Unidad para las Víctimas

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2023-2026

UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

Oficina de Tecnologías de la Información
2025

Dirección: Carrera 85D No. 46A-65 Bogotá, Colombia
Conmutador: +57 (601) 796 5150
Línea Gratuita: (+57) 01 8000 911119

Unidad para las Víctimas

Control de Versiones

Versión	Fecha	Modificación
1.0	16/01/2023	Versión inicial del documento
2.0	22/01/2024	Actualización
3.0	30/01/2025	Actualización para la vigencia 2025, teniendo en cuenta el banco de iniciativas de Arquitectura Empresarial actualizado a 12/12/2024 y los resultados de la ejecución de los proyectos de Ciberseguridad 360 y SOC. Inclusión del numeral 7.Análisis Presupuestal

Unidad para las Víctimas

Tabla de contenido

Unidad para las Víctimas

Plan de Seguridad y Privacidad de la Información & Portafolio de Proyectos

1. Objetivo

Proteger la información y sistemas de información de la Unidad para la Atención y Reparación Integral de las Víctimas, a través de la implementación y/o fortalecimiento de controles de aseguramiento en el marco de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2026.

1.1 Objetivos Estratégicos (OE)

El Plan Estratégico de Seguridad y Privacidad de la Información, contempla como base los objetivos del Sistema de Gestión de Seguridad de la Información, establecidos por la Entidad, los cuales se listan a continuación:

A. Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.
B. Implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad.
C. Realizar seguimiento a los eventos e incidentes de seguridad para obtener lecciones aprendidas y mejorar periódicamente el sistema de gestión de Seguridad de la Información.
D. Promover, mantener y establecer la cultura de seguridad de la información en la Unidad para las Víctimas y partes interesadas.
E. Incrementar la disponibilidad de servicios de TI y de operación, a través del plan de continuidad de negocio.

F. Suministrar información confiable, íntegra, oportuna, accesible y de valor a la población Víctima.

2. Alcance

El Plan Estratégico de Seguridad de la Información involucra la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información estableciendo la estrategia de seguridad digital de la entidad, en el marco del alcance definido en la Política General de Seguridad de la Información e incluye la implementación de controles relacionados con la confidencialidad, integridad, privacidad y disponibilidad de la información, en un escenario de corresponsabilidad con los procesos y Direcciones Territoriales de la Unidad para la Atención y Reparación Integral a las Víctimas.

3. Documentos de Referencia

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Ley 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales"*
- Ley 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*
- Decreto único reglamentario 1078 de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*", el cual mediante el título 9, capítulo 1 establece la política de gobierno digital.
- Decreto único reglamentario 1083 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"*
- Decreto 612 de 2018, "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de*

las entidades del Estado", donde se encuentra el Plan de Seguridad y Privacidad de la Información incluido en el presente Plan Estratégico de Seguridad de la Información (PESI).

- Resolución 500 de 2021 del MinTIC, "*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 2022 del MinTIC, *"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 número 500 de 2021"*
- Resolución 3157 de 2021 de la UARIV, "*Por la cual se establecen los Objetivos, Política General y Políticas Específicas del Sistema de Gestión de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas y se deroga la Resolución No 740 del 11 de noviembre de 2014*".
- Manual de Gobierno Digital – MINTIC.
- Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4 de 2021
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Lineamiento de Seguridad y canal de comunicaciones Microsoft Teams, versión 1 del 18-10-2024, Código:140,06,04-9.
- Lineamiento de Continuidad de Negocio, versión 1 del 25/10/2024, Código: 140,06,04-10.
- Lineamiento de Tecnologías de la Información, versión 1 del 02/12/2024, Código: 140,06,04-12, el cual incluye el Dominio de Seguridad de la Información.
- Guía para la Gestión ante el Incumplimiento de las Políticas de Seguridad de la Información, versión 1 del 25/10/2024, Código: 140,06,04-11

4. Estado actual de la Entidad respecto al Sistema de Gestión de Seguridad de la Información

La Unidad para la Atención y Reparación Integral a las Víctimas, ha avanzado en la implementación del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de las Tecnologías de la Información y las Comunicaciones a través de la ejecución del Plan Estratégico de Seguridad de la Información que durante los años 2023 y 2024 ha consolidado las actividades de operación y portafolio de proyectos relacionados con la Seguridad de la Información. A continuación, se presenta el resultado del diagnóstico de evaluación de controles realizado a través del instrumento dispuesto por el MinTIC a corte 2024:

