1. OBJETIVO

Establecer el procedimiento macro para la gestión de la Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, el ciclo PHVA, y los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de proteger los activos de información institucionales, garantizar la confidencialidad, integridad y disponibilidad de los datos, y cumplir con la normativa vigente.

2. ALCANCE

Este procedimiento contempla inicialmente la planificación estratégica de la seguridad de la información hasta la implementación, seguimiento, evaluación y mejora continua de los controles, riesgos, incidentes y los planes de continuidad. Así mismo, aplica a todas las dependencias de la Unidad, incluyendo la Oficina de Tecnologías de la Información junto con el rol de los Administradores de Sistemas de Información, Oficina Asesora de Planeación, Oficina Asesora de Comunicaciones, Direcciones Territoriales, Procesos Estratégicos, misionales, de apoyo y de Seguimiento y Control.

3. DEFINICIONES

Activos de Información:
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

ANS:
Acuerdo de Nivel de Servicio.

BCP (Business Continuity Planning / Plan de Continuidad de Negocios)[1]:
Es un plan logístico detallado de cómo una entidad debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

ColCERT[2]:
Por sus siglas en inglés Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual se encuentra enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica cibernética del Estado Colombiano frente a emergencias de Ciberseguridad que atenten y comprometan la seguridad y defensa nacional.

---

[1] Fuente: Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC versión 5 del 21/04/2025
[2] ibidem

DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres)[3]:
Es un documento formal creado por una organización que contiene instrucciones detalladas con la definición de los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

Ley de Transparencia y Acceso a la Información Pública[4]:
Se refiere a la Ley Estatutaria 1712 de 2014, o aquella que la modifique, adicione o sustituya.

MSPI (Modelo de Seguridad y Privacidad de la Información)[5]:
Modelo diseñado por el MinTIC para orientar a las entidades públicas en la implementación de prácticas de seguridad digital, protección de datos personales y gestión de riesgos tecnológicos.

PESI:
Plan Estratégico de Seguridad de la Información.

SOA (Statement of Applicability):
Declaración de aplicabilidad de controles, que identifica qué controles de seguridad son pertinentes para cada proceso o área de la entidad, según los riesgos identificados.

4. CRITERIOS DE OPERACIÓN

Los siguientes criterios definen las condiciones bajo las cuales se ejecutan las actividades del procedimiento, asegurando su eficacia, trazabilidad y alineación con el marco normativo institucional

a) La implementación de la Seguridad de la Información es de responsabilidad de todos los procesos y del recurso humano, en un escenario de corresponsabilidad y articulación armónica para la implementación de controles de aseguramiento.

b) Las actividades deben ejecutarse conforme a la Política de Seguridad de la Información establecida mediante Resolución vigente por la Unidad para las Víctimas.

c) Toda acción y proyecto relacionado con Seguridad de la Información debe estar alineada con el Plan Estratégico de Seguridad de la Información (PESI).

d) Los Procesos Estratégicos, Misionales, de Apoyo y de Seguimiento y Control, así como las Direcciones Territoriales deben avanzar en la implementación de los controles aplicables según la Declaración de Aplicabilidad (SOA).

---

[3] ibidem
[4] ibidem
[5] Gobierno digital. ¿Qué es el MSPI?. 2025. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

e) La gestión de riesgos debe seguir la metodología institucional definida por la Oficina Asesora de Planeación.

f) Las actualizaciones del inventario de activos, matriz de riesgos y la declaración de aplicabilidad de controles debe realizarse con una periodicidad anual.

g) Las actividades de sensibilización deben ejecutarse mensualmente, mediante el uso de diferentes estrategias de comunicación tales como la ejecución de charlas de seguridad y el envío de infografías relacionadas con la Seguridad de la Información.

h) Los eventos e incidentes de seguridad deben registrarse en la Mesa de Servicios Tecnológicos y deben gestionarse por demanda, siguiendo el Instructivo de soporte Mesa de Servicios vigente.

i) Las pruebas de continuidad (BCP/DRP) deben realizarse al menos una vez al año o cuando se presenten cambios significativos.

j) La Normatividad requerida para el desarrollo de las actividades citadas en el presente procedimiento se encuentra definida en el Normograma de la Unidad, disponible para consulta en la página web.

