UNP

Plan

DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GTE-PL-02-V8

Gestión tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
31-01-2025

Tabla de contenido

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2025-2026.

1.2. Objetivos Específicos

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la UNP, comparte el alcance definido en la Política de Seguridad de la Información.

3. DEFINICIONES:[1]

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- Activo: En relación con la seguridad de la información, se refiere a cualquier información elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

[1] Fuente. Modelo de Seguridad y Privacidad de la Información" - Anexo 1 de la Resolución 500 de 2021 de MinTIC https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como Testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados

de los mismos (Ley 1712 de 2014, art 6)

- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- Información Pública Clasificada: Es aquella información que estando en poder o

custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, amonificación o cifrado.

- Partes interesadas (Stakeholders): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de

  demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada,

que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. MARCO LEGAL:

Tabla 1 MARCO LEGAL

Norma	Número	Año	Descripción - Epígrafe
Constitución Política	N_A	1991	Constitución Política de Colombia
Ley	1915	2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Ley	1712	2014	Ley de transparencia y del derecho de acceso a la información pública nacional
Ley	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Norma	Número	Año	Descripción - Epígrafe
Ley	1341	2009	Por el cual las Entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones
Ley	1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto	1263	2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública
Decreto	767	2022	Por el cual se establecen los lineamientos generales de la Norma de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto	2106	2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
Decreto	612	2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015
Decreto	1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto	1083	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública
Decreto	886	2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto	1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto	2609	2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto	4065	2011	Por el cual se crea la Unidad Nacional de Protección (UNP), se establecen su objetivo y estructura.
Resolución	746	2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No.500 de 2021.

Norma	Número	Año	Descripción - Epígrafe
Resolución	500	2021	Por el 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. (MinTIC)
Resolución	1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
Resolución	1773	2024	Por medio de la cual se establece la Política Integral de Administración de Riesgos de la Unidad Nacional de Protección
Resolución	1774	2024	Por la cual se dictan lineamientos para la implementación del Modelo de seguridad y privacidad de la información de la Unidad Nacional de Protección, se actualiza la Política de Seguridad y Privacidad de la información y se deroga la Resolución 1847 de 2018
Resolución	1767	2024	Por la cual se organizas el Modelo Integrado de planeación y Gestión (MIPG-SIG) de la Unidad Nacional de Protección y se dictan otras disposiciones
Resolución	0649	2024	Por medio de la cual se adopta la Política del Modelo Integrado de Planeación y Gestión – Sistema Integrado de Gestión de la UNP
Resolución	0054	2024	Por medio de la cual se actualiza la Plataforma Estratégica de la Unidad Nacional de Protección – UNP para el período 2023 – 2026 y se deroga la Resolución 0199 del 2 de marzo de 2020
Resolución	0932	2023	Por medio de la cual se crea el Grupo de las Tecnologías (GGT) y modifica parcialmente la Resolución número 501 de 2021.
Resolución	2460	2022	Por medio de la cual se regula la Norma de Teletrabajo en la Unidad Nacional de Protección, se derogan las Resoluciones 1228 y 1826 de 2021, y se dictan otras disposiciones".
Directiva Presidencial	9	2018	Directrices de Austeridad.
Directiva Presidencial	4	2012	Eficiencia Administrativa y Lineamientos de la Norma Cero Papel en la Administración Pública.
CONPES	3995	2020	Norma Nacional de Confianza y Seguridad Digital "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías".
CONPES	3854	2016	Nacional de Seguridad Digital. Busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.

Norma	Número	Año	Descripción - Epígrafe
NTC-ISO/IEC	27001	2022	Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.
NTC-ISO	9001	2015	Norma Técnica Colombiana NTC-ISO 9001 Sistemas de Gestión de la Calidad.
NTC-ISO	22301	2029	Norma Técnica Colombiana NTC-ISO 22301 Sistemas de Gestión de la Continuidad del Negocio.
Modelo		2021	Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Versión 4 28/10/2021 Ministerio de Tecnologías de la Información y las Comunicaciones
Documento Maestro		2021	Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4 22/02/2021 Ministerio de Tecnologías de la Información y las Comunicaciones
Modelo		2021	Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.

