Agencia Nacional Digital

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -SEGURIDAD DIGITAL

BOGOTÁ, ENERODE 2025

CONTENIDO

1. INTRODUCCIÓN

La Corporación Agencia Nacional de Gobierno Digital —AND—, mediante la Resolución 35 de 2023, " *Por la cual se integra y se establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Corporación Agencia Nacional Digital*", en su artículo tercero, entre las funciones, se encuentra en el ítem 6, "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información". Igualmente la normatividad vigente mediante 1083 de 2015 en su el artículo 2.2.22.2.1 menciona; Las Políticas de Gestión y Desempeño Institucional se regirán por las normas que las regulan o reglamentan y se implementarán a través de planes, programas, proyectos, metodologías y estrategias, Además el Decreto 1008 de 2018 en el artículo 2.2.9.1.1.3. menciona Principios; Define la seguridad de la información como principio que 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, de igual manera el Decreto 767 de 2022 en el artículo 2.2.9.1.2.1 define la estructura a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. Así mismo, el numeral 3.2 del mismo artículo define la Seguridad y Privacidad de la Información como habilitador que busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos; en el mismo sentido el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (…)Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.(…). En cumplimiento de este Decreto se emite la Resolución 500 de 2021 , expedida por el MinTIC, estableció los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del modelo de seguridad y privacidad -MSPI con la adopción de mejores prácticas basada en el estándar ISO/IEC 27001:2022[1] Seguridad de la información, ciberseguridad y protección de la intimidad . Sistemas de gestión de la seguridad de la información . Requisitos, como habilitador de la política de Gobierno Digital. En consecuencia, la seguridad y privacidad de la información, y el Modelo de Seguridad y Privacidad de la Información son adoptadas en la Corporación Agencia Nacional de Gobierno Digital —AND—.

[1] https://www.iso.org/es/contents/data/standard/08/28/82875.html

2. OBJETIVO GENERAL

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC, estándar ISO/IEC 27001:2022 y la Política pública de Seguridad Digital, que permitan mantener la seguridad y privacidad de la información que circula en los procesos de la Corporación Agencia Nacional de Gobierno Digital —AND—.

2.1. OBJETIVOS ESPECIFICOS

- ✓ Establecer las principales líneas de actuación a seguir en el corto y mediano plazo para la implementación y mantenimiento del SGSI, con acciones durante el diagnóstico, planificación, operación, evaluación y mejoramiento del Modelo de Seguridad y Privacidad - MSPI en cuanto al cumplimiento como entidad de diseñar, implantar y mantener actualizada la seguridad digital a partir de los activos a proteger y de los riesgos a que están sometidos.
- ✓ Promover una cultura de seguridad y privacidad de la información para los empleados de planta y contratistas, con el fin de proteger adecuadamente los activos de información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y cumplir con las regulaciones y estándares pertinentes en relación a las medidas de seguridad digital a partir de la construcción de estrategias de comunicación y sensibilización que divulguen las directrices, políticas y beneficios de la Seguridad Digital en la AND.
- ✓ Detectar, informar, evaluar, responder, minimizar, aprender y resolver incidentes de seguridad de la información con el propósito de realizar una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.
- ✓ Identificar y gestionar activos de seguridad digital y de la información para los procesos de la AND, como ejercicio fundamental para la gestión de Riesgos de Seguridad Digital, así como la valoración e implementación de controles con el fin de incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la Entidad.
- ✓ Establecer los principios y lineamientos que deben regir el tratamiento de los datos personales dentro la Corporación Agencia Nacional Digital- AND. Esto incluye la recolección, almacenamiento, uso, divulgación y disposición de los datos personales, asegurando que se realicen de manera legal, transparente, y respetando los derechos de los titulares de los datos enmarcados en la Seguridad Digital

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Corporación Agencia Nacional de Gobierno Digital —AND—, comprende la implementación del Modelo de Seguridad y Privacidad de la Información, aplicable a los dieciocho (18) procesos institucionales. Así mismo aplica para todos los usuarios internos, externos,

proveedores y a la ciudadanía en general, que en cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien o consulten la información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. En conformidad con la normatividad vigente y el estándar ISO2701:2022.

