Departamento Nacional de Planeación

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE TECNOLOGÍA Y SISTEMAS DE LA INFORMACIÓN

DEPARTAMENTO NACIONAL DE PLANEACIÓN
2025

Tabla de contenido

1. OBJETIVOS 3
1.1. OBJETIVO GENERAL 3
1.2. OBJETIVOS ESPECÍFICOS 3
2. ALCANCE 3
3.DOCUMENTOS DE REFERENCIA Y GLOSARIO 3
4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5
4.1. Resultados Instrumentos de medición 5
4.2. Balance APCM 6
4.3. Indicadores del componente de seguridad de la información 7
5. ESTRATEGIA DE SEGURIDAD DIGITAL 7
5.1. Descripción de las estrategias específicas (ejes) 8
5.2. Actividades 8
5.3. Alineación con los objetivos del componente de seguridad de la información 8
5.3.1. Plan de Seguridad y Privacidad de la Información 9
5.3.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 19
5.4. Análisis Presupuestal 40
6. CONTROL DE VERSIONES 40

1. OBJETIVOS

1.1. Objetivo General

Realizar 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.

1.2. Objetivos Específicos

- Fortalecer la cultura de seguridad de la información en la Entidad a través de la ejecución integral del Plan de capacitación, sensibilización y comunicación de seguridad de la información alineado con el Plan institucional de Capacitación PIC.
- Mejorar la protección y gestión de los activos de información del DNP mediante la actualización periódica de los activos de información y la declaración de aplicabilidad ISO 27001.
- Evaluar y mitigar riesgos de seguridad de la información mediante la realización de ejercicios de ingeniería social, el monitoreo de primera y segunda línea de defensa y la actualización del autodiagnóstico del Anexo 3 de Seguridad Digital de la Resolución 1519 de 2019.
- Actualizar el autodiagnóstico Modelo de seguridad y Privacidad de la información (MSPI), el autodiagnóstico de la Resolución 500 de 2021 y el autodiagnóstico Resolución 746 de 2022.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la mejora continua el componente de Gestión de Seguridad de la Información y la estrategia de seguridad digital del DNP, comparte el alcance definido dentro M-PG-07 Manual Operativo de Seguridad de la información y el MC Manual del SIG, donde se indica que el componente de seguridad aplica a todos los procesos de la Entidad incluidos en el Modelo de Operación por procesos.

3.DOCUMENTOS DE REFERENCIA Y GLOSARIO

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para la definición de actividades:

- Decreto 612 de 2018[1]. “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”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 1519 de 2019[2] Anexo 3. “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 500 de 2021[3]. “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”.
- Resolución 746 de 20224.“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 500 de 2021”

---

[1] https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30034635

[2] https://www.suin-juriscol.gov.co/viewDocument.asp?id=30044657

[3] https://www.suin-juriscol.gov.co/viewDocument.asp?id=30044822

[4] https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf

- Manual de Gobierno Digital – MINTIC[5].
  - Modelo de Seguridad y Privacidad de la Información – MINTIC[6].
  - Anexo 1 - Normograma y otros documentos de origen externo[7] que contiene la normativa relacionada con seguridad de la información.
  - Índice de Gobierno Digital[8]
  - Medición del Desempeño Institucional (Política Seguridad Digital) 2022[9].
  - Medición del Desempeño Institucional (Política Seguridad Digital) 2023[10].
  - Normas ISO de Seguridad de la información ISO 27001:2013[11], ISO 27002:2015[12]; ISO 27001:2022; ISO 27002:2022[13].
  - Informes de auditorías de control interno[14]: AUDITORÍA INTERNA - PROCESO GESTIÓN JURIDICA(20243400095733), AUDITORÍA INTERNA - PROCESOS LIDERADOS DPIP(20243400095683), AUDITORÍA INTERNA - PROCESOS LIDERADOS POR LA SGTH(20243400164113), AUDITORÍA INTERNA - MODELO DE OPERACIÓN POR PROCESOS MOP(20243400149903, 20243400167553, 20243400167533, 20243400164663), AUDITORIA INTERNA - PROCESO DE GESTIÓN FINANCIERA 2024(20243400211443), AUDITORÍA INTERNA - PROCESO GESTIÓN CONTRACTUAL(20243400204333), AUDITORÍA INTERNA - PROCESOS ASISTENCIA TÉCNICA Y GESTIÓN DE INFORMACIÓN, CONOCIMIENTO E INNOVACIÓN(20243400205873), EVALUACIÓN DERECHOS DE AUTOR DNP(20243400058843), EVALUACIÓN A LA GESTIÓN DE LAS DEPENDENCIAS 2023 Y FORMULACIÓN PLAN DE ACCIÓN 2024-DEPENDENCIA OTSI(20243400042673), EVALUACIÓN A LA GESTIÓN DE DEPENDENCIAS - OTSI(20243400124873), EVALUACIÓN PROYECTOS DE INVERSIÓN 2024 – – BPIN:2022011000029(20243400179213), SEGUIMIENTO SEGURIDAD SIIF NACIÓN(20243400201213), INFORME CONSOLIDADO - SISTEMA DE SEGURIDAD DE LA INFORMACIÓN(20243400212013), INFORME CONSOLIDADO DE GESTIÓN INTEGRAL DE RIESGOS DEL DNP(20243400212983), INFORME CONSOLIDADO SISTEMA DE GESTIÓN ANTISOBORNO(20243400213503), INFORME CONSOLIDADO DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN MIPG(20243400213153), SEGUIMIENTO PLANES DE MEJORAMIENTO AUDITORÍAS CGR(20246800201303).