Fuente: Elaboración Propia

5. CONDICIONES GENERALES:

El presente documento está enmarcado en las directrices contenidas en la Norma NTC-ISO/IEC ISO 27001:2022 y las Guías publicadas por MinTIC que busca el mejoramiento continuo del componente de gestión de seguridad de la información en el DNP, con fin de mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información digital institucional, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2025.

6. CONTENIDO

6.1 Estado Actual de la Entidad respecto al SGSI

La UNP evalúa el cumplimiento de las políticas de Gobierno Digital y Seguridad Digital a través del Formulario Único Reporte de Avances de la Gestión (FURAG) del Modelo Integrado de Planeación y Gestión, del autodiagnóstico del MSPI y la declaración de Aplicabilidad SOA GTE-FT-46.

En este sentido, con base en el resultado del autodiagnóstico interno en Seguridad y Privacidad de la Información y la Declaración de Aplicabilidad SOA GTE-FT-46, se ha obtenido el estado actual en la implementación de los controles de la Norma ISO/IEC 27001:2022:

Tabla 2 Instrumento MSPI

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad de control
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	98	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	97	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	85	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	100	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	90	100	**OPTIMIZADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	96	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	97	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	94	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	90	100	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	90	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	97	100	**OPTIMIZADO**
A.18	CUMPLIMIENTO	97,5	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**95**	**100**	**OPTIMIZADO**