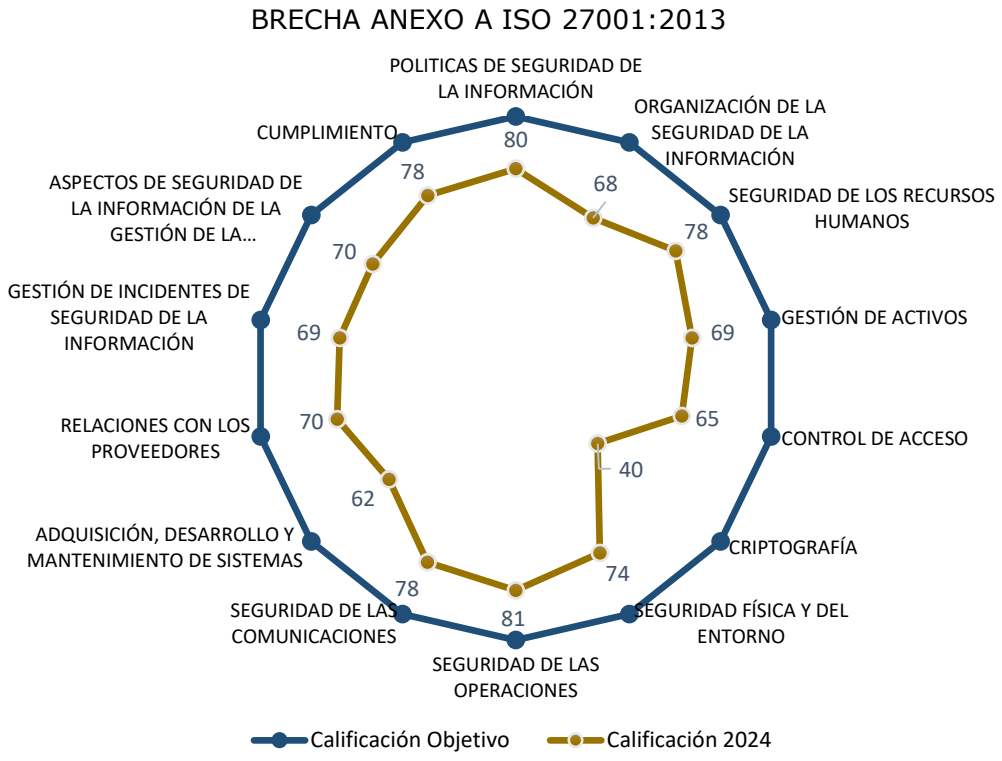


Gráfico 1: Evaluación de efectividad de controles - ISO 27001:2013 Anexo A – Instrumento MSPI del MinTIC

Es importante indicar que, el instrumento para el diagnóstico de la implementación del Modelo de Seguridad y Privacidad de la Información que actualmente dispone el MinTIC tiene como base la Norma NTC ISO/IEC 27001:2013 aunque esta norma fue actualizada en el año 2022.

Teniendo en cuenta lo anterior, el promedio de la medición de evaluación a corte 2024, asciende a 70%.

El mencionado Instrumento del MinTIC, permite identificar la calificación de la Entidad respecto al Modelo Framework de Ciberseguridad NIST, con el siguiente resultado a corte 2024:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
ÍTEM	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	75	100
DETECTAR	76	100
RESPONDER	72	100
RECUPERAR	53	100
PROTEGER	75	100
PROMEDIO CALIFICACIÓN	**70**	**100**

Tabla 1: Calificación Ciberseguridad NIST – Instrumento MSPI del MinTIC diligenciado a corte 2024

Adicional a lo anterior, la Unidad para la Atención y Reparación Integral a las Víctimas ha obtenido los siguientes resultados a través de la medición del indicador "Política Seguridad digital", realizado por el Departamento Administrativo de la Función Pública, a través del FURAG.

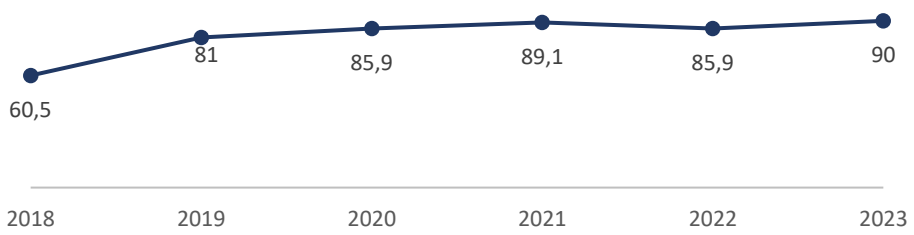


Gráfico 2: Fuente: Departamento Administrativo de la Función Pública. Medición de la política de Seguridad Digital - FURAG

Por otra parte, la medición del indicador de Seguridad y Privacidad de la Información de la política de Gobierno Digital tiene el siguiente comportamiento:

Indicador Gobierno digital: Seguridad y Privacidad de la Información

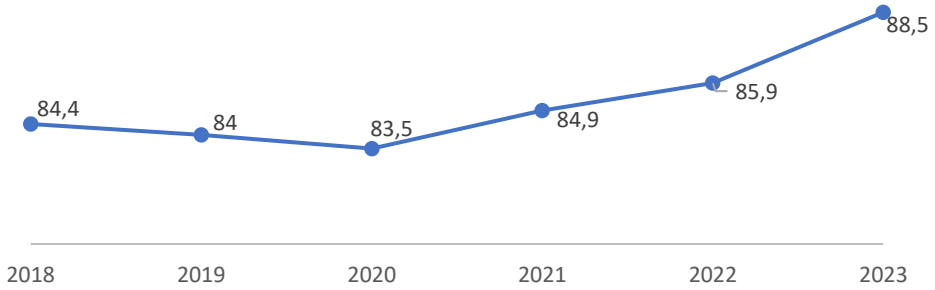


Gráfico 3: Fuente: Departamento Administrativo de la Función Pública. Medición de la política de Seguridad Digital - FURAG

Respecto a la medición realizada en el 2024 por el Departamento Administrativo de la Función Pública, con corte 2023, dicha Entidad emite las siguientes

recomendaciones relacionadas con la seguridad digital, en los siguientes términos:

Gráfico 4: Fuente DAFP, recomendaciones de seguridad digital, medición a corte 2023.