- **GLOSARIO[15]**

  - Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas

  - Seguridad de la Información: Este principio de la Política de Gobierno Digital busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

---

5 https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf
6 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
7 https://colaboracion.dnp.gov.co/CDT/DNP/SIG/Anexo%201%20-%20Normograma%20y%20otros%20documentos%20de%20origen%20externo.xlsx
8 https://gobiernodigital.mintic.gov.co/portal/Mediciones/
9 https://www1.funcionpublica.gov.co/web/mipg/resultado-historico-2022
10 https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion
11 https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/
12 https://tienda.icontec.org/gp-tecnologia-de-la-informacion-tecnicas-de-seguridad-codigo-de-practica-para-controles-de-seguridad-de-la-informacion-gtc-iso-iec27002-2015.html
13 https://tienda.icontec.org/gp-gtc-iso-iec-seguridad-de-la-informacion-ciberseguridad-y-proteccion-de-la-privacidad-controles-de-seguridad-de-la-informacion-gtc-iso-iec27002-2022.html
14 Sistema de Gestión Documental ORFEO
15 Anexo 1. Glosario Manual Operativo https://colaboracion.dnp.gov.co/CDTI/SGSI/ANEXO%20GLOSARIO%20M-PG-07.pdf

- Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

- Seguridad Informática: o también llamada ciberseguridad, se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes datos demuestran la mejora continua y el compromiso de la Entidad por la implementación de controles y lineamientos en seguridad de la información, seguridad informática y seguridad digital acorde a los lineamientos del Gobierno Nacional.

4.1. Resultados Instrumentos de medición

Como entidad del Gobierno Nacional, el DNP evalúa el cumplimiento de las políticas de Gobierno Digital y Seguridad Digital a través diferentes instrumentos. La siguiente tabla presenta el porcentaje obtenido en cada vigencia

Instrumento	Año	% Calificación	Objetivo 2025	Herramienta
Índice de Gobierno Digital (Seguridad y Privacidad de la información)	2023	84,50%	Subir Calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información. 6240 7.Plan implementación y mantenimiento de la política de gobierno digital en el DNP
	2022	94,40%		
Medición del Desempeño Institucional (Política Seguridad Digital)	2023	91,90%	Mantener calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.
	2022	90,40%		
Modelo de Seguridad y privacidad de la Información	2024	98%	Mantener calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.
	2023	96%		
	2022	95%		
Resolución 1519 de 2019 Anexo 3*	2024	46%	Subir Calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.
	2022	69%		
Resolución 746 de 2022	2023-2024	70%	Mantener calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.
ISO 27001:2022	2023-2024	94%	Mantener calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.
ISO 27002:2022	2023-2024	35%	Subir Calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.
Resolución 500 de 2021	2022-2024	93%	Mantener calificación	6232 4. Plan especial de gestión de seguridad y privacidad de la información.

* En 2022 sólo se evaluó el portal del DNP, la calificación del Anexo 3 de la resolución 1519 de 2019 disminuyó en la vigencia 2024 porque se realizó el diagnóstico de los 68 Sistemas de información incluidos en el catálogo de sistemas de información vigentes durante el periodo de evaluación, identificando herramientas y criterios comunes en la evaluación.

4.2. Balance APCM

De acuerdo con el Balance de acciones disponible en O:\Plan de Mejoramiento\Balance APCM 17.12.2024 p.xlsx con corte a diciembre de 2024, se definieron 55 APCM, distribuidas así

