir en las estrategias de la Institución, la normatividad, las tendencias, las necesidades y las prioridades institucionales.

5.2. Presupuesto

La Entidad dispondrá los recursos requeridos para fortalecer y mantener el Modelo de Seguridad y Privacidad de la Información, y la seguridad digital, acorde con las disponibilidades presupuestales y las necesidades y prioridades identificadas.

5.3. Seguimiento y evaluación

El Plan de Seguridad y Privacidad de la Información 2023-2026 será objeto de seguimiento y control mensual, a través del monitoreo realizado al Plan Integrado Anual, y se realizará una evaluación finalizada cada vigencia, con el fin de identificar mejoras para incluir en el detalle de actividades y tareas propuestas, en cumplimiento de los objetivos, estrategias y acciones definidas.

Las auditorías de gestión realizadas por la Oficina de Control Interno, serán un insumo para continuar fortaleciendo la gestión estratégica del Modelo de Seguridad y Privacidad de la Información y la Seguridad Digital, cuyos resultados serán tenidos en cuenta en la programación detallada de cada vigencia.

La Entidad continuará gestionando las auditorías externas requeridas para mantener el cumplimiento de requisitos de las buenas prácticas implementadas, con base en el estándar internacional ISO 27001.

Periódicamente se realizará seguimiento a través de los indicadores de desempeño del Modelo de Seguridad y Privacidad de la Información, con el fin de evidenciar los avances o retrocesos y tomar las medidas necesarias para garantizar su correcta implementación y mantenimiento.

5.4. Mejora continua

La gestión del sistema de seguridad y privacidad de la información mantendrá la mejora continua como parte del día a día, y tomará como insumo las diferentes herramientas de seguimiento y evaluación para diseñar los planes de mejoramiento continuo, acorde con los lineamientos establecidos en el Procedimiento [redacted] - [7] Acciones de mejoramiento.

5.5. Anexos

[redacted]

[redacted]. -[8]

[redacted]

[redacted] -[9]

1. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

2. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

3. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.
4. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

5. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

6. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

7. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

8. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, información reservada de la Entidad, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.

9. Se protegen del Plan de Seguridad y Privacidad de la Información 2023-2026, los datos de identificación del jefe del CPD, de acuerdo con el Artículo 21 de la Ley 1712 de 2014, por contener información clasificada como reservada conforme lo establece el Artículo 33 de la Ley Estatutaria 1621 de 2013, y el Libro 2, Parte 2, Título 3, Capítulo 1, del Decreto 1070 de 2015.