Teniendo en cuenta lo anterior, la Unidad para la Atención y Reparación Integral a las Víctimas define el presente Plan Estratégico de Seguridad de la Información (PESI), que incluye proyectos y operación relacionada con la seguridad de la información, para el cumplimiento de los objetivos estratégicos mencionados en el presente documento.

5. Estrategia de Seguridad Digital

La Unidad para la Atención y Reparación Integral a las Víctimas establece una estrategia de seguridad de la información en la que se integran los principios, políticas, procedimientos, guías, instructivos/manuales, formatos y lineamientos para la gestión de aseguramiento, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Por tal motivo, La Unidad para la Atención y Reparación Integral a las Víctimas adopta las siguientes 5 estrategias específicas propuestas por el MinTIC[1], que permitirán establecer en su conjunto una estrategia general de seguridad digital:

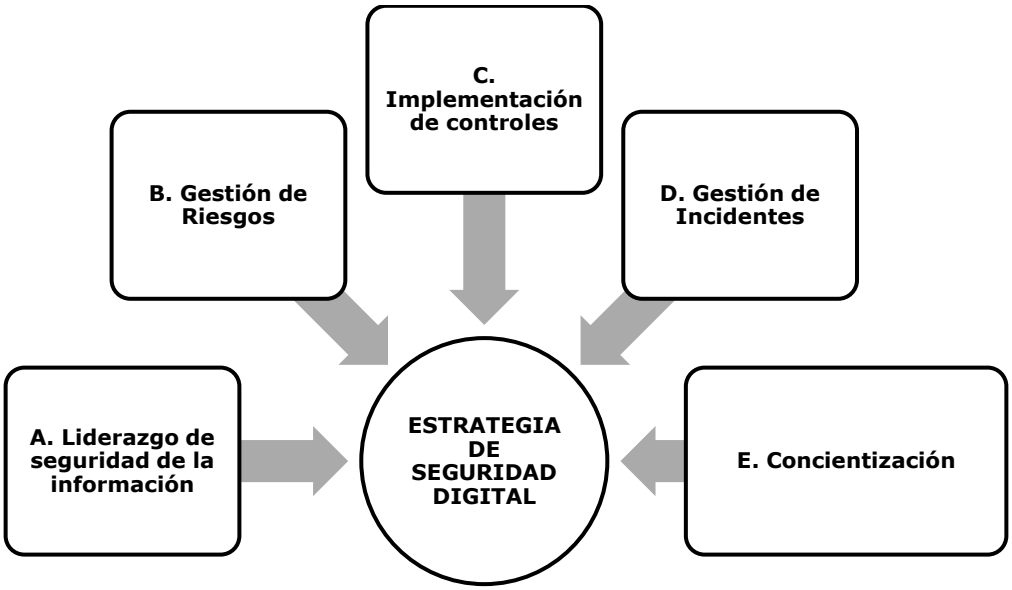


Gráfico 5: Fuente MinTIC, 5 Estrategias propuestas por el MinTIC para definir una Estrategia Integral de seguridad digital.

Estas estrategias planteadas por el MinTIC han sido consideradas por la Unidad para la Atención y Reparación Integral a las Víctimas y se han tiendo en cuenta en la formulación del Plan Estratégico de Seguridad de la Información 2023-2024 desde su elaboración inicial y sus correspondientes actualizaciones.

[1] Estrategias tomadas del manual de gobierno digital, publicado por el MinTIC, en la sección de seguridad y privacidad de la información, producto "Plan Estratégico de Seguridad de la Información (PESI)."
Fuente:
https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html?__noredirect=1

5.1 Descripción de las Estrategias Específicas (Ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas para dar continuidad a su implementación:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO[2]
A. Liderazgo de seguridad de la información	Establecer y apropiar los roles y responsabilidades en seguridad de la información en el marco de la gestión de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), tomando como referencia la Resolución 3157 de 2021 de la UARIV, la cual establece la política general y las políticas específicas, así como los lineamientos que tienen como propósito proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso y corresponsabilidad de la Dirección General y de los(as) Directores(as), subdirectores(as) y Jefes de Oficina de las diferentes dependencias y/o procesos estratégicos, misionales y de apoyo de la Entidad. Respecto al liderazgo de seguridad de la información en la Unidad para la Atención y Reparación Integral a las Víctimas, se resalta la siguiente decisión administrativa: Resolución 2728 de 2021 *Por la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, se derogan las Resoluciones No 1250 de 2018 y 1538 de 2019 sobre el Comité de Gestión Institucional y Desempeño y se dictan otras disposiciones*, la cual en el artículo 4 establece las Políticas de Gestión y Desempeño Institucional y sus Líderes, donde en el numeral 11 establece el liderazgo de la implementación de la política de Seguridad Digital a la Oficina de

[2] Las descripciones de las estrategias se han incluido tomando como referencia el manual de gobierno digital, publicado por el MinTIC, en la sección de seguridad y privacidad de la información, producto "Plan Estratégico de Seguridad de la Información (PESI)."
Fuente:
https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html?__noredirect=1