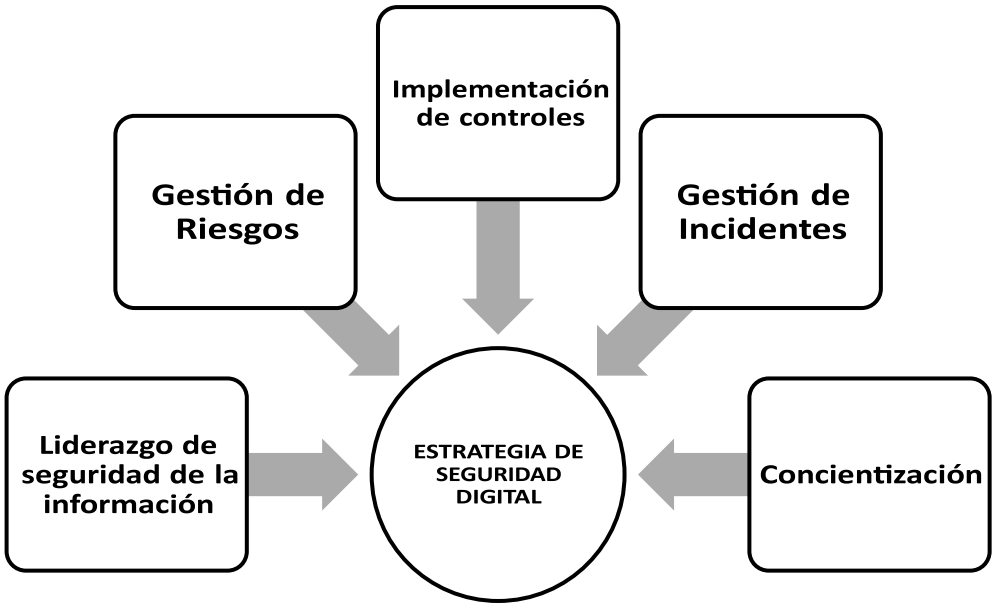
Estado	Tema	Dependencia	Numero de APCM	Situación Identificada	Criticidad
Debería Reprogramar	Documentos del SGSI	OTSI	1	Oportunidad de Mejora	Media
	Riesgos	OTSI	1	No Conformidad	Alta
Dentro del plazo	activos de información	SGTH	2	No Conformidad	Alta
	Alistamiento de equipos	OTSI	1	Corrección	Alta
	Catálogo de Sistemas de Información	OTSI	2	No Conformidad	Alta
	Catálogo de Sistemas de Información	DSECSGR	1	No Conformidad	Alta
	Datos personales	SGTH	1	No conformidad	Alta
	Datos personales	OTSI	1	No conformidad	Alta
	Documentos del SGSI	OTSI	5	Oportunidad de Mejora	Media
	Documentos del SGSI	OTSI - OAP	1	Oportunidad de Mejora	Media
	Entregables del Sistema de Información.	OTSI	2	No Conformidad	Alta
	Gesproy	DSEC-SAR	1	No Conformidad	Alta
	Gestión documental	SARC - GBB	3	No Conformidad	Alta
	Información Intranet	OTSI	1	Oportunidad de Mejora	Media
	Inventario de software	OTSI	1	No Conformidad	Alta
	ORFEO	DC	1	No Conformidad	Alta
	ORFEO	SARC - GBB	1	No Conformidad	Alta
	ORFEO	OTSI	1	No Conformidad	Alta
	políticas de Seguridad en el Puesto de trabajo	SGTH	2	No Conformidad	Alta
	políticas de Seguridad en el Puesto de trabajo	SGTH - OTSI	1	No Conformidad	Alta
	Proyecto BPIN 2022011000029	OTSI-GGIT OTSI-GGSI OTSI-GGU OTSI-GPGT OAP	2	Oportunidad de Mejora	Media
	Proyecto BPIN 2022011000029	OAP - OTSI	1	Oportunidad de Mejora	Media
	Proyecto BPIN 2022011000029	OTSI - DPIIP - OAP	1	Oportunidad de Mejora	Media
	Proyecto BPIN 2022011000029	OAP -OTSI	1	Oportunidad de Mejora	Media
	Proyecto BPIN 2022011000029	OTSI	1	Oportunidad de Mejora	Media
	Riesgos	OTSI	5	No Conformidad	Alta
	SISGESTION	OTSI	1	No Conformidad	Alta
	SUCOP	OTSI	1	No Conformidad	Alta
	SUIFP SGR	DPIP	1	No Conformidad	Alta
Vencida	Gesproy	SARC	1	No Conformidad	Alta
	Gestión documental	SARC	4	Oportunidad de Mejora	Media
	Permisos Discos de red	OAJ	1	No Conformidad	Alta
	SISGESTION	OAP	1	No Conformidad	Alta
		OAP	4	Oportunidad de Mejora	Media
		Total	55		

4.3. Indicadores del componente de seguridad de la información

Tipo	Vigencia	Cantidad	Objetivo 2025	Herramienta
Activos de Información identificados	2024	1146	Subir número de activos, se incluirán las tipologías documentales	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
	2022	518		
	2023	789		
Riesgos de seguridad de la información	2022	6	Mantener el número de riesgos, monitorear el indicador GSI-03	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
	2023	6		
	2024	6		
Indicador GSI-01 Tratamientos de eventos relacionados con la seguridad y privacidad de la información	2024	93,75%	Mantener calificación	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
Indicador GSI-02 Cumplimiento del plan de implementación de aspectos de seguridad de la información en la continuidad de negocio en el componente tecnológico	2024	100%	Mantener calificación	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
Indicador GSI-03 Porcentaje de avance en la implementación de controles de seguridad de la información	2024	75%	Mantener calificación	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
Indicador GSI-04 Medición de la Efectividad del Plan de sensibilización del componente de seguridad de la Información	2024	96%	Mantener calificación	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
APCM	Debería Reprogramar	2	Apoyar a las dependencias en el cierre de las acciones	6232 4.Plan especial de gestión de seguridad y privacidad de la información.
	Dentro del plazo	42		
	Vencida	11		

5. ESTRATEGIA DE SEGURIDAD DIGITAL

En cumplimiento de la Resolución 500 de 2021 la entidad establece una estrategia de seguridad digital que integra los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia se basa en la implementación del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC, el procedimiento PT-PG-01 Gestión integral de riesgos y el procedimiento PTTI-01 Atención a Requerimientos de Servicios TIC que incluye la de gestión de incidentes. Por lo anterior la Entidad adopta las 5 estrategias específicas propuestas por MINTIC, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Fuente: MINTIC https://gobiernodigital.mintic.gov.co/portal/Biblioteca/#data=%7B%22filter%22:%2247254%22,%22page%22:6%7D

5.1. 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:

ESTRATEGIA/EJE[16]	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 las diferentes dependencias y/o 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.

5.2. Actividades

Las estrategias se incluyen en el producto denominado "4. Plan especial de gestión de seguridad y privacidad de la información." que hace parte del plan de acción institucional disponible en https://www.dnp.gov.co/LaEntidad_/Direcciongeneral/oficina-asesora-planeacion/Paginas/planeacion-institucional.aspx

Objetivo Institucional: Gestión integral institucional - Posicionar al DNP como referente en gestión institucional articulada, innovadora y efectiva

Eje estratégico / Proyecto: 5. Fortalecer las capacidades de articulación interna y de gestión integral, hacia la toma de decisiones, para la generación de resultados efectivos y con vocación de servicio hacia los grupos de valor.