Fuente: *Elaboración propia.*

Grafica 1 Instrumento madurez MSPI

Fuente Instrumento MSPI

Gráfica 2 formato SOA

Unidad Nacional de Protección

FORMATO DE DECLARACIÓN APLICABILIDAD - SOA

GESTIÓN TECNOLÓGICA

UNIDAD NACIONAL DE PROTECCIÓN

Interior

DECLARACIÓN DE APLICABILIDAD - SOA
Numeral 6.1.3 ISO 27001:2022

Control (Anexo A) ISO 27001:2022	CONTROL	Descripción del Control y Objetivo	¿Aplica? SI / No	Detallar justificación o exclusión de la aplicabilidad en la UNP	Declaración de aplicabilidad (Describir soporte)
5. ORGANIZACIONAL					
5.1	Políticas de seguridad de la información	Control: La política de seguridad de la información y las políticas de temas específicos deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal y las partes interesadas pertinentes y revisadas a intervalos planificados y si se producen cambios significativos. Objetivo: Garantizar la idoneidad, adecuación y eficacia continuas de la dirección y el apoyo a la seguridad de la información de acuerdo con los requisitos empresariales, legales, reglamentarios y contractuales.	X	La Unidad Nacional de Protección justifica la aplicación de este control a través del Manual de políticas específicas de seguridad y privacidad de la información donde se establecen lineamientos particulares de cumplimiento de cada una de las políticas internas definidas por el área de tecnología y de obligatorio cumplimiento por todas las partes interesadas internas y externas de la entidad. Adicional a esto, la UNP define a traves de acto administrativo la adopción de la Política del Sistema de Gestión de Seguridad de la información y la política general de Seguridad y privacidad de la información en cumplimiento del marco legal de la resolución 500 del 2021 del MinTic, aprobada y socializada ante el Comité Institucional de Gestión y Desempeño.	GTE-MA-02 Manual de políticas específicas de seguridad y privacidad de la información Resolución 0649 del 2024 Resolución 1774 del 2024
5.2	Roles y responsabilidades de SI	Control: Las funciones y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización. Objetivo: Establecer una estructura definida, aprobada y entendida para la implementación operación y gestión de la seguridad de la información dentro de la organización.	X	La Unidad Nacional de Protección justifica la aplicación de este control a través de la matriz de roles, responsabilidades y autoridades del SIG, se establecen los roles y responsabilidades pertinentes en SI de acuerdo con las necesidades de la entidad.	GIN-FT-33 Anexo 7. Matriz de responsabilidades y autoridades
5.3	Segregación de funciones	Control: Las funciones y las áreas de responsabilidad conflictivas deben estar separadas. Objetivo: Reducir el riesgo de fraude, error y omisión de los controles de seguridad de la información.	X	La Unidad Nacional de Protección justifica la aplicación de este control a través de la matriz de roles, responsabilidades y autoridades del SIG, se establecen los roles y responsabilidades pertinentes en SI de acuerdo con las necesidades de la entidad.	GIN-FT-33 Anexo 7. Matriz de responsabilidades y autoridades Organigrama
5.4	Responsabilidades de la dirección	Control: La administración debe exigirle a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos de cada tema de la organización. Objetivo: Garantizar que la dirección comprenda su papel en la seguridad de la información y emprender acciones encaminadas a garantizar que todo el personal sea consciente y cumpla con sus responsabilidades en materia de seguridad de la información.	X	La UNP, dentro de la segregación de responsabilidades justifica el cumplimiento de aplicación de este control a traves de los compromisos de la alta dirección definidas en acto administrativo interno de adopción de la política integrada del SIG, a su vez se aprobó y se socializó en Comité Institucional de Gestión y Desempeño. Por otro lado, la dirección tiene sus responsabilidades definidas en la Matriz de roles, responsabilidades y autoridades del SIG	Resolución 0649 del 2024 GIN-FT-33 Anexo 7. Matriz de responsabilidades y autoridades Organigrama
5.5	Contacto con autoridades	Control: La organización debe establecer y mantener contacto con las autoridades pertinentes. Objetivo: Garantizar un flujo de información adecuado con respecto a la seguridad de la información entre la organización y las autoridades legales, reglamentarias y de supervisión pertinentes.	X	Se garantiza el flujo de la información adecuada con respecto a la seguridad de la información a traves de la guía de contacto con autoridades y grupos de interés especial definidas en el SIG, dentro de este documento se definen las autoridades y como se establecen las comunicaciones y contactos entre la entidad y cada uno de ellos de acuerdo con el incidente o suceso identificado que pueda afectar la seguridad de la información.	GTE-GU-06 Guía de contacto con autoridades y grupos de interés especial
5.6	Contacto con grupos de interés especial	Control: La organización debe establecer y mantener contacto con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales. Objetivo: Garantizar que se produce un flujo adecuado de información con respecto a la seguridad de la información.	X	Se garantiza el flujo de la información adecuada con respecto a la seguridad de la información a traves de la guía de contacto con autoridades y grupos de interés especial definidas en el SIG, dentro de este documento se definen las autoridades y como se establecen las comunicaciones y contactos entre la entidad y cada uno de ellos de acuerdo con el incidente o suceso identificado que pueda afectar la seguridad de la información.	GTE-GU-06 Guía de contacto con autoridades y grupos de interés especial
5.7	Inteligencia de Amenazas - NEW	Control: La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia sobre amenazas. Objetivo: Dar a conocer el entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas.	X	La UNP define dentro de la información documenta del SIG, procedimiento de incidentes donde se referencian las clasificación de incidentes y la criticidad de cada uno de ellos y así mismo las posibles soluciones brindadas por el equipo de mesa de servicios de la entidad.	GTE-PR-43 Procedimiento Gestion de incidentes Plataforma Ivanti
5.8	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe integrar en la gestión de proyectos. Objetivo: Garantizar que los riesgos de seguridad de la información relacionados con los proyectos y los productos finales se aborden de forma eficaz en la gestión de proyectos durante todo el ciclo de vida del proyecto.	X	La UNP define lineamientos para el cumplimiento de este control descritos en documentos internos como procedimientos y formatos donde se conserva los registros de los ejercicios realizados	GTE-PR-42 Procedimiento Gestion de proyectos de TI y proveedores