4. MARCO CONCEPTUAL

El Sistema de Gestión de Seguridad de la Información hace parte del Sistema Integrado de Gestión de la Corporación Agencia Nacional de Gobierno Digital —AND, por lo tanto, los documentos procesos y procedimientos resultantes de la implementación de controles, que son adoptados y formalizados en este último.

Por los anterior la AND ha adoptado el MSPI como guía para la construcción del Subsistema de Gestión de Seguridad de la Información (SGSI), este modelo está basado en el Marco de Referencia de Arquitectura TI el cual fue propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en soporte de la Política de Gobierno Digital, para la gestión de Sistema de Gestión de Seguridad de la Información se realizará en la plataforma tecnológica que la Entidad dispone para tal f in, en la cual se consolidará los resultados de la ejecución del Modelo de Seguridad y Privacidad de la Información – MSPI definido por el MinTIC, contempla su operación basándose en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades públicas puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, se abordan las siguientes fases:

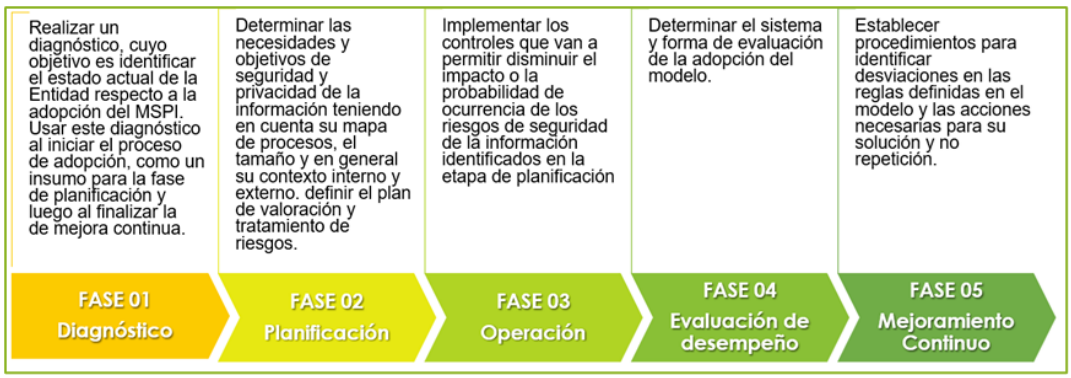

Ilustración 1 Fases MSPI - MinTIC

Igualmente se debe contemplar los cambios del estándar vigente la ISO/IEC 27001:2022 que contiene los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el

contexto de la organización y la ISO/IEC 27002:2022 que proporciona un conjunto de referencia de controles genéricos de seguridad de la información.

5. ALINEACIÓN A POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON LAS POLÍTICAS DE USO DE LA INFORMACIÓN Y DATOS PERSONALES.

La Corporación Agencia Nacional de Gobierno Digital —AND—, por medio de su Política de Seguridad y Privacidad de la Información que tiene por objeto definir los lineamientos para preservar la integridad, disponibilidad y confidencialidad de la información de la AND, a través del Sistema de Gestión de Seguridad de la (SGSI–PDP), implementando acciones de aseguramiento, conforme al cumplimiento de los requisitos legales, estratégicos, operativos, tecnológicos y tácticos, aplicando las buenas prácticas de seguridad de la información fundamentadas en el estándar ISO/IEC 27001, en el contexto de direccionamiento estratégico y gestión del riesgo de la Corporación Agencia Nacional de Gobierno Digital —AND—. Comprometiendo la participación de empleados de planta, contratistas y terceros en lograr el nivel de cumplimiento adecuado de los lineamientos y requisitos de seguridad de la información (tendrán la responsabilidad de divulgar y sensibilizar las políticas y procedimientos de seguridad y privacidad de la información). Así mismo la política y lineamientos expuestos en el "Manual de normas y políticas de seguridad y privacidad de la información", son de obligatorio cumplimiento para los empleados de planta y contratistas de la entidad. En el caso de cualquier sugerencia de cambio o normatividad actualizada se tramitará a través del profesional se seguridad de la información de la AND, quien se encargará de realizar el cambio y socialización en la Entidad.