Proceso: Planeación y gestión orientada a resultados
Dependencia: Oficina de Tecnología y Sistemas de la Información

Nombre Línea Acción	Nombre Procedimiento	Código Producto	Nombre Producto	Tipo Seguimiento	Meta	Código Entregable	Denominación Entregable	Fecha Inicio	Fecha Fin	Clasificador Producto
Administración y mantenimiento del MOP	Planeación y mantenimiento del MOP	6482	4.Plan especial de gestión de seguridad y privacidad de la información.	Servicio por Oferta	3	17944	4.Informes plan especial de gestión de seguridad y privacidad de la información	2/01/2025	31/12/2025	11. MIPG - Seguridad digital 10. MIPG - Gobierno digital 20. Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI 21. Plan de Seguridad y Privacidad de la Información 53. ODS 16 - Paz, Justicia e Instituciones Solidas 68. BPIN 2022011000029 Fortalecimiento de las TIC para el cumplimiento de los objetivos del DNP a nivel Nacional

Proceso: Planeación y gestión orientada a resultados
Dependencia: Oficina Asesora de Planeación

Nombre Línea Acción	Nombre Procedimiento	Código Producto	Nombre Producto	Tipo Seguimiento	Meta	Código Entregable	Denominación Entregable	Fecha Inicio	Fecha Fin	Clasificador Producto
Gestión integral de riesgos	Gestión integral de riesgos	6530	Informe de seguimiento al monitoreo de gestión de riesgos en el DNP publicado.	Servicio por Oferta	3	18198	Informe de seguimiento al monitoreo de gestión de riesgos en el DNP publicado	1/01/2025	31/12/2025	01. MIPG - Planeación Institucional 74. BPIN 202300000000064 Fortalecimiento Institucional de la Planeación, Gestión y Evaluación del DNP A Nivel Nacional

5.3. Alineación con los objetivos del componente de seguridad de la información

Las actividades definidas están alineadas a los 4 objetivos específicos del componente de seguridad de la información

16 Fuente: MINTIC https://gobiernodigital.mintic.gov.co/portal/Biblioteca/#data=%7B%22filter%22:%2247254%22,%22page%22:6%7D