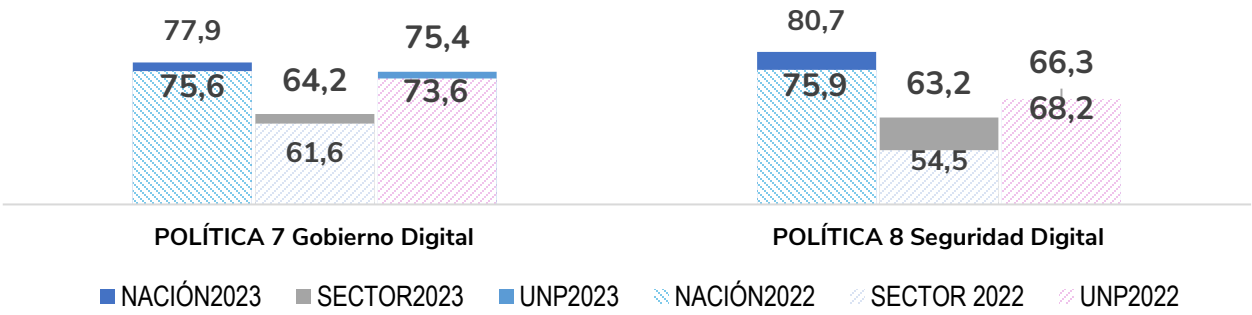
ATRIBUTOS DE ISO 27002:2022

Control	TIPO DE CONTROL			PROPIEDADES DE LA SEGURIDAD DE LA INFORMACIÓN			CONCEPTOS DE CIBERSEGURIDAD					CAPACIDAD OPERACIONAL															DOMINIOS DE SEGURIDAD			
	PREVENTIVO	DETECTIVO	CORRECTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR	GOBERNANZA / GESTIÓN	GESTIÓN DE ACTIVOS	PROTECCIÓN DE LA INFORMACIÓN Y DATOS	SEGURIDAD DE RH	SEGURIDAD FÍSICA	SEG. SISTEMAS & REDES	SEG. APLICACIONES	CONFIG. SEGURA	GEST. IDENTIDAD Y ACCESO	GESTIÓN DE AMENAZAS Y VULNERABILIDADES	CONTINUIDAD DE NEGOCIO	SEG. RELACIÓN CON PROVEEDORES	REQ. LEGALES Y DE CUMPLIMIENTO	GEST. EVENTOS Y SEG. INFORMACIÓN	GARANTÍAS DE SEG. INFORMACIÓN	GOBIERNO Y ECOSISTEMA	PROTECCIÓN	DEFENSA	RESILIENCIA
5.1	X			X	X	X	X					X															X			X
5.2	X			X	X	X	X					X															X	X		X
5.3	X			X	X	X		X				X								X							X			
5.4	X			X	X	X	X					X															X			
5.5	X		X	X	X	X	X	X		X	X	X																	X	X
5.6	X		X	X	X	X		X		X	X	X																	X	
5.7	X	X	X	X	X	X	X		X	X											X								X	X
5.8	X			X	X	X	X	X				X															X	X		

Fuente Aplicabilidad SOA GTE-FT-46

Respeto a los resultados obtenidos por las políticas de Gobierno Digital y de Seguridad Digital en la Medición del Desempeño Institucional a través del diligenciamiento del Formulario Único de Reporte y Avance de Gestión (FURAG) en línea, la Entidad obtuvo en la primera un puntaje de 75,4 en la vigencia 2023 superando el sector que alcanzó 64,2 puntos.

Gráfico 3 Resultados FURAG



Elaboración propia
Fuente: https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

Por su parte el resultado en la política de Seguridad Digital arrojó un resultado de 66, 3 puntos en la vigencia 2023 superando al sector que alcanzó 63,2 puntos.

Para mayor visibilidad en los resultados a continuación se detallan los puntajes de los índices desagregados por estas políticas en la vigencia 2023.

Tabla 3 Gobierno Digital:

I11.Gobernanza	I12.Innovación Pública Digital	I13.Arquitectura	I14.Seguridad y Privacidad de la información	I15.Servicios Ciudadanos Digitales
100,0	70,8	68,0	90,4	0,0

I16.Cultura y apropiación	I17.Servicios y Procesos Inteligentes	I18.Estado abierto	I19.Decisiones basadas en datos	I20.Proyectos de Transformación Digital
60,0	64,3	82,4	80,0	77,8

Tabla 4 Seguridad Digital

I22.Asignación de Recursos	I23.Implementación Lineamientos de Política	I24.Despliegue de Controles
61,1	66,7	82,1

Elaboración propia
Fuente: https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

Estos puntajes demuestran la mejora continua y el compromiso en la materia acorde a los lineamientos del Gobierno Nacional.