La AND, está comprometida en garantizar el tratamiento de los datos personales, por lo cual se acoge a las disposiciones contenidas en la Ley 1581 de 2012 y la Política de Tratamiento de Datos Personales-AND, que tiene por objetivo establecer los criterios bajo los cuales se recolectan, almacenan, usan, circulan y suprimen los datos personales tratados por la Corporación Agencia Nacional de Gobierno Digital —AND, así como el procedimiento para la garantía de los derechos de los titulares de los datos personales.

6. GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Respecto a los resultados del MSPI del año 2024, se encontró que para la vigencia 2025 es necesario atender las siguientes recomendaciones:

- ✓ Fortalecer participación en la mejora de las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del de seguridad digital convocadas por la AND.

- ✓ Adelantar acciones para la gestión sistemática de los riesgos de seguridad digital en la entidad tales como gestión de vulnerabilidades.
- ✓ Adelantar acciones para la gestión de la continuidad de los servicios de infraestructura tecnológica.
- ✓ Comprometer la seguridad de la información para la gestión de incidentes y/o eventos e incluir los de datos personales.
- ✓ Realizar la implementación de la gestión de riesgos de seguridad digital en la AND con la aplicación de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas de su versión vigente.

Adicionalmente, en el análisis de brechas del Modelo de Seguridad y Privacidad de la Información – MSPI realizado en 2024, se obtuvo el 78% con el ejercicio de linealidad con el estándar ISO 27002:2022.

Ilustración 2 autoevaluación MSPI Producto tipo MinTIC

De la gráfica anterior, se identifican aspectos por mejorar en los siguientes controles de seguridad de la información.

ITEM	DESCRIPCION	Control ISO 27002: 2013 / 27002: 2022
SEGURIDAD DE LAS OPERACIONES	Elaborar y aplicar la documentación sociedad al proceso de Gestión de TI en relación a los Controles tecnológicos: Gestión de la capacidad Gestión de vulnerabilidades técnicas Copia de seguridad de la información Separación de los entornos de desarrollo, prueba y producción Gestión de cambios	A.12.1.2 A.12.1.3 A.12.1.4 A.12.3.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.5.1 A.12.6.1 A.12.6.2 / 8.6 -8.8- 8.13-8.15- 8.17- 8.19- 8.31- 8.32
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA	Elaborar Plan de continuidad del negocio que deben desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos comerciales	A. 17.1.1 - 17.1.2 17.1.3 5.29 - 8.14

ITEM	DESCRIPCION	Control ISO 27002: 2013 / 27002: 2022
CONTINUIDAD DEL NEGOCIO	críticos luego de una interrupción o falla. La seguridad de la información debe restaurarse al nivel requerido y en los plazos requeridos. Así mismo se debe actualizar el análisis de impacto empresarial (BIA), elaborar e implementar el plan de pruebas de restauración.	
SEGURIDAD DE LAS COMUNICACIONES	Se deben implementar controles para garantizar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado. En particular, se deben considerar documentar Seguridad de redes, Seguridad de los servicios de red y Segregación de redes, adicionalmente las políticas de navegación de la Entidad.	A 13.2.1- 13.2.2 -13.2.3-13.2.4-13.1.1 -13.1.2-13.1.3 5.14-6.6-8.20-8.218.22
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Fortalecer el desarrollo seguro que es un requisito para crear un servicio, una arquitectura, un software y un sistema seguro con la solicitud de Pruebas de seguridad en desarrollo y aceptación, así los diagramas de arquitecturas de los sistemas de información internos y externos documentados , así como las integraciones de bases de datos para su protección.	A 14.2.1 -14.1.2, 14.1.3 -14.2.5 -14.2.8 -14.2.9-14.2.714.3.1 8.25-8.26-8.27-8.29-8.30-8.33
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Ajustar el procedimiento de gestión de Incidentes para la AND del proceso de Gestión de TI e incluir los incidente y eventos de seguridad Digital.	A16.1.1 A16.1.4 A16.1.5 A16.1.6 A16.1.7 A16.1.2 A16.1.3 / 5.24 -5.25 -5.26-5.27 -5.28-6.8

Tabla 1 Controles ISO27002:2022 a mejorar

6.1. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Corporación Agencia Nacional de Gobierno Digital —AND—, realizó diversas actividades orientadas a la implementación y fortalecimiento del Sistema Integrado de Gestión en la Entidad.