5.3.1. Plan de Seguridad y Privacidad de la Información

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	1	Estructurar los planes de seguridad de acuerdo con el Decreto 612 de 2018	*Correo a gpcalidad@dnp.gov.co con la solicitud de publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan de Seguridad y Privacidad de la Información y Plan Estratégico de Seguridad y Privacidad en el portal del DNP	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	1	Estructurar los planes de seguridad de acuerdo con el Decreto 612 de 2018	*Publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan de Seguridad y Privacidad de la Información y Plan Estratégico de Seguridad y Privacidad en la intranet en la sección del componente de seguridad de la información	Jefe OTSI.Oficial de Seguridad.	Gestor Integral OTSI.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	2	Reportar planes de seguridad de acuerdo con el Decreto 612 de 2018	*Correo a gpcalidad@dnp.gov.co con el reporte cuatrimestral de los planes para su publicación Portal del DNP(abril, agosto, diciembre)	Jefe OTSI.	Gestor Integral OTSI.Oficial de Seguridad.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	2	Reportar planes de seguridad de acuerdo con el Decreto 612 de 2018	*Publicación del reporte cuatrimestral de los planes en la intranet en la sección del componente de seguridad de la información(abril, agosto, diciembre)	Jefe OTSI.	Gestor Integral OTSI.Oficial de Seguridad.Delegado Web OTSI.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Correo de gpcalidad@dnp.gov.co con la solicitud de actualización cuatrimestral del Anexo 1 - Normograma y otros documentos de origen externo al (abril, agosto, diciembre)	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Correo de gpcalidad@dnp.gov.co con la solicitud de actualización del Anexo 2 - Despliegue del modelo de operación por procesos al	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Correo a gpcalidad@dnp.gov.co con la solicitud de actualización de la matriz de cambios del SIG	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.		#										
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Correo a gpcalidad@dnp.gov.co con la solicitud de actualización de la Matriz de Comunicación, Participación y Consulta del SIG	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
legales vigentes aplicables a la utilización de la información digital.																		
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Correo a gpcalidad@dnp.gov.co con la solicitud de actualización semestral del Manual operativo de seguridad de la información M-PG-07	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.Asesor seguridad de la información.Dependencias.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento actualizado del autodiagnóstico del Modelo de seguridad y privacidad de la Información de MINTIC (semestral)	Jefe OTSI.	Oficial de Seguridad.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento actualizado del autodiagnóstico de la norma ISO 27001:2013 (Semestral)	Jefe OTSI.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento actualizado del autodiagnóstico de la norma ISO 27001:2022 (Semestral)	Jefe OTSI.	Oficial de Seguridad.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento actualizado del autodiagnóstico de la Resolución 500 de 2021	Jefe OTSI.	Oficial de Seguridad.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento actualizado del autodiagnóstico de la Resolución 746 de 2022	Jefe OTSI.	Oficial de Seguridad.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento con la revisión y actualización de los enlaces componente seguridad de la información en la intranet	Jefe OTSI.	Oficial de Seguridad.Delegado Web OTSI.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
legales vigentes aplicables a la utilización de la información digital.																		
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	3	Actualizar los documentos del componente de seguridad de la información	*Documento con la revisión y actualización de los enlaces componente seguridad de la información en el portal web del DNP	Oficial de Seguridad.	Delegado Web OTSI.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	4	Revisión por la Dirección	*Correo a gpcalidad@dnp.gov.co con la estructura de presentación para la alta dirección	Jefe OTSI.Oficial de Seguridad.	Asesor seguridad de la información.Arquitecto Empresarial.Contratista Gobierno Digital .												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	*Correo a gpcalidad@dnp.gov.co con la actualización del procedimiento, manual, formatos de activos de información	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.Subdirección Administrativa y Relacionamiento con la Ciudadanía.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	Correo a gpcalidad@dnp.gov.co con la actualización del formato inventario de datos personales	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Gestor Integral OTSI.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	*Solicitud de actualización semestral de activos de información a las dependencias (I Semestre)	Oficial de Seguridad.	Gestor Integral OTSI.Dependencias.Gestor SIG dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	*Consolidación semestral de los activos de información de las dependencias	Oficial de Seguridad.	Dependencias.Gestor SIG dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	*Publicación semestral de los activos de información	Oficial de Seguridad.	Oficina Asesora de Comunicaciones.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	*Solicitud revisión jurídica a la OAJ de los activos de información (activos, nuevos o que cambiaron la clasificación)	Jefe OTSI.	Oficial de Seguridad.Oficina Asesora Jurídica.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	5	Actualizar los activos de información	*Publicación de los activos de información (Luego revisión Final OAJ)	Oficial de Seguridad.	Oficina Asesora de Comunicaciones.												
OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Concientización	6	Actualizar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información	*Documento con la estructura del Plan de capacitación, sensibilización y comunicación del componente de seguridad de la información	Jefe OTSI.	Oficial de Seguridad.												
OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Concientización	6	Actualizar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información	*Diseño y ejecución Charlas (Inducción y reinducción inicio marzo, Inducción OTSI mitad marzo, Continuidad de negocio final marzo)	Oficial de Seguridad.	Oficina Asesora de Planeación.Dependencias.Gestor SIG dependencias.Subdirección de Gestión del Talento Humano.												
OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Concientización	6	Actualizar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información	*Informe a las dependencias de la ejecución del Plan de capacitación, sensibilización y comunicación de seguridad de la información (correos y/o memorandos)	Jefe OTSI.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Concientización	6	Actualizar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información	*Envío de mensajes mensuales de correo electrónico de bienvenida a nuevos colaboradores	Oficial de Seguridad.	Centro de servicios.												
OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Concientización	6	Actualizar y ejecutar el plan de capacitación, sensibilización y comunicación de seguridad de la información	*Generar estadísticas cuatrimestrales de participación	Oficial de Seguridad.	Dependencias.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de incidentes	7	Realizar el reporte de los Indicadores de seguridad de la información	*Reporte Indicador GSI-01 Tratamientos de eventos relacionados con la seguridad y privacidad de la información	Jefe OTSI.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de incidentes	7	Realizar el reporte de los Indicadores de seguridad de la información	*Reporte del incidentes de seguridad a Colcert y actualización del expediente de Orfeo	Jefe OTSI.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de incidentes	7	Realizar el reporte de los Indicadores de seguridad de la información	* Seguimiento al reporte Indicador GSI-02 Cumplimiento de la gestión de la seguridad de la información en la continuidad de negocio en el componente tecnológico	Jefe OTSI.Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de incidentes	7	Realizar el reporte de los Indicadores de seguridad de la información	*Reporte Indicador GSI-04 Medición de la Efectividad del Plan de sensibilización del componente de seguridad de la Información	Jefe OTSI.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de incidentes	7	Realizar el reporte de los Indicadores de seguridad de la información	*Reporte de los indicadores del MSPI no incluidos en el SIG	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Oficial de Seguridad.												
OECS3: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.	Implementación de controles	8	Realizar el seguimiento a la implementación de Directiva Presidencial 1 de 2024 (Ahorro Energía)	* Reporte del apagado de equipos	Jefe OTSI.	Grupo Soporte a usuarios OTSI.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Ajustar la designación de un responsable de la Seguridad Digital - (Ciberseguridad)	Jefe OTSI.	Oficial de Seguridad.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Escalar la necesidad a la Secretaria General, porque el rol de Oficial de Protección de datos con perfil de abogado y experiencia en la materia.(Para implementar un sistema para el cumplimiento de la ley 1581 de 2012 - Ley de Protección de Datos Personales)	Jefe OTSI.	Oficial de Seguridad.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Análisis opción de certificación externa en ISO 27001	Jefe OTSI.	Oficial de Seguridad.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Recolección evidencia FURAG 2024 Politica de Seguridad Digital(Gobernanza, Presupuesto, Backup, DRP, Riesgos, Controles, Datos personales, Incidentes) y Politica de Gobierno Digital habilitador Seguridad y Privacidad de la información (Temas: IPV6, Sensibilización. MSPI,)	Jefe OTSI.Oficina Asesora de Planeación.	Oficial de Seguridad.Dependencias.Contratista Gobierno Digital .Centro de servicios.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	Registro / Soporte	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Inventario del estado de las licencias y soporte de TIC, para garantizar la continuidad del soporte, actualización y mantenimiento de las herramientas, plataformas, licencias, servicios y sistemas de información que hacen parte de la infraestructura tecnológica de la entidad	Jefe OTSI.	Dependencias.Centro de servicios.Coordinador de plataforma TI.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Recolección evidencia MRAE Habilitador Seguridad y Privacidad de la Información	Jefe OTSI.	Oficial de Seguridad.Dependencias.Arquitecto Empresarial.Contratista Gobierno Digital .Centro de servicios.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Liderazgo de seguridad de la información	9	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Recolección evidencia cumplimiento Manual Gobierno Digital (Habilitador Seguridad y Privacidad de la información)	Jefe OTSI.	Oficial de Seguridad.Dependencias.Arquitecto Empresarial.Contratista Gobierno Digital .Centro de servicios.												