5. DESCRIPCION DE ACTIVIDADES

Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
PLANEAR						
Instrumento MSPI del MinTIC[6] Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MinTIC)[7]	**1.** Realizar y actualizar el diagnóstico del MSPI.	Oficina de Tecnologías de la Información	Diligenciar el instrumento del Modelo de Seguridad y Privacidad de la Información - MSPI del MinTIC (periodicidad semestral)		Registro del Instrumento (MSPI) del MinTIC diligenciado	Comité Institucional de Gestión y Desempeño Entes de Control Departamento Administrativo para la Prosperidad Social
Instrumento (MSPI) diligenciado Documento Maestro de Los	**2.** Gestionar la formulación o actualización el PESI	Oficina de Tecnologías de la Información	Formular o actualizar el Plan Estratégico de Seguridad de la Información (PESI) (periodicidad anual)		Documento PESI con: Plan Operativo Equipo de	Comité Institucional de Gestión y Desempeño

[6] Gobierno digital. Instrumento MSPI de MinTIC. 2025. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401779_recurso_1.xlsx
[7] Gobierno digital. Lineamientos MSPI de MinTIC. 2025. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
Lineamientos del Modelo de Seguridad y Privacidad de la Información (MinTIC) Resultado FURAG					Seguridad de Oficina de TI Plan de Implementación SIG[8] Proyectos para articulación con el PETI	Entes de Control Procesos y Direcciones Territoriales Departamento Administrativo para la Prosperidad Social
Plan de Implementación SIG – SGSI Inventario de activos de la vigencia anterior	**3.** Generar o Actualizar el inventario de activos	Todos los procesos y/o Direcciones Territoriales	Ejecutar el Procedimiento de Generación del Inventario de Activos de Información (periodicidad anual)		Registro del inventario de activos actualizado Registro de identificación de activos críticos Registro de los Instrumentos de Gestión de Información Pública (Ley 1712 de 2014)	Comité Institucional de Gestión y Desempeño Procesos y Direcciones Territoriales Entes de Control
Registro de identificación de activos críticos	**4.** Verificar la identificación de activos críticos de información de la entidad	Equipo de Seguridad de la Informacion - OTI	Verificar la identificación de activos críticos de información de la entidad ¿Se registran activos críticos? SI: Continúa a la actividad 5 NO: Continúa a la actividad 6	**X**	Verificación de la identificación de activos críticos. Socialización de activos críticos a todos los procesos de la Unidad.	Equipo de Seguridad de la Informacion OTI. Todos los procesos de la Unidad
Inventario de activos actualizado Identificación de activos críticos Matriz de riesgos por	**5.** Gestionar la identificación o actualización de riesgos SGSI	Todos los procesos y/o Direcciones Territoriales	Ejecutar el Procedimiento de Administración de Riesgos de la Oficina Asesora de Planeación (periodicidad anual)		Matriz de riesgos SGSI por Proceso y Riesgo tipo para las Direcciones Territoriales	Comité Institucional de Gestión y Desempeño Oficina de Tecnologías de la Información

[8] Esta salida hace referencia a la participación de la Oficina de Tecnologías de la Información en la actividad "Presentar y socializar a los enlaces del nivel nacional y territorial la propuesta" del procedimiento formulación, aprobación y seguimiento al plan de implementación del sistema integrado de gestión". Recuperado de: https://www.unidadvictimas.gov.co/documentos_bibliotec/procedimiento-formulacion-y-seguimiento-al-plan-de-implementacion-del-sistema-integrado-de-gestion-v3/

Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
proceso de la vigencia anterior						Entes de control
Instrumento MSPI del MinTIC Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MinTIC)	**6.** Diligenciar aplicabilidad de controles (SOA)	Todos los procesos y/o Direcciones Territoriales	Definir los controles de Seguridad de la Información aplicables, mediante el diligenciamiento de la sección de aplicabilidad de controles para los procesos y Direcciones Territoriales (periodicidad anual)		Formato de declaración de aplicabilidad de controles SOA – Asignación de controles a Procesos y DTs	Procesos y Direcciones Territoriales
Instrumento MSPI del MinTIC Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MinTIC)	**7.** Formular el plan de cultura y sensibilización SGSI	Oficina de Tecnologías de la Información	Formular o actualizar periódicamente el Plan de Cultura y Sensibilización en Seguridad de la Información (periodicidad anual)		Plan de cultura y sensibilización en Seguridad de la Información (SGSI)	Procesos y Direcciones Territoriales
Instrumento MSPI del MinTIC Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MinTIC)	**8.** Establecer Planes de Continuidad de Negocio	Todos los procesos y/o Direcciones Territoriales	Formular los planes de continuidad de negocio a partir del análisis de impacto operacional, teniendo en cuenta la Metodología de Continuidad de Negocio u Operación (periodicidad anual)		Registro de Planes de continuidad BCP por proceso Plan de recuperación ante desastres tecnológicos DRP (Documento interno Clasificado)	Comité Institucional de Gestión y Desempeño
HACER						
Instrumento MSPI del MinTIC Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MinTIC)	**9.** Realizar análisis de vulnerabilidades	Oficina de Tecnologías de la Información	Identificar y gestionar las vulnerabilidades de Seguridad en la Infraestructura Tecnológica de la Entidad. (periodicidad por demanda)		Informe de vulnerabilidades técnicas de Sistemas de Información y elementos de Infraestructura TI	Equipo de Sistemas de Información Equipo de Infraestructura TI Equipo de Seguridad de la Información

Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
						Equipo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT del MinTIC
Requerimientos registrados en la