El modelo de operación actual de la AND se encuentra orientado mediante la gestión de procesos, y se representan en la siguiente ilustración la posición del Proceso Estratégico de Seguridad y privacidad de la información que debe definir e implementar lineamientos, estrategias y actividades orientadas a la seguridad y privacidad de la información conforme a la normatividad aplicable, así como proteger la disponibilidad, integridad y confidencialidad de los activos de información en la AND, a través de la gestión de riesgos de segundad y privacidad de la información y la implementación de políticas, procedimientos y controles necesarios y suficientes,

de manera que se puedan prevenir y gestionar los incidentes de seguridad de la información y violaciones de privacidad contribuyendo al cumplimiento de la misión institucional y los objetivos estratégicos

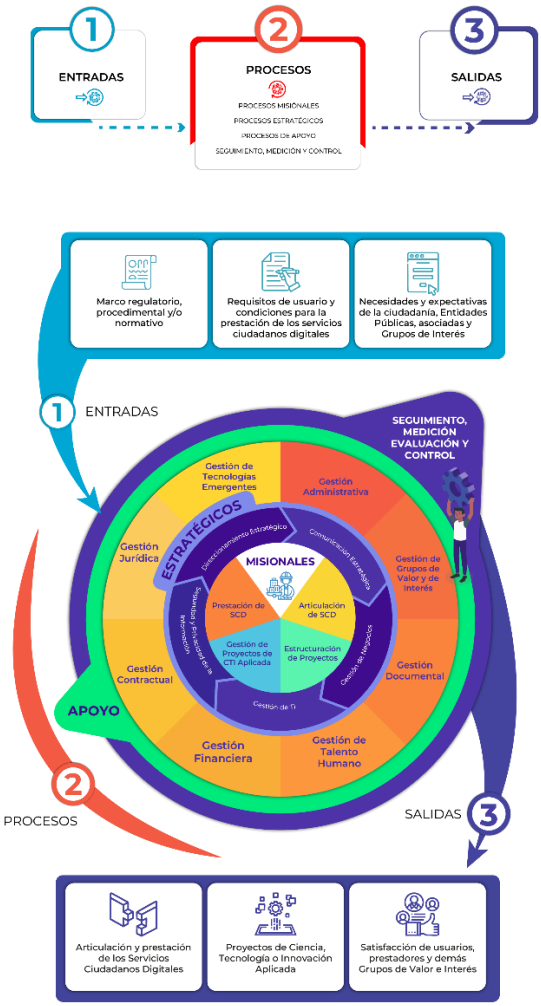

Ilustración 3 Procesos AND

6.2. SENSIBILIZACIÓN Y CONCIENTIZACIÓN

Desarrollo de estrategias de sensibilización y formación en Seguridad de la Información que permiten involucrar a todos los actores que forman parte de la implementación del SGSI, a través de la creación de conciencia y entendimiento de estos, enmarcadas en diferentes temáticas de seguridad de la información, dando cumplimiento al control 6.3 de la Norma ISO 27002:2022 "Concientización, educación y capacitación en seguridad de la información". El diseño y desarrollo de la estrategia de sensibilización, tiene como objetivo aportar en el desarrollo de las actividades que

giran alrededor de la formación de competencias en los colaboradores de la AND, que les sirva de base en la toma de decisiones acertadas y bien informadas sobre los temas de seguridad de la información, sus actuaciones y responsabilidades que se generen.

6.3. INDICADORES

De acuerdo con el Manual de Gobierno Digital, se realiza el seguimiento de la eficacia de la implementación del Modelo de Seguridad y Privacidad de la Información, adicionalmente se adoptarán mecanismos de medición de eficacia en la implementación de controles contenidos en la declaratoria de aplicabilidad y de la efectividad de estos.