5.3.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el	Implementación de controles	1	Actualizar controles de seguridad de la información	* Informe semestral de la implementación de la herramienta de prevención de fuga de información (DLP) de Trellix	Especialista Seguridad informática OTSI.	Centro de servicios.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
entorno y las tecnologías.																		
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	1	Actualizar controles de seguridad de la información	*Anexo 2. Clasificación de las Políticas de seguridad actualizado con la coherencia de las políticas definidas en el Manual Operativo de SI con respecto a los controles definidos en la norma ISO 27001:2013 e ISO 27001:2022	Jefe OTSI.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	1	Actualizar controles de seguridad de la información	*Declaración de aplicabilidad (SOA) ISO 27002:2013 (Semestral)	Jefe OTSI.Oficial de Seguridad.	Oficina Asesora de Planeación.Delegado Web OTSI.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	1	Actualizar controles de seguridad de la información	*Documento Diagnostico ISO 27002:2022 actualizado (Semestral)	Jefe OTSI.	Oficial de Seguridad.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	1	Actualizar controles de seguridad de la información	*Revisión controles en base de datos	Oficial de Seguridad.	Grupo Soporte a usuarios OTSI.Administrador de base de datos.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	1	Actualizar controles de seguridad de la información	*Plan de mejoramiento redes sociales de la OAC	Oficina Asesora de Comunicaciones.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	1	Actualizar controles de seguridad de la información	*Diseño de la Estructura de la DMZ	Especialista Seguridad informática OTSI.	Oficial de Seguridad.Dependencias.Grupo Sistemas de Información OTSI.Administrador de base de datos.Centro de servicios.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los	Implementación de controles	2	Monitoreo primera línea de defensa	*Realizar el monitoreo (cuatrimestral) de los riesgos de seguridad de la información	Jefe OTSI.Oficial de Seguridad.	Oficial de Seguridad.Dependencias.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
cambios que se produzcan en el entorno y las tecnologías.																		
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	2	Monitoreo primera línea de defensa	*Revisión medidas de seguridad en bases de datos personales SGTH	Subdirección de Gestión del Talento Humano.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	2	Monitoreo primera línea de defensa	*Revisión medidas de seguridad en bases de datos personales SCT	Dependencias.	Oficial de Seguridad.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	3	Realizar el reporte de los Indicadores de seguridad de la información	*Análisis cuatrimestral del indicador GSI-03 Porcentaje de avance en la implementación de controles de seguridad de la información que mide los controles incluidos en la matriz integral de riesgos en los sistemas, aplicativos y portales incluidos en el catálogo de sistemas e información	Jefe OTSI.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	4	Monitoreo segunda línea de defensa	* Enviar recordatorio sobre la importancia del monitoreo de primera línea de defensa de los riesgos de seguridad de la información, para asegurar que los líderes técnicos y/o administradores funcionales de los sistemas de información realicen el reporte cuatrimestral sobre el estado de implementación de los controles de seguridad en los sistemas de información.	Oficial de Seguridad.	Dependencias.													
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	4	Monitoreo segunda línea de defensa	*Estructurar Plan de análisis de vulnerabilidades	Jefe OTSI.Oficial de Seguridad.Especialista Seguridad informática OTSI.	Dependencias.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	4	Monitoreo segunda línea de defensa	*Seguimiento semestral a los análisis de vulnerabilidades	Oficial de Seguridad.Especialista Seguridad informática OTSI.	Dependencias.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y	Gestión de riesgo	5	Actualizar el diagnostico del Anexo de Seguridad Digital en la resolución 1519 de 2020	*Mesas de trabajo para la alineación del M-TI-01 , Anexo de Seguridad Digital en la resolución 1519 de 2020 actualizado para los sistemas, aplicativos y portales incluidos en el catálogo de sistemas e información y la Matriz Integral de Riesgos	Oficial de Seguridad.	Grupo Sistemas de Información OTSI.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
adaptada a los cambios que se produzcan en el entorno y las tecnologías.																		
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de riesgo	5	Actualizar el diagnostico del Anexo de Seguridad Digital en la resolución 1519 de 2020	*Diagnostico del Anexo de Seguridad Digital en la resolución 1519 de 2020 actualizado para los sistemas, aplicativos y portales incluidos en el catálogo de sistemas e información	Oficial de Seguridad.	Dependencias.Grupo Sistemas de Información OTSI.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de riesgo	6	Realizar ejercicios de ingeniera social	* Diseño, ejecución e Informe de ejercicios de ingeniera social	Jefe OTSI.Especialista Seguridad informática OTSI.	Oficial de Seguridad.Centro de servicios.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	7	Documentar lecciones aprendidas Traslado data center	*Informe semestral de la gestión de las lecciones aprendidas Traslado data center	Jefe OTSI.Oficial de Seguridad.Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Especialista Seguridad informática OTSI.	Centro de servicios.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	8	Actualizar los documentos del componente de seguridad de la información	* Informe con la relación de los documentos actualizados de la plataforma de seguridad perimetral (catálogo de servicios, Hoja técnica de servicio, inventario (publicaciones, perfiles de navegación), mantenimientos, matriz de escalamiento, manuales, instructivos, planes de contingencia de FW, relación de backups, revisión de las obligaciones del centro de servicios respecto a seguridad perimetral, VPN, Sesiones de revisión con el Oficial de Seguridad de la Información),	Oficial de Seguridad.Especialista Seguridad informática OTSI.	Centro de servicios.													
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	8	Actualizar los documentos del componente de seguridad de la información	*Informe con la relación de los documentos actualizados de la plataforma del análisis de vulnerabilidades (catálogo de servicios, Hoja técnica de servicio, mantenimientos, matriz de escalamiento, manuales, instructivos, planes de contingencia de análisis de vulnerabilidades, inventario (licencias asignadas), relación de backups, revisión de las obligaciones del centro de servicios respecto a seguridad perimetral, Sesiones de revisión con el Oficial de Seguridad de la Información),	Oficial de Seguridad.Especialista Seguridad informática OTSI.	Centro de servicios.													
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones	Implementación de controles	8	Actualizar los documentos del componente de seguridad de la información	*Informe con la relación de los documentos actualizados del servicio de antivirus (catalogo de servicios, Hoja técnica, inventario, mantenimientos, matriz de escalamiento, manuales, instructivos)	Oficial de Seguridad.	Centro de servicios.													

