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

Control de Versiones

Versión	Fecha	Modificación
1.0	16/01/2023	Versión inicial del documento

Tabla de contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN & PORTAFOLIO DE PROYECTOS 3
1. OBJETIVO 3
1.1 OBJETIVOS ESPECÍFICOS (OE) 4
2. ALCANCE 4
3. DOCUMENTOS DE REFERENCIA 4
4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5
5. ESTRATEGIA DE SEGURIDAD DIGITAL 8
5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES) 9
6. ESTRUCTURA DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI) 10
6.1 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 11
6.1.1 PLAN DE CONTROL OPERACIONAL 12
6.1.2 PLAN DE TRABAJO – ENLACES SIG 13
6.1.3 INDICADORES SGSI – PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 14
6.2 PORTAFOLIO DE PROYECTOS: 16
6.2.1 CRONOGRAMA DE ACTIVIDADES / PROYECTOS: 19
7. RESPONSABLES 20
8. APROBACIÓN 20

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 partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2026.

1.1 OBJETIVOS ESPECÍFICOS (OE)

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 al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información e incluye la implementación de controles relacionados con la privacidad de la información de identificación personal, contemplando 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:

- 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 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 presente Plan Estratégico de Seguridad de la Información (PESI), ya que incluye el plan de seguridad y privacidad de la información, el cual corresponde a uno de los requisitos a desarrollar para cumplir con esta normativa.
- 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.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

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 los planes de seguridad y privacidad de la información que se han establecido en la Entidad en vigencias anteriores. A continuación, se presenta el resultado del diagnóstico de evaluación de controles realizado a través del instrumento dispuesto por el MinTIC:

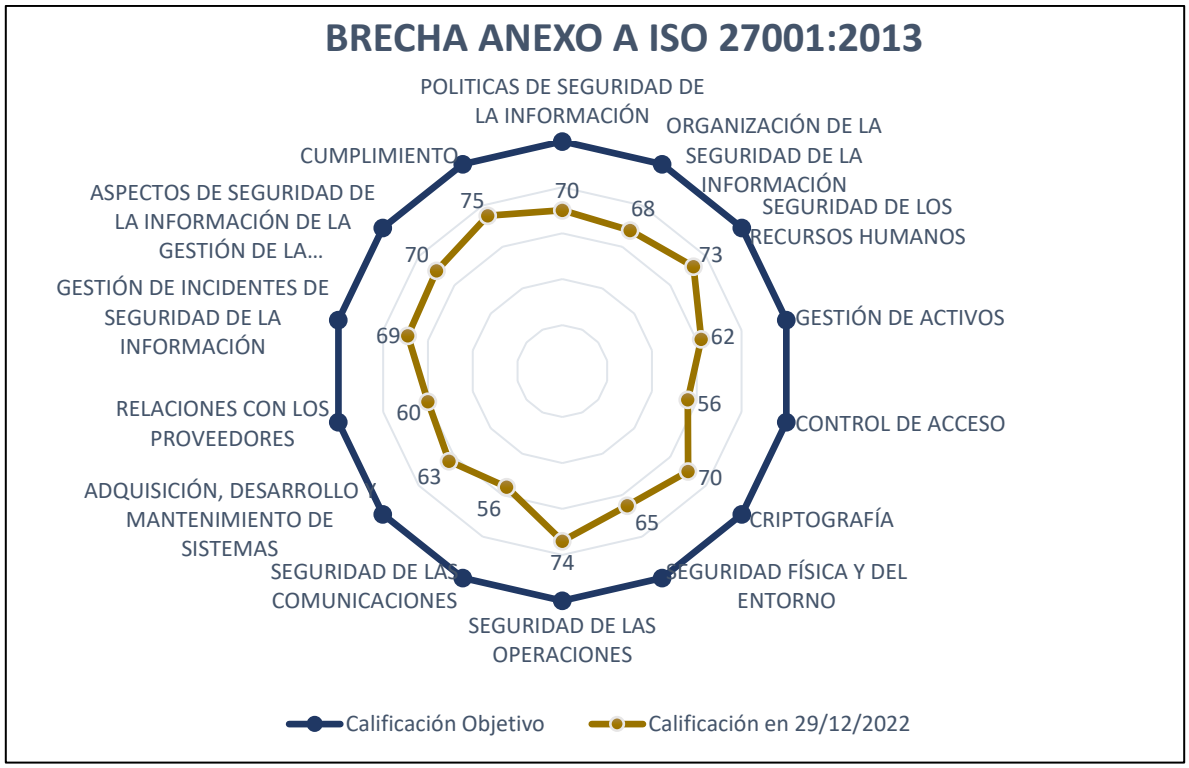

Gráfico 1: evaluación de efectividad de controles - ISO 27001:2013 Anexo A – Instrumento MSPI del MinTIC

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 7 - Seguridad digital", realizado por el Departamento Administrativo de la Función Pública, a través del FURAG.

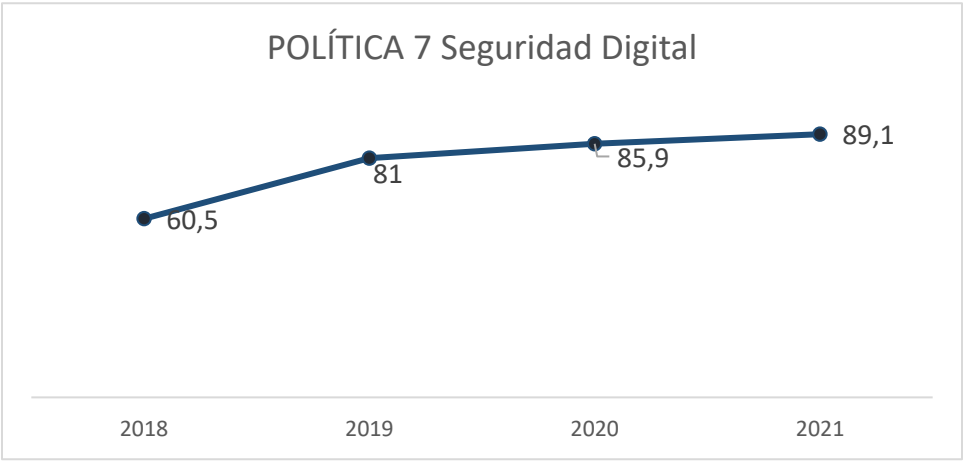

Gráfico 2: Fuente DAFP, medición MIPG, indicador Política 7 seguridad digital

Por otra parte, la medición del indicador "I21GOBIERNO DIGITAL Fortalecimiento de la Seguridad y Privacidad de la Información", tiene el siguiente comportamiento:

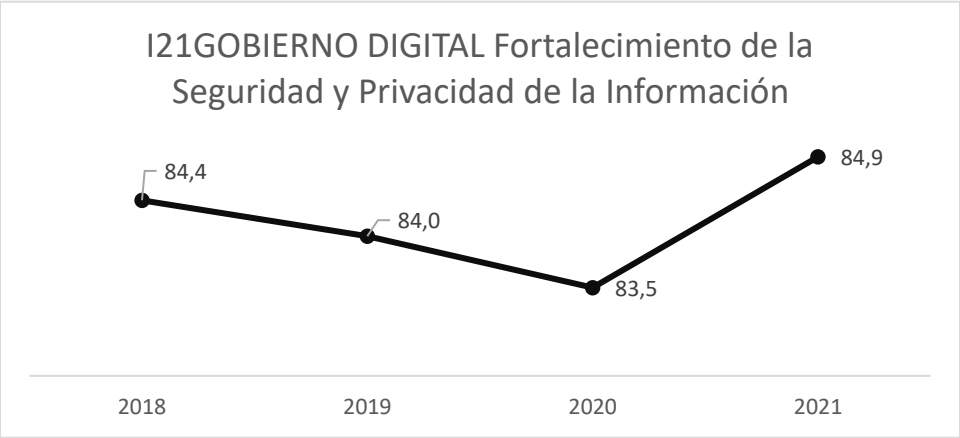

Gráfico 3: Fuente DAFP, medición MIPG, indicador I21 gobierno digital – fortalecimiento de la seguridad y privacidad de la información