7. MEDICIÓN

Tipo de indicador: Cumplimiento
Nombre: Avance plan de seguridad
Formula: (No. de actividades ejecutadas / No. Actividades programadas) * 100
Meta: 90% Fuente de información: Plan de seguridad y privacidad de la información

8. CRONOGRAMA

El Plan de implementación de Seguridad y Privacidad de la Información, para la aplicación del habilitador de seguridad de la información de la política de Gobierno Digital, se proyecta con el fin de proteger y preservar la integridad, disponibilidad y confidencialidad de la información de la AND y se ejecuta de acuerdo con el siguiente cronograma, al cual se le hace seguimiento por parte de oficial de Seguridad de información y el Plan de Acción.

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
DIAGNOSTICO MSPI	Actualizar el documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad	01-01-2025	30-12-2025	Documento autodiagnóstico de MSPI actualizado semestralmente	Profesional de seguridad de la Información
PLANIFICACION SDI	Actualizar el Plan de Seguridad y Privacidad de la Información con su respectivo Alcance MSPI, asociadas a la seguridad Digital	15-12-2024	30-01-2025	Documento Plan de Seguridad y Privacidad de la Información – Seguridad Digital 2025	Profesional de seguridad de la Información
	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	15-12-2024	30-01-2025	Documento Plan de Tratamiento de Riesgos de Seguridad y	Profesional de seguridad de la Información

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
				Privacidad de la Información- Seguridad Digital 2025	
	Definir una metodología de pruebas de efectividad	01-04-2025	30-05-2025	Documento guía metodología de pruebas de efectividad AND Infraestructura tecnológica	Profesional de seguridad de la Información/Profesional de Gestión de TI
	Revisión anual de la Política de seguridad y privacidad de la información.	15-12-2024	30-01-2025	Acta de revisión de la política de seguridad y privacidad de la información y/o Resolución de actualización	Profesional de seguridad de la Información
	Actualizar el Análisis de Impacto de la Operación.	1-04-2025	30-05-2025	Documento Actualizado del Análisis de Impacto del Negocio BIA	Profesional de seguridad de la Información/Profesional de Gestión TI
	Actualizar la gestión de Continuidad del Negocio de AND	1-04-2025	30-06-2025	Documento Actualizado Plan de Continuidad del Negocio de AND alineado al proceso de gestión e la tecnología	Profesional de seguridad de la Información/Profesional de Gestión de TI
	Definir el Plan de pruebas de la infraestructura tecnológica	1-01-2024	30-03-2025	Documento Plan de pruebas de restauración de la infraestructura tecnológica	Profesional de seguridad de la Información/Profesional de Gestión de TI
OPERACION SDI	Realizar la Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	30-01-2025	15-03-2025	Actualizar la Mapa de Riesgos Sistema Seguridad de la Información	Profesional de seguridad de la Información/ Todas las Áreas
	Elaborar un de Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y Estado de implementación .	1-03-2025	30-04-2025	Documento Plan de implementación de controles de seguridad y privacidad de la información	Profesional de seguridad de la Información

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	Identificar nuevos activos de información en cada dependencia en el Levantamiento Activos de Información con alcance a los procesos modificados en el 2024	20-02-2025	20-04-2025	Matriz actualizada Identificación y clasificación de activos de información	Profesional de seguridad de la Información/ Todos los procesos
	Envío del consolidado de activos de seguridad digital a la gestión Documental , para el respectivo reporte del índice de información clasificada y reservada y de Publicación de activos de la información AND	25-05-2025	30-06-2025	Entrega de Matriz actualizada Identificación y clasificación de activos de información	Profesional de seguridad de la Información/ Gestión Documental
	Recolectar bases de datos, bases de datos personales de acuerdo con los estándares emitidos por la Superintendencia de Industria y Comercio	30-01-2025	30-03-2025	Matriz de bases de datos personales de para reportar	Oficina Asesora de jurídica
	Registrar y actualizar de las bases de datos Gestión de datos personales ante la Superintendencia de Industria y Comercio	01-04-2025	31-12-2025	Soporte de registro de actualización de las bases de datos personales de para reportar la AND	Oficina Asesora de jurídica
	Elaborar e incluir avisos de la privacidad que contenga el lenguaje mínimo señalado en la ley 1581 de 2012 y decreto 1377 de 2013.	30-01-2025	30-06-2025	Generar y entregar los Avisos de la privacidad de datos personales para los diferentes aplicativos, formularios y donde requiera a aceptación de tratamiento de datos	Oficina Asesora de jurídica
	Actualizar el proceso de gestión de la tecnología en la seguridad de las comunicaciones	01-02-2025	30-04-2025	Documentar en la gestión de Redes en AND que incluya (Seguridad de redes, Seguridad de los servicios de red y Segregación de redes,	Profesional de Gestión de TI