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
legales vigentes aplicables a la utilización de la información digital.																		
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	8	Actualizar los documentos del componente de seguridad de la información	*Informe con la relación de los documentos actualizados del servicio de WAF/Balanceador (catalogo de servicios, Hoja técnica, inventario, mantenimientos, matriz de escalamiento, manuales, instructivos)	Especialista DRP OTSI.	Centro de servicios.												
OECS1: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital.	Implementación de controles	8	Actualizar los documentos del componente de seguridad de la información	*Informe con la relación de los documentos actualizados de la plataforma de O365 (catalogo de servicios, Hoja técnica, inventario, mantenimientos, matriz de escalamiento, manuales, instructivos, Sesiones de revisión con el Oficial de Seguridad de la Información), a más tardar el 30 de noviembre de 2025.	Especialista O365.	Centro de servicios.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de riesgo	9	Gestion de vulnerabilidades de SUCOP	* Pruebas funcionales y técnicas de la migración de SUCOP de SharePoint 2013 a 2019	Especialista SharePoint.Lideres Técnico y Funcional SUCOP.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de riesgo	9	Gestion de vulnerabilidades de SUCOP	* Reescaneo de vulnerabilidades a nivel servidor y aplicación	Especialista Seguridad informática OTSI.	Dependencias.Centro de servicios.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de riesgo	9	Gestion de vulnerabilidades de SUCOP	*Estructuracion del plan de remediación	Oficial de Seguridad.Especialista Seguridad informática OTSI.Especialista SharePoint.Lideres Técnico y Funcional SUCOP.	Dependencias.Centro de servicios.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Gestión de riesgo	9	Gestion de vulnerabilidades de SUCOP	*Mesas para seguimiento al Plan	Especialista Seguridad informática OTSI.Especialista SharePoint.Lideres Técnico y Funcional SUCOP.	Oficial de Seguridad.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	* Informe de identificación de herramientas, procedimientos de TI para dar cumplimiento de los tiempos de RTO y RPO de los sistemas de información, aplicativos y portales críticos de la Entidad	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	* Informe de pruebas de recuperación de cada una de los sistemas de información críticos	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Pruebas de recuperación de información y continuidad de los sistemas de información críticos en la vigencia evaluada	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Actualizar la documentación del diagnóstico e implementación de la continuidad del negocio en el componente tecnológico.	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	* Identificar herramientas y gestionar los procedimientos para la implementación del RTO y RPO del análisis de impacto de negocio para los sistemas de información, aplicativos y portales críticos que apoyan los procesos de la Entidad	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	* Almacenar las copias de respaldo en un lugar aislado, en un segmento diferente de red a la de servidores y equipos	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												
OECS2: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información	Implementación de controles	10	Realizar el reporte de avance en la mejora del FURAG en la política de seguridad digital (SDI)	*Actualizar el Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Dependencias.												
OECS4: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías.	Implementación de controles	11	Seguimiento ejecución APCM de Seguridad de la información	*Apoyar en la ejecución de APCM del Componente de seguridad de la Información	Dependencias.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Actualizar diagnóstico ISO 22301:2019	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Comunicaciones.Subdirección Administrativa y Relacionamiento con la Ciudadanía.Subdirección de Gestión del Talento Humano.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Formalización del plan de trabajo 2024 y Socialización de roles y responsabilidades a los líderes que componen la GCN	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Comunicaciones.Subdirección Administrativa y Relacionamiento con la Ciudadanía.Subdirección de Gestión del Talento Humano.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Actualizar el Manual del GCN	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Comunicaciones.Subdirección Administrativa y Relacionamiento con la Ciudadanía.Subdirección de Gestión del Talento Humano.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Levantamiento de lineamientos de monitoreo a la implementación, mantenimiento y pruebas del plan de continuidad del negocio	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Planeación.Oficina Asesora de Comunicaciones.Subdirección Administrativa y Relacionamiento con la Ciudadanía.Subdirección de Gestión del Talento Humano.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Actualización de los planes de emergencia	Subdirección de Gestión del Talento Humano.	Oficina Asesora de Planeación.Subdirección Administrativa y Relacionamiento con la Ciudadanía.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Evaluación a los riesgos orientados al GCN	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Comunicaciones.Subdirección Administrativa y Relacionamiento con la Ciudadanía.Subdirección de Gestión del Talento Humano.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Validación de los resultados obtenidos en la proforma de análisis del impacto del negocio - BIA	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.	Oficina Asesora de Planeación.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Validación y actualizar el listado de brigadistas inscritos y Actualización del listado de colaboradores por sede	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Dependencias.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Revisión equipos de prevención y atención de emergencias	Subdirección de Gestión del Talento Humano.	Oficina Asesora de Planeación.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Revisión rutas de evacuación (Edificio FONADE y otras sedes)	Subdirección de Gestión del Talento Humano.	Oficina Asesora de Planeación.Subdirección Administrativa y Relacionamiento con la Ciudadanía.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Seguimiento al cronograma de mantenimiento del edificio. (Depende del plan anual de mantenimiento del Edificio - PLANTAS ELECTRICAS, BOMBAS Y EYECTOR, SUBESTACIONES ELECTRICAS, ALARMAS Y CITOFONOS, ASCENSORES Y EXTINTORES).	Subdirección Administrativa y Relacionamiento con la Ciudadanía.	Oficina Asesora de Planeación.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Realizar la verificación de las instalaciones físicas de archivo y biblioteca ubicadas en los diferentes centros de trabajo del DNP	Subdirección Administrativa y Relacionamiento con la Ciudadanía.	Oficina Asesora de Planeación.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Realizar la verificación de las instalaciones físicas tercerizadas que presta servicios de servicio de depósito, custodia, organización, reprografía y conservación de los documentos de archivo al DNP	Subdirección Administrativa y Relacionamiento con la Ciudadanía.	Oficina Asesora de Planeación.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Charla de Gestión de Continuidad del negocio - Atención a Emergencias - Brigadistas y Equipo de Atención a Emergencias	Subdirección de Gestión del Talento Humano.	Oficina Asesora de Planeación.Dependencias.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Capacitación de gestión documental enfocada en el manejo de documentos de archivo en caso de siniestro y programa de prevención de emergencia y atención de desastres para archivo del Sistema Integrado de Conservación	Subdirección Administrativa y Relacionamiento con la Ciudadanía.	Oficina Asesora de Planeación.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Envió material de sensibilización GCN (Maillings, videos, presentaciones, etc.)	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficial de Seguridad.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Prueba de acceso remoto CCA	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Planeación.Dependencias.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Diseñar de la prueba de ciberseguridad	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficina Asesora de Planeación.Dependencias.Centro de servicios.												