Respecto a la medición realizada en el 2022 por el Departamento Administrativo de la Función Pública, con corte 2021, dicha Entidad emite las siguientes recomendaciones relacionadas con la seguridad digital, en los siguientes términos:

#	RECOMENDACIÓN
1	Fortalecer las capacidades en seguridad digital de la entidad estableciendo convenios o acuerdos con otras entidades en temas relacionados con la defensa y seguridad digital.
2	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética.
3	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC.
4	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.
5	Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.

Tabla 1: Fuente DAFP, recomendaciones de seguridad digital, medición a corte 2021.

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 definidos en la Resolución 3157 de 2021 de la Unidad.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

La Unidad para la Atención y Reparación Integral a las Víctimas establece una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, instructivos/manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.

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:

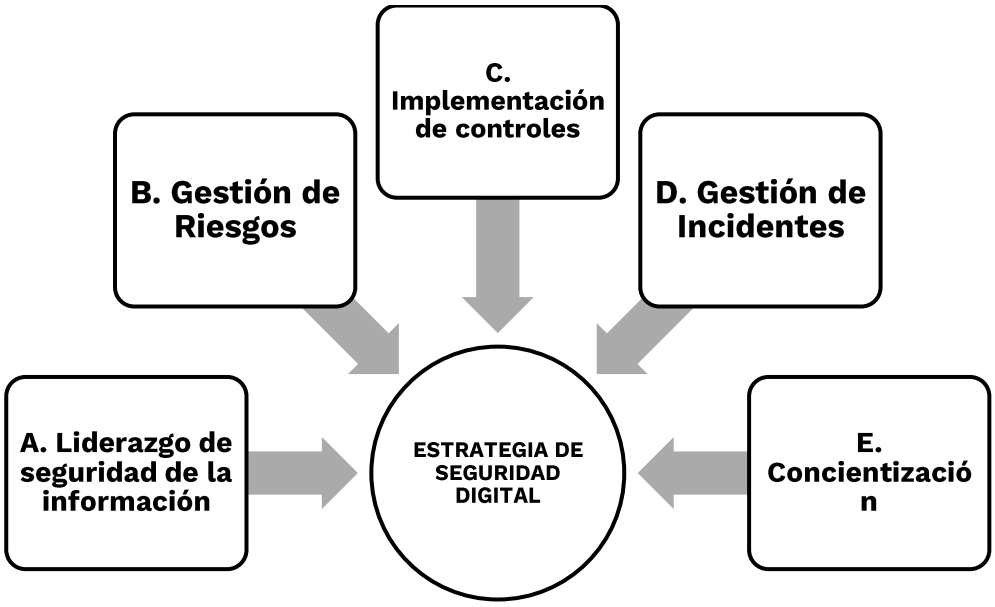

Gráfico 4: Fuente MinTIC, 5 Estrategias propuestas por el MinTIC para definir una Estrategia Integral de seguridad digital.

[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 a implementar:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO[2]
A. Liderazgo de seguridad de la información	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 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, en un escenario de corresponsabilidad, a través del establecimiento de roles y responsabilidades requeridas para el aseguramiento de la información.
B. Gestión de riesgos	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. Ver procedimiento: https://www.unidadvictimas.gov.co/es/prueba-sig/direccionamiento-estrategico
C. Implementación de controles	Planificación e implementación 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

[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

	Unidad para la Atención y Reparación Integral a las Víctimas.
D. Gestión de incidentes	Atención y respuesta 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.
E. Concientización	Implementación y fortalecimiento de la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, lineamientos, controles, procedimientos y buenas prácticas la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

Tabla 2: Fuente MinTIC, 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), contempla 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.