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
				adicionalmente las políticas de navegación de la Entidad)	
	Elaborar Documentación del proceso de gestión de la tecnología en la seguridad de eliminación de la Información	01-03-2025	30-07-2025	Documento Instructivo de borrado de la información sobre sistemas, aplicaciones y servicios, que no debe conservarse más tiempo del necesario para reducir el riesgo de divulgación no deseada	Profesional de Gestión de TI
EVALUACIÓN Y DESEMPEÑO SDI	Seguimiento de indicadores de SDI	30-09-2025	31-12-2025	Reportar el Monitoreo y seguimiento de indicadores de SDI	Planeación AND / Profesional de seguridad de la Información
	Elaborar reporte ejecución y Seguimiento de Plan de implementación de controles de seguridad y privacidad de la información	30-09-2025	31-12-2025	Reporte de gestión de Plan de implementación de controles de seguridad y privacidad de la información – Seguridad Digital	Planeación AND / Profesional de seguridad de la Información
	Elaborar los informes de Seguimiento de riesgos de Seguridad de la Información – Seguridad Digital	30-04-2025	31-12-2025	Informe cuatrimestral de Riesgos de seguridad de la Información – Seguridad Digital	Planeación AND Profesional de seguridad de Información
	Elaborar reporte de gestión de incidentes de Seguridad de la Información – Seguridad Digital y Datos personales	30-09-2025	31-12-2025	Reporte de gestión de incidentes de Seguridad Digital y de la Información/ Datos personales	Planeación AND Profesional de seguridad de Información
	Actualizar el Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos	30-09-2025	31-12-2025	Documento Reporte de matriz de control de controles	Planeación AND Profesional de seguridad de Información

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	Evaluación de Plan de Continuidad de La Operación	30-09-2025	31-12-2025	Realizar Informe de cumplimiento del Plan de Continuidad del negocio	Profesional de seguridad Información/ Profesional Gestión TI
	Realizar las acciones del Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, con seguimiento de Control Interno	01-03-2025	31-12-2025	Ejecución de Planes de mejora SDI programados	Profesional de seguridad de Información Planeación Control Interno
	Reporte de cumplimento de Plan Sensibilización de Seguridad y Privacidad de la Información y Datos Personales	01-12-2025	31-12-2025	Documento de reporte de la vigencia de cumplimiento de Plan Sensibilización de Seguridad y Privacidad de la Información y Datos Personales	Profesional de seguridad de Información Profesional de Gestión de TI Planeación
MEJORAMIENTO CONTINUO SDI	Medir el cumplimiento Plan de Seguridad y Privacidad de la Información – Seguridad Digital 2025	01-02-2025	31-12-2025	Talero de control y/o cronograma de cumplimiento con el avance Plan de Seguridad y Privacidad de la Información – Seguridad Digital 2025	Profesional de seguridad de Información Profesional de Gestión de TI Planeación
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos	01-02-2025	31-12-2025	Informe de cumplimiento de acciones preventivas y correctivas de los planes de mejora propuestos de seguridad de la información – Seguridad Digital	Profesional de seguridad de Información Planeación Control Interno

Tabla 2 Plan SYPI Cronograma

9. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	CAMBIOS
1	30-01-2025	Emisión del documento con actividades para la vigencia 2025 en el cumplimiento de Decreto 612 de 2018 y alineación con la norma ISO 27001:2022

Revisó y aprobó: Comité Institucional de Gestión y Desempeño de la Corporación Agencia Nacional Digital, sesión del 28 de enero de 2025.

Elaboró: Catherine Suarez Rodriguez; Profesional de seguridad de la información