Con base en estos resultados, se propone para el cumplimiento del plan el desarrollo de las siguientes fases en la vigencia, las cuales se detallan en el numeral 6.2.3. Hoja de Ruta Plan de Seguridad y Privacidad de la información y Estrategia Digital

- Actualización del alcance del SGSI
- Actualización de los objetivos del SGSI
- Realización de pruebas de vulnerabilidades de infraestructura
- Documento del DRP y sus acciones
- Actualizar el documento del BIA
- Realizar pruebas de contingencia infraestructura continuidad de negocio
- Realizar pruebas de contingencia sistemas de información
- Realizar pruebas de vulnerabilidades sistemas de información
- Desarrollo de Auditorías Internas en Seguridad y Privacidad de la Información
- Maduración de Controles en Seguridad y Privacidad de la Información

6.2. Estrategia de Seguridad Digital

La Unidad Nacional de Protección UNP establece la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, bajo la premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse.

Por tal motivo, la Unidad Nacional de Protección UNP define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Grafica 5 Estrategia de seguridad digital

Fuente: Tomado de MINTIC

6.2.1. Descripción de las Estrategias Específicas (Ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

Tabla 5 Descripción de estrategias

Estrategia / Eje	Descripción/Objetivo
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de los procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Fuente: *Elaboración propia. A partir de información MINTIC*

6.2.2. Ejes de la Estrategia de Seguridad Digital / fases:

Para cada estrategia específica, la Unidad Nacional de Protección UNP define los siguientes fases y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Tabla 6 Ejes de la Estrategia de Seguridad Digital

Estrategia /eje	Fases	Productos Esperados
Liderazgo de seguridad de la información	1. Aprobación del Plan de Seguridad y Privacidad de la información con la Estrategia Digital para la vigencia 2. Actualizar la Política de Política de Seguridad y Privacidad de la Información Incorporando la Estrategia Digital 3. Definición de Roles y Responsabilidades de Seguridad de la Información.	1. Constancia Secretarial 2. Política Actualizada acto administrativo 3. Roles y Responsabilidades en Seguridad de la Información formalizados en las políticas de seguridad
Gestión de riesgos	1. Identificar, valorar y clasificar los riesgos asociados a los activos de información. 2. Definir planes de tratamiento de riesgos de seguridad	1. Matriz de riesgos de seguridad digital en el Plan de Tratamiento de Riesgos 2. Plan de tratamiento de riesgos Aprobado
Concientización	1. Establecer desde el inicio de cada año la planeación de sensibilización para todo el año. 2. Realizar trasferencia de conocimiento a los servidores y contratistas 3. Medir el grado de sensibilización a toda la UNP	1. Propuesta de sensibilización para el Plan Institucional de Capacitaciones PIC 2. Evidencias de las actividades desarrolladas certificaciones de cursos si aplica 3. Resultado de encuesta de medición
Implementación de documentación controles	1. Creación, actualización y formalización de documentos	1. Procedimientos, guías, manuales según corresponda
Gestión de incidentes	1. Sensibilizar al personal en la gestión de incidentes de seguridad de la información.	1. Sesiones de sensibilización desarrolladas.

Fuente: *Elaboración propia. A partir de información MINTIC*

7. META ESTABLECIDA

La meta para el Plan de Seguridad y Privacidad de la Información será de 100% de cumplimiento.

8. INDICADOR DE MEDICIÓN

Para la gestión del indicador del Plan se realizará un seguimiento a cada una de las Actividades así:

Tabla 7 indicador

Nombre del indicador	Objetivo	Fórmula	Meta Trimestral
Cumplimiento del Plan de Seguridad y Privacidad de la Información (incluye la Estrategia de Seguridad Digital)	Medir el porcentaje de cumplimiento de las Actividades definidas en el Plan de Seguridad y Privacidad de la Información (incluye la Estrategia de Seguridad Digital)	(Actividades ejecutadas / Actividades programadas) *100%	100%

Fuente: Elaboración Propia

Tabla 8 Ponderación y meta del indicador

Trimestre	Ponderación Actividades del trimestre	META Anual
I Trimestre	25%	100%
II Trimestre	25%	
III Trimestre	25%	
IV Trimestre	25%	