Departamento Nacional de Planeación	PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2025	Versión 1.0 20-01-2025

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Simulacro de Evacuación edificio FONADE	Subdirección de Gestión del Talento Humano.	Oficina Asesora de Planeación.												
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Simulacro de rescate de documentos de archivos (Edificio PATRIA piso 7 y Edifico FONADE piso 5)	Subdirección Administrativa y Relacionamiento con la Ciudadanía.	Oficina Asesora de Planeación.												

OBJETIVO SGSI o GCN	ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	CONSECUTIVO	ACTIVIDAD EN EL PLAN	ENTREGABLE	Responsable Principal	Responsable Apoyo	Seguimiento											
							Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
GCN: Implementar el componente de la Gestión de Continuidad del Negocio (GCN) para el Departamento Nacional de Planeación DNP con el fin de evaluar y sostener en niveles previamente definidos y aceptados en las operaciones y servicios de la Oficina de Tecnología y Sistemas de Información para el DNP y sus partes interesadas los cuales deben ser desarrollados, probados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.	Gestión de riesgo	12	Gestionar la continuidad de negocio	*Presentación del resultado de la GCN al CIGD 2025	Especialistas Continuidad de negocio OTSI.Especialista DRP OTSI.Oficina Asesora de Planeación.	Oficial de Seguridad.												

5.4. Análisis Presupuestal

Las adquisiciones de seguridad de la información que se requieran se gestionan a través del plan anual de adquisiciones disponible en https://www.dnp.gov.co/LaEntidad_/secretaria-general/Subdireccion-contratacion/contratacion/Paginas/plananual-de-adquisiciones.aspx y el proyecto de inversión "Fortalecimiento de las tic para el cumplimiento de los objetivos del DNP a nivel Nacional"

6. CONTROL DE VERSIONES

Los planes de tratamiento de riesgos de seguridad y privacidad de la información, así como el plan de seguridad y privacidad de la información en los que se basa este documento, fueron presentados para la consideración y revisión de la alta dirección y el comité de gestión y desempeño institucional, con el objetivo de ser aprobados y aplicados de acuerdo con lo aquí establecido.

Elaboró:

Sandra Fernanda Poveda Oficial de Seguridad de la información.
17 de enero de 2025
Versión 0

Revisó:
Orlando Benavides Santacruz
Jefe Oficina de Tecnología y sistemas de la información
20 de enero de 2025
Versión 1.0

Oficina Asesora de planeación

Soporte: Correo Formulación planes especiales 2025 - Decreto 612 del 2018 enviado a Sistema Gestion de Calidad gpcalidad@dnp.gov.co
21 de enero de 2025

Aprobó:
Comité institucional de Gestión y Desempeño
31 enero 2025