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO[2]
	Tecnologías de la Información y a la Subdirección Red Nacional de Información. Adicionalmente el artículo 8 de la mencionada Resolución, establece como función del Comité Institucional de Gestión y Desempeño de la Entidad, en el numeral 6, *"Asegurar la implementación y desarrollo de las políticas de gestión y las directrices en materia de seguridad digital y de la información"* Adicionalmente, el artículo 21 establece los líderes de la ejecución del Sistema Integrado de Gestión, asignando el liderazgo del Sistema de Gestión de Seguridad de la Información a la Oficina de Tecnologías de la Información.
B. Gestión de riesgos	Realizar la identificación, análisis, valoración, evaluación y tratamiento de los riesgos de seguridad de la información a través de la ejecución del procedimiento para la administración de riesgos establecido por la Oficina Asesora de Planeación de la Unidad para la Atención y Reparación Integral a las Víctimas, en articulación con los Procesos Estratégicos, Misionales y de Apoyo. Ver procedimiento: https://www.unidadvictimas.gov.co/documentos_bibliotec/procedimiento-de-administracion-de-riesgos-v7/
C. Implementación de controles	Realizar la planificación e implementación de 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, tomando como referencia la declaración de aplicabilidad de controles (SOA por sus siglas en inglés) establecida en el marco del Sistema de Gestión de Seguridad de la Información de la Unidad para la Atención y Reparación Integral a las Víctimas.
D. Gestión de incidentes	Realizar la oportuna atención y respuesta de incidentes de seguridad de la información con un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO[2]
	seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad. La Unidad para la Atención y Reparación Integral a las Víctimas cuenta con el procedimiento de atención de incidentes de seguridad, que involucra a la Mesa de Servicios Tecnológicos de la Oficina de TI para el registro y seguimiento de los casos que se generen.
E. Concientización	Fortalecer la cultura organizacional en la seguridad de la información para que la aplicación de los controles asociados al recurso humano sean parte de la cotidianidad, a través de la socialización de las políticas, lineamientos, controles, procedimientos y buenas prácticas incluyendo la transferencia de conocimiento y la generación de conciencia respecto a las responsabilidades del personal de la Entidad en relación con el aseguramiento de la información.

Tabla 2: Fuente de las Estrategias: MinTIC. Se adiciona el objetivo y la descripción de las estrategias para el diseño y ejecución del Plan Estratégico de Seguridad de la Información en la Unidad para las Víctimas, tomando como referencia el MSPI del MinTIC y demás lineamientos y guías.

6. Estructura del Plan Estratégico de Seguridad de la Información (PESI)

En el marco del Sistema de Gestión de Seguridad de la Información, el presente Plan Estratégico de Seguridad de la Información (PESI), involucra la siguiente estructura de trabajo, la cual permite categorizar las diferentes actividades requeridas para la consecución de los objetivos específicos definidos en el presente documento.

Gráfico 6: Estructura Plan Estratégico de Seguridad de la Información (PESI)

6.1 Plan de Seguridad y Privacidad de la Información

El Plan de Seguridad y Privacidad de la Información se construye en el marco del Sistema de Gestión de Seguridad de la Información de la Entidad, teniendo como referencia el ciclo PHVA[3] y las cinco (5) fases del Modelo de Seguridad y Privacidad de la Información del MinTIC que se definen como Diagnóstico, Planificación, Operación, Evaluación de Desempeño y Mejoramiento Continuo. A continuación, los requisitos definidos por el MinTIC para cada fase del Modelo:

[3] PHVA (Planear, hacer, verificar y actuar), conocido como Ciclo Deming, publicado en los años 50 por Edwards Deming

Gráfico 7: Ciclo del Modelo de Seguridad y Privacidad de la Información.

Teniendo en cuenta el ciclo de operación del modelo, la Unidad para la Atención y Reparación Integral a las Víctimas establece en este documento el plan de control operacional que contempla las actividades base asignadas al equipo de seguridad de la información de la Oficina de Tecnologías de la Información y el plan de trabajo para ejecución en articulación con los enlaces del Sistema Integrado de Gestión y/o Apoyos SGSI, de los diferentes procesos y Direcciones Territoriales de la Entidad. Adicionalmente, se establece el mecanismo de seguimiento, medición, análisis y evaluación de la ejecución del Plan de Seguridad y Privacidad de la Información.

6.1.1 Plan de Control Operacional

Este plan tiene como objetivo planificar, ejecutar y realizar seguimiento a las actividades relacionadas con el sostenimiento del Modelo de Seguridad y Privacidad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas, determinando las actividades base asignadas al Equipo de Seguridad de la Información y las actividades que requieren articulación con los Enlaces del Sistema Integrado de Gestión y/o Apoyos SGSI de los Procesos Estratégicos, Misionales y de Apoyo.

6.1.1.1 Actividades del Equipo de Seguridad de la Información - OTI

Las actividades establecidas en esta sección se enfocan en la gestión de actualización de políticas y lineamientos de seguridad de la información, así como de la actualización de la línea base de controles de seguridad aplicables para la Entidad y la correspondiente gestión de implementación en el marco del Modelo de Seguridad y Privacidad de la Información.

No	Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[4]
1	Realizar la actualización (en caso de ser necesario) y socialización de políticas, procedimientos y/o protocolos de seguridad de la información	OE.A OE.B OE.D	EJE A EJE D	Equipo de Seguridad de la Información - OTI	Nacional	01/02/2023	31/12/2026

[4] Aunque la fecha final corresponde al cierre del Plan Estratégico de Seguridad de la Información 2023-2026, las actividades aquí listadas deben ejecutarse una vez por cada vigencia.