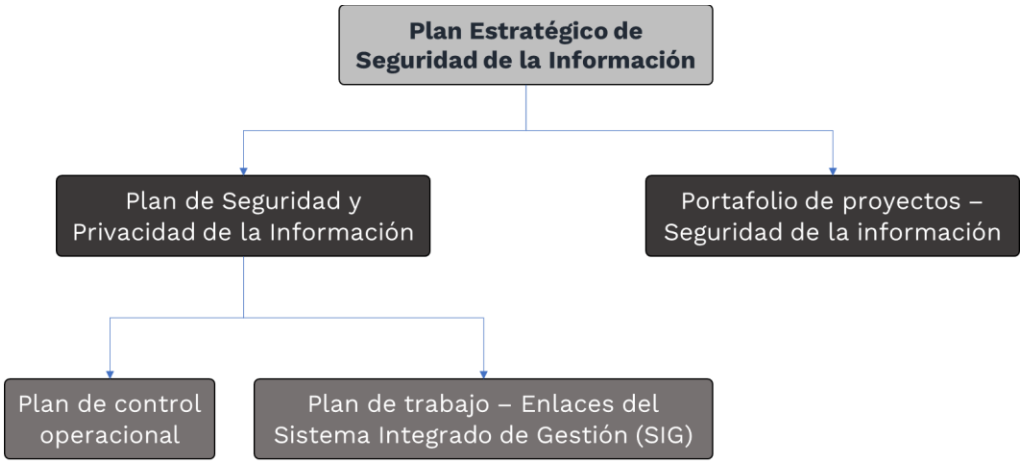

Gráfico 5: Estructura Plan Estratégico de Seguridad de la Información (PESI).

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], el cual según el Modelo de Seguridad y Privacidad de la Información del MinTIC se define como planificación, implementación, evaluación de desempeño y mejora continua.

A continuación, se el ciclo de operación, tomando como referencia el Modelo de Seguridad y Privacidad de la Información del MinTIC:

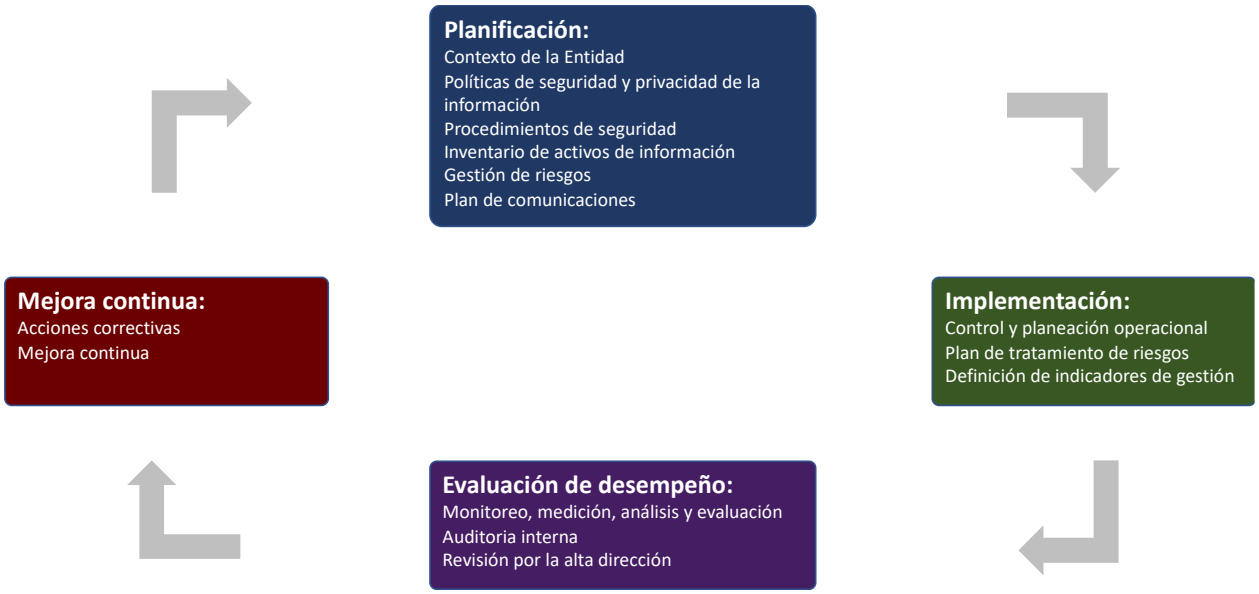

Gráfico 6: Ciclo de operación del Modelo de Seguridad y Privacidad de la Información).

Teniendo en cuenta el ciclo de operación del modelo, la Unidad para la Atención y Reparación Integral a las Víctimas establece por medio de este documente el plan de control operacional y el plan de trabajo para ser ejecutado en articulación con los enlaces del Sistema Integrado de Gestión, de los diferentes procesos y Direcciones Territoriales de la Entidad.

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

6.1.1 PLAN DE CONTROL OPERACIONAL

Este plan tiene como objetivo planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos, para esto se establecen las siguientes actividades a implementar de manera cíclica, una vez cada vigencia, durante los años 2023 al 2026:

No	Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[4]
1	Actualización (en caso de ser necesario) y socialización de políticas de seguridad de la información clasificadas por componente de aplicación (datos, aplicaciones, infraestructura, factor humano)	OE.A OE.D	EJE A EJE D	Equipo de Seguridad de la Información - OTI	Nacional	01/02/2023	31/12/2026
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	Implementación de políticas y controles de seguridad de la información aplicables a los procesos y Direcciones Territoriales	OE.A OE.B 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] 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 durante los 4 años incluidos en el alcance del presente documento.

No	Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[4]
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 seguridad de la información	OE.C	EJE D	Equipo de Seguridad de la Información - OTI	Nacional	01/02/2023	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).

6.1.2 PLAN DE TRABAJO – ENLACES SIG

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

No.	Macro Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[5]
1	Gestionar la identificación y clasificación de activos de información	OE.A	EJE B	Procesos	Nacional	01/02/2023	31/12/2026
2	Identificar, valorar, definir plan de	OE.B	EJE B	Procesos	Nacional	01/02/2023	31/12/2026

[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 durante los 4 años incluidos en el alcance del presente documento.

No.	Macro Actividad	Objetivo Específico	Estrategia Seguridad MinTIC	Responsable	Cobertura	Fecha Inicio	Fecha Final[5]
	tratamiento y realizar seguimiento de riesgos de activos críticos						
3	Implementar los controles de seguridad aplicables al Proceso o DT, de acuerdo con la Declaración de aplicabilidad (SOA)	OE.A OE.B OE.E OE.F	EJE B EJE C	Procesos	Nacional	01/02/2023	31/12/2026
4	Gestionar las actividades complementarias para el SGSI de la vigencia.	OE.D	EJE D EJE E	Procesos	Nacional	01/02/2023	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).

6.1.3 INDICADORES SGSI – PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se relacionan los indicadores relacionados con cada objetivo específico del Sistema de Gestión de Seguridad de la Información:

No	Objetivo	Ecuación del Indicador	Meta
1	Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.	No. De Riesgos con nivel de riesgo residual bajo/Total de Riesgos identificados	85%
		No de Activos críticos con nivel riesgo residual Bajo /No. de Activos Críticos	70%
		No. Planes de tratamiento cerrados a conformidad al cierre de la vigencia /No. Planes de tratamiento	100%

No	Objetivo	Ecuación del Indicador	Meta
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%
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	>= 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%
		Número de eventos reportados por los colaboradores internamente/ Número de eventos Totales	50%
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	80%
		Número de participantes en campañas de concientización / Número de funcionarios y contratistas totales	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 del negocio /No. simulacros en gestión de continuidad del negocio	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 PORTAFOLIO DE PROYECTOS:

La Oficina de Tecnologías de la Información, a través del dominio de Arquitectura y Gobierno TI, realizó jornadas de planeación estratégica durante el último trimestre del año 2022, mediante las cuales se definieron y priorizaron iniciativas relacionadas con Tecnologías e Información para la Unidad para las Víctimas, donde se incluyeron las relacionadas 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
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)

TIPO	ESTRATEGIAS / EJES	PROYECTO/ OPERACIÓN	PRODUCTOS O SERVICIOS ESPERADOS
Proyecto	B. Gestión de riesgos D. Gestión de incidentes	Estructuración SOC	Contratación de servicio de SOC (Security Operation Center)
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
Proyecto	C. Implementación de controles	Gestión de identidades	Articulación de sistemas de información priorizados con el Directorio Activo Portal único de acceso a Sistemas de información de la Entidad
Proyecto	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 Documentación de las pruebas controladas de los planes de recuperación de desastres

TIPO	ESTRATEGIAS / EJES	PROYECTO/ OPERACIÓN	PRODUCTOS O SERVICIOS ESPERADOS
Proyecto	C. Implementación de controles D. Gestión de incidentes	Apoyo Plan Continuidad	Generación del Plan de Continuidad de Negocio (operaciones) que involucre los procesos misionales, las DTs y puntos de atención. Documentación de las pruebas controladas de los planes de continuidad de negocio (operación)
Operación	C. Implementación de controles	Atención No Conformidades auditorías	Evidencias o soportes de la ejecución de los planes establecidos para el cierre de las No conformidades relacionadas con el SGSI
Operación	C. Implementación de controles E. Concientización	Implementación capacidad de seguridad de la información en territorio	Implementación de controles aplicables de seguridad de la información en Direcciones Territoriales y Puntos de Atención Jornadas de sensibilización en seguridad de la información

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

6.2.1 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

A partir de las jornadas de planeación estratégica realizadas por la Oficina de Tecnologías de la Información, a continuación, se presenta el cronograma a alto nivel de los proyectos y operaciones establecidos en el marco del Plan Estratégico de Seguridad de la Información, alineado con el Plan Estratégico de Tecnologías de la Información – PETI (2023-2026).

UNIDAD PARA LAS VÍCTIMAS				Plan Estratégico de Seguridad de la Información - PESI (2023-2026)							
Capacidades				Portafolio TI							
Componentes		Capacidad		2023		2024		2025		2026	
ID	Nombre	ID	Nombre	S1	S2	S1	S2	S1	S2	S1	S2
CO1	Habilitadores	1.2	Seguridad y Privacidad de la Información	Ciber-seguridad 360°							
						Estructuración SOC	Operación servicio SOC				
				Atención No Conformidades auditorías		Gestión de identidades					
					Implementación capacidad de seguridad de la información en territorio						
						Plan recuperación de desastres	Plan Continuidad				

Convenciones:

Proyecto	Producto, servicio o resultado
Proyecto (Liderado por otra área)	Producto, servicio o resultado liderado por otra área
Operación	Actividades continuas que contribuyen a metas PETI
----------	División por vigencia
CO	Componente

7. RESPONSABLES

1. Comité Institucional de Gestión y Desempeño (Alta Dirección): Aprobar los documentos de Alto Nivel
2. Dirección General, Oficinas Asesoras, Subdirección General, Secretaría General, Direcciones y Subdirecciones: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Oficina de Tecnologías de la Información: Coordinar las actividades de implementación del MSPI
4. Funcionarios, Contratistas y Colaboradores: Implementación de políticas, lineamientos y controles de seguridad aplicables.

8. 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	REVISÓ	APROBÓ
Nombre: Joaquín Rojas Palomino **Cargo: Contratista**	Nombre: Darío Eduardo Muñetón Zuluaga **Cargo: Jefe de la Oficina de Tecnologías de la Información**	Comité Institucional de Gestión y Desempeño **Acta No:** **Fecha:**