Fuente: Elaboración Propia

9. Hoja de Ruta Plan de Seguridad y Privacidad de la información y Estrategia Digital (Cronograma)

Plan / Estrategia		PROGRAMACIÓN 2025											
Proyecto	Actividades	En	Feb	Mar	Abr	May	Jun	Jul	Ag	Sep	Oct	Nov	Dic
Plan de Seguridad y Privacidad de la Información	Actualización del alcance del SGSI	15%											
	Actualización de los objetivos del SGSI												
	Realización de 2 pruebas de vulnerabilidades infraestructura												
	Actualizar un documento del DRP y sus acciones												
	Actualizar un documento del BIA				15%								
	Realizar una prueba de contingencia de continuidad de negocio												
	Realizar una prueba de contingencia a sistemas de información												
	Realización de 2 pruebas de vulnerabilidades de infraestructura							15%					

Plan / Estrategia		PROGRAMACIÓN 2025											
Proyecto	**Actividades**	**En**	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ag**	**Sep**	**Oct**	**Nov**	**Dic**
	Realización una prueba de vulnerabilidades sistemas de información												
	Desarrollo de una Auditoría en Seguridad y Privacidad de la Información										**15%**		
	Realización una prueba de contingencia a sistemas de información.												
	Aplicación del autodiagnóstico MINTIC												
Estrategia Digital	Aprobación del Plan de Seguridad y Privacidad de la información con la Estrategia de Seguridad Digital	**10%**											
	Actualizar la Política de Seguridad y Privacidad de la Información incorporando la Estrategia de Seguridad Digital												
	Creación y/o actualización de un documento que apoye la operación												
	Entrega de una propuesta de sensibilización para incluir en el Plan Institucional de Capacitación PIC.												
	Definición un documento de roles y responsabilidades de Seguridad de la Información.				**10%**								
	Realizar una trasferencia de conocimiento a los servidores y contratistas												
	Acto administrativo de la Política con inclusión de la Estrategia de Seguridad Digital												
	Creación y/o actualización de un documento que apoye la operación.												
	Solicitar reporte del PIC en relación con la sensibilización propuesta.							**10%**					
	Realizar una sensibilización al personal en la gestión de incidentes de seguridad de la información.												
	Realizar una trasferencia de conocimiento a los servidores y contratistas.												
	Definición de las tecnologías de la información y las comunicaciones, incluida la adopción de nuevas tecnologías o tecnologías emergentes.										**10%**		
	Realizar una sensibilización al personal en la gestión de incidentes de seguridad de la información.												

10. DOCUMENTOS RELACIONADOS:

- GTE-MD-01 Modelo de Seguridad y Privacidad de la Información.
- GTE-FT-46 Declaración de Aplicabilidad SOA.

11. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del Plan Seguridad y Privacidad de la Información	31/01/2019	01
01	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02
02	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2021	20/01/2021	03
03	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2022	20/01/2022	04
04	Actualización de las fechas propuestas en el cronograma de actividades del plan de Seguridad y Privacidad de la Información y desglose de la meta propuesta en el indicador, por valores acumulativos de porcentaje en cada uno de los semestres.	17/05/2022	05
05	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia, se hace claridad con relación a la metodología de trabajo y actualización de las actividades en el cronograma para el Anexo y el plan de Seguridad y Privacidad de la Informaciónn para la vigencia 2024.	29/01/2024	06
06	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia, enmarcado en las directrices contenidas en la Norma NTC-ISO/IEC ISO 27001:2022 y las Guías publicadas por MinTIC	20/03/2024	07
07	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2025, se incluyen las actividades de Estado Actual del Sistema de Gestión en Seguridad y Privacidad de la Información, Proceso de Seguridad y Privacidad de la Información, Política general de Seguridad y Privacidad de la Información, Ámbito general de Seguridad y Privacidad de la Información. Se incluye el cronograma en el contenido del plan.	31/01/2025	08

12. CRÉDITOS:

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró: Nombre: Elsa Marlen Baracaldo Huertas Cargo: Contratista Grupo de Gestión de las Tecnologías (GGT) – Oficina Asesora de Planeación e Información	
Elaboró: Nombre: John Anderson Hernandez Correa Cargo: Contratista Grupo de Gestión de las Tecnologías (GGT) – Oficina Asesora de Planeación e Información	
Revisó: Nombre: Javier Francisco Rodríguez Moreno Cargo: Jefe (E) Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Augusto Rodriguez Ballesteros Cargo: Director General	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG-SIG	
Oficializó: Nombre: Javier Francisco Rodríguez Moreno Cargo: Jefe (E) Oficina Asesora de Planeación e Información	