No	Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[4]
2	Actualizar la declaración de aplicabilidad de controles en la Entidad	OE.B	EJE C	Equipo de Seguridad de la Información - OTI	Nacional	01/02/2023	31/12/2026
3	Gestionar la implementación de políticas y controles de seguridad de la información aplicables a los procesos y Direcciones Territoriales	OE.A OE.B OE.D OE.E OE.F	EJE B EJE C	Equipo de Seguridad de la Información – OTI Procesos de la Entidad Direcciones Territoriales	Nacional	01/02/2023	31/12/2026
4	Realizar seguimiento a la implementación del MSPI - Seguimiento a la implementación de políticas - Plan de tratamiento de riesgos	OE. B	EJE C	Equipo de Seguridad de la Información - OTI	Nacional	01/02/2023	31/12/2026
5	Realizar la atención y seguimiento a los eventos e incidentes de	OE.C	EJE D	Equipo de Seguridad de la Información - OTI	Nacional	01/02/2023	31/12/2026

No	Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[4]
	seguridad de la información						
6	Gestionar la ejecución de pruebas de Continuidad de la Operación Tecnológica	OE.E	EJE B EJE C	Equipo de Seguridad de la Información - OTI	Nacional	3/02/2025	31/12/2026

Tabla 3: Actividades – Plan de Control Operacional – Plan de Seguridad y Privacidad de la Información del Plan Estratégico de Seguridad de la Información (PESI)

Según la tabla 3, las actividades numeradas de la uno (1) a la cinco (5) tienen ejecución anual desde la vigencia 2023, por otra parte, la actividad seis (6) inicia ejecución en la vigencia 2025.

6.1.1.2 Plan de Trabajo – Articulación con Enlaces SIG

A continuación, se listan las macro actividades establecidas en el marco del Sistema de Gestión de Seguridad de la Información, para la correspondiente ejecución en articulación con el Sistema Integrado de Gestión.

No	Macro Actividad	Subactividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[5]
1	Actualizar inventario de activos de información y gestionar la publicación de los instrumentos de gestión de información en página Web Institucional[6]	Socializar el procedimiento para la generación y/o actualización del inventario de activos de información, a los enlaces del Sistema Integrado de Gestión- SIG (Procesos y DTs)	OE.A	EJE B	Procesos y Direcciones Territoriales	Nacional y Territorial	01/02/2023	31/12/2026
		Ejecutar el procedimiento para la generación y/o actualización del inventario de activos de información, a los enlaces del Sistema Integrado de Gestión- SIG (Procesos y DTs)						
2	Identificar, valorar y evaluar los Riesgos de Seguridad de la información y definir el correspondiente plan de tratamiento y realizar seguimiento con respecto a las evidencias de controles, riesgos y planes de tratamiento al riesgo (Ejecución del plan de tratamiento de Riesgos)	Cada uno de los procesos a nivel nacional debe realizar la actualización de los riesgos del SGSI, así como definir el plan de tratamiento de riesgos. Respecto a las Direcciones Territorial se definirán riesgos estandarizados, asociado a Seguridad de la Información.	OE.B	EJE B	Procesos y Direcciones Territoriales	Nacional y Territorial	01/02/2023	31/12/2026
		Realizar al seguimiento de los controles y planes a los riesgos asociados a Seguridad de la Información (plan de tratamiento 2025)						

[5] Aunque la fecha final corresponde al cierre del Plan Estratégico de Seguridad de la Información 2023-2026, las actividades aquí listadas deben ejecutarse una vez por cada vigencia acorde con lo establecido en el plan SIG articulado con la Oficina Asesora de Planeación.

[6] La publicación de los instrumentos de gestión de información en página Web Institucional, hace referencia al Registro de Activos de Información, Esquema de Publicación e Índice de Información Clasificada y Reservada. La actividad de publicación de estos instrumentos no hace parte del plan SIG debido a que corresponde a la Oficina de Tecnologías de la Información posterior a la gestión de aprobación por parte del Comité Institucional de Gestión y Desempeño.

No	Macro Actividad	Subactividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[5]
3	Realizar diagnóstico técnico de implementación de controles de seguridad aplicables al Proceso, de acuerdo con la Declaración de aplicabilidad (SOA)	Realizar capacitación certificada por Oficina de TI a enlaces SIG y/o apoyos SGSI en Fundamentos de Seguridad de la Información Realizar diagnóstico de implementación de controles en procesos y DTs por parte de los Enlaces y/o apoyos SGSI tomando como base la matriz de Declaración de Aplicabilidad que sean aplicables	OE.A OE.B OE.D OE.F	EJE C	Procesos y Direcciones Territoriales	Nacional y Territorial	01/02/2025	31/12/2026
4	Realizar prácticas de Ingeniería social - Vishing.	Llevar a cabo actividades de ingeniería social Vishing con el fin de medir e identificar el nivel de entendimiento de seguridad de los colaboradores de cada una de las DTs. Esta actividad se puede realizar con llamadas telefónicas, acatando los lineamientos de la Oficina de TI.	OE.C OE.D	EJE D EJE E	Procesos y Direcciones Territoriales	Nacional y Territorial	01/02/2025	31/12/2026
5	Establecer el repositorio de información oficial del proceso o dependencia o DT en la herramienta SharePoint, que permita resguardar la información importante para la operación	Identificación y apropiación de la información para respaldo o cargue de la información relevante e importante.	OE.A OE.B	EJE C EJE E	Procesos y Direcciones Territoriales	Nacional y Territorial	01/02/2025	31/12/2026

Tabla 4: Actividades – Plan de trabajo base para ejecución en articulación con los enlaces del Sistema Integrado de Gestión, en el marco del Plan de Seguridad y Privacidad de la Información del Plan Estratégico de Seguridad de la Información (PESI).

Como se observa en la tabla 4, las actividades relacionadas con la actualización de activos y gestión de riesgos tienen ejecución en el marco del PESI desde la vigencia 2023. Por otra parte, las actividades de la tres (3) a la cinco (5) son nuevas para inicio en la vigencia 2025.

6.1.2 Seguimiento, medición, análisis y evaluación

A continuación, se presentan los indicadores relacionados con cada objetivo específico del Sistema de Gestión de Seguridad de la Información que permiten el seguimiento, medición, análisis y evaluación de cumplimiento de Plan de Seguridad y Privacidad de la Información:

No	Objetivo	Indicador Plan de Acción	Indicadores parciales	Meta
1	Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.	Índice de ciberseguridad de la Unidad Fórmula: Sumatoria de la contribución ponderada de los proyectos y operaciones del Plan estratégico de Seguridad de la Información Línea base 50% Meta: 65%	(No. De Riesgos con nivel de riesgo residual bajo/Total de Riesgos identificados) *100	85%
			(No de Activos críticos con nivel riesgo residual Bajo /No. de Activos Críticos) *100	70%
			(No. Planes de tratamiento cerrados a conformidad al cierre de la vigencia /No. Planes de tratamiento) *100	100%
2	Implementar los controles de seguridad de la información, para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad.		Promedio efectividad de controles del Instrumento MSPI del MinTIC	80%
			Calificación Modelo de Ciberseguridad NIST del Instrumento MSPI del MinTIC	80%
3	Realizar seguimiento a los eventos e incidentes de seguridad, para obtener lecciones aprendidas y mejorar periódicamente el sistema de gestión de Seguridad de la Información.		(Suma de vulnerabilidades gestionadas y solucionadas / Suma de vulnerabilidades priorizadas remitidas a los dominios) *100	>= 80%
			(Número de tickets de mesa de servicios tecnológicos de seguridad resueltos / Número de tickets de mesa de servicios tecnológicos escalados al equipo de seguridad) *100	100%

No	Objetivo	Indicador Plan de Acción	Indicadores parciales	Meta
4	Promover, mantener y establecer la cultura en seguridad de la información en la Unidad para las Víctimas y partes interesadas.		Promedio Calificaciones Obtenidas en evaluaciones de Seguridad de la Información y Ciberseguridad	4,5
			(Número de participantes en campañas de concientización / Número de funcionarios y contratistas totales) *100	80%
			(Número de participantes en campañas de concientización / Número de funcionarios y contratistas totales) *100	80%
5	Incrementar la disponibilidad de servicios de TI y de operación, a través del plan de continuidad de negocio.		(No. Simulacros Éxitos en gestión de continuidad Tecnológica y/o negocio /No. simulacros realizados) *100	100%
6	Suministrar información confiable, íntegra, oportuna, accesible y de valor a la población Víctima.		Porcentaje de disponibilidad de la infraestructura tecnológica	99,9%

Tabla 5: Indicadores por objetivo del SGSI, para el cumplimiento con la ejecución del Plan de Seguridad y Privacidad de la Información del Plan Estratégico de Seguridad de la Información (PESI).

6.2 Proyectos y Operaciones

La Oficina de Tecnologías de la Información, a través del dominio de Arquitectura y Gobierno TI, ha establecido el Plan Estratégico de Tecnologías de la Información donde se consolidan los proyectos y operaciones de TI, incluyendo lo relacionado con la Seguridad de la Información. A continuación, se presentan los proyectos y operaciones definidos en el marco del Plan Estratégico de Seguridad de la Información, alineadas con el Plan Estratégico de Tecnologías de la Información de la Entidad.

TIPO	ESTRATEGIAS / EJES	PROYECTO/ OPERACIÓN	PRODUCTOS O SERVICIOS ESPERADOS	OBSERVACIÓN
Proyecto	A. Liderazgo de seguridad de la información B. Gestión de riesgos C. Implementación de controles E. Concientización	Ciber-seguridad 360°	Implementación de controles de seguridad y protección de información en equipos de cómputo Fortalecimiento en la definición de requisitos de seguridad en el ciclo de vida de desarrollo de software Anonimización de datos en ambientes de pruebas Fortalecimiento del control de acceso a servidores y bases de datos Análisis de vulnerabilidades y hacking ético Sensibilización de usuarios (funcionarios, contratistas y colaboradores contratados por terceros)	Finalizado en el 2024
Proyecto	B. Gestión de riesgos D. Gestión de incidentes	Estructuración SOC	Contratación de servicio de SOC (Security Operation Center)	Finalizado en 2024
Operación	B. Gestión de riesgos D. Gestión de incidentes	Operación servicio SOC	Servicio de monitoreo activo 7/24 de los activos críticos de software e infraestructura TI para la atención oportuna de eventos e incidentes de seguridad digital Gestión de eventos e incidentes de seguridad digital	En definición
Proyecto	C. Implementación de controles	Gestión de identidades	Articulación de sistemas de información priorizados con el Directorio Activo	En definición
Operación	C. Implementación de controles D. Gestión de incidentes	Plan recuperación de desastres	Actualización del DRP (plan de recuperación de desastres) de la Unidad para la Atención y Reparación Integral a las Víctimas (Finalizado) Documentación de las pruebas controladas de los planes de recuperación de desastres	En Definición

TIPO	ESTRATEGIAS / EJES	PROYECTO/ OPERACIÓN	PRODUCTOS O SERVICIOS ESPERADOS	OBSERVACIÓN
Operación	C. Implementación de controles D. Gestión de incidentes	Plan Continuidad	Generación del Plan de Continuidad de Negocio (operaciones) que involucre los procesos misionales y DTs. Documentación de las pruebas controladas de los planes de continuidad de negocio (operación)	En definición
Operación	C. Implementación de controles	Atención No Conformidades auditorías y oportunidades de mejora	Evidencias o soportes de la ejecución de los planes establecidos para el cierre de las No conformidades relacionadas con el SGSI	En ejecución
Operación	C. Implementación de controles E. Concientización	Implementación capacidad de seguridad de la información en procesos y Direcciones Territoriales	Implementación de controles aplicables de seguridad de la información en Direcciones Territoriales y Puntos de Atención Jornadas de sensibilización en seguridad de la información	En ejecución
Proyecto	C. Implementación de controles	Cambio de equipos de seguridad perimetral e implementación controles DLP	Adquisición de Firewall Implementación de DLP (Data Loss Prevention) para la prevención de fuga de información.	En definición
Proyecto	C. Implementación de controles	Tratamiento de datos Personales Fase 1	Documentación de políticas, lineamientos y/o protocolos orientados al tratamiento de datos personales Definición e implementación de controles de tratamiento de datos personales – fase 1	En definición

Tabla 6: Portafolio de proyectos y operaciones del Plan Estratégico de Seguridad de la Información (PESI)

Estos proyectos y operaciones contemplan lo documentado en el banco de iniciativas de Arquitectura Empresarial, donde se identifican las siguientes propuestas relacionadas con seguridad de la información:

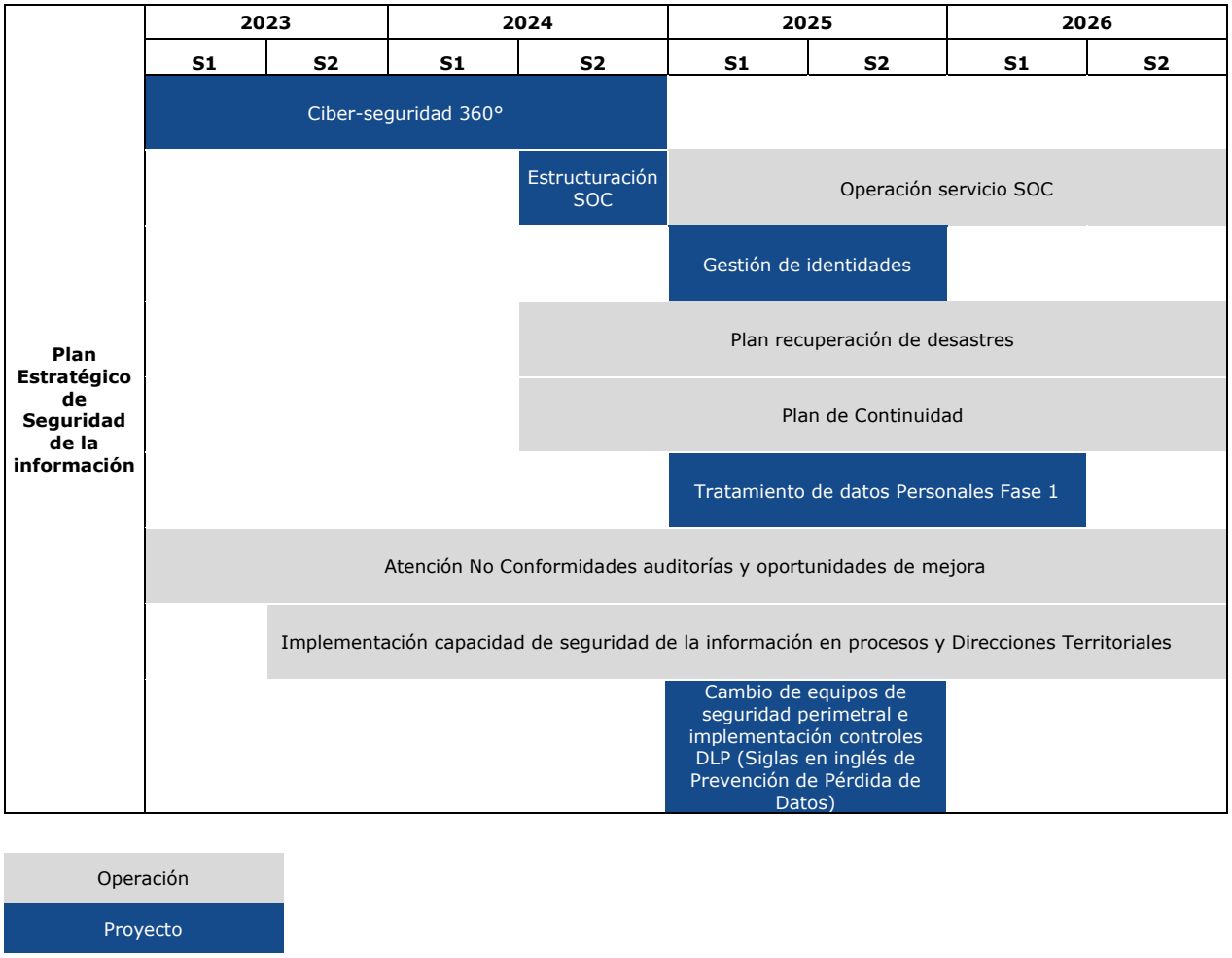
Fecha y Hora de registro de iniciativa	Ingresa un Título o Nombre a tu iniciativa	Identifica y describe de manera breve y concisa tu necesidad o problemática a resolver	Selecciona el o los procesos que impactan y benefician la iniciativa planteada	Proyecto u Operación que aborda la iniciativa
10/16/23 13:23:50	Inclusión de hash en el envío y recepción de archivos planos	1. Incluir código Hash al archivo con la colocación que se carga en Azure	Gestión para la Asistencia;	Implementación capacidad de seguridad de la información en procesos y Direcciones Territoriales
10/16/23 14:44:11	Implementar monitoreo detallado en equipos de cómputo donde se descarga o se maneja el listado de pagos	Implementar monitoreo detallado en equipos de cómputo donde se descarga o se maneja el listado de pagos	Gestión para la Asistencia;	Implementación Controles DLP
10/16/23 14:44:45	Seguridad y perfilamiento de acceso a datos (acceso a objetos de BD)	Seguridad y perfilamiento de acceso a datos (acceso a objetos de BD)	Gestión para la Asistencia;	Implementación capacidad de seguridad de la información en procesos y Direcciones Territoriales
10/16/23 16:01:52	Seguridad en los documentos de envío	Seguridad en los documentos de envío	Gestión Documental;	Implementación Controles DLP
8/29/24 11:36:05	Intercambio de la información	Mantener actualizadas las bases de datos	Registro y Valoración; Gestión de la Información; Gestión Interinstitucional;	Implementación capacidad de seguridad de la información en procesos y Direcciones Territoriales

Tabla 7: Banco de Iniciativas relacionadas principalmente con Seguridad de la Información, documentadas en el marco del Dominio de Arquitectura Empresarial.

Es importante indicar que el banco de iniciativas de Arquitectura Empresarial es un instrumento dinámico que puede permitir la identificación de nuevas necesidades relacionadas con Seguridad de la Información, las cuales serán evaluadas para determinar si es necesario la creación de un nuevo proyecto o es incluida en la operación existente.

6.2.1 Mapa de Ruta de proyectos y operaciones

A continuación, se presenta el mapa de ruta de los proyectos y operaciones de Seguridad de la información:



7.Análisis Presupuestal

A partir de los proyectos contemplados en el mapa de ruta se realiza la estimación del presupuesto aproximado por vigencia que determina su viabilidad para aprobación del Comité Institucional de Gestión y Desempeño:

AÑO 2023		AÑO 2024		AÑO 2025	
Proyecto	**Inversión**	**Proyecto**	**Inversión**	**Proyecto**	**Presupuesto preliminar[7]**
Ciberseguridad 360[8]	$ 480.462.487,50	Ciberseguridad 360	$480.462.487,50	Gestión de Identidades	$ 101.763.622,50
		Estructuración SOC	$ 292.658.152,00	Tratamiento de datos Personales Fase 1	$ 101.763.622,50
				Cambio de equipos de seguridad perimetral e implementación controles DLP	$750.000.000,00
TOTAL PRESUPUESTO	**$480.462.487,50**	**TOTAL PRESUPUESTO**	**$773.120.639,50**	**TOTAL PRESUPUESTO**	**$ 953.527.245,00**

[7] Presupuesto preliminar: corresponde a una estimación inicial, toda vez que los valores se definirán e incluirán en el PETI cuando se definan las actas de constitución de proyectos.

[8] En el plan de dirección del proyecto "Ciberseguridad 360" se documentó un presupuesto total de $960.924.975 con una duración de 15 meses, ejecutado entre el 2023 y 2024, por tal razón, para la estimación anual se asigna el 50% (480.462.487,5) para la vigencia 2023 y el 50% (480.462.487,5) para la vigencia 2024.

Unidad para las Víctimas

8.Responsables

A continuación, se listan las instancias y dependencias involucradas en la definición e implementación del Plan Estratégico de Seguridad de la Información y las funciones correspondientes:

1. Comité Institucional de Gestión y Desempeño (Alta Dirección):
    - Aprobar y establecer el Plan Estratégico de Seguridad de la Información, así como las directrices que permitan su implementación a nivel nacional.
    - Realizar seguimiento a la implementación del Plan Estratégico

2. Dirección General, Oficinas Asesoras, Subdirección General, Secretaría General, Direcciones y Subdirecciones:
    - Participar en un escenario de corresponsabilidad en la implementación del Plan Estratégico de Seguridad de la Información y garantizar los recursos requeridos.

3. Oficina de Tecnologías de la Información:
    - Coordinar las actividades de implementación del Plan Estratégico de Seguridad de la Información

4. Funcionarios, Contratistas y Colaboradores:
    - Implementar las políticas, lineamientos y controles de seguridad aplicables.

9. Aprobación

El presente plan ha sido sometido a consideración y conocimiento de la Alta Dirección, a través del Comité Institucional de Gestión y Desempeño con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ/ACTUALIZÓ	REVISÓ	APROBÓ
Nombre: Joaquín Rojas Palomino **Cargo: Profesional Especializado**	Nombre: Darío Eduardo Muñetón Zuluaga **Cargo: Jefe de la Oficina de Tecnologías de la Información**	Comité Institucional de Gestión y Desempeño **Acta No:** 1 **Fecha:** 31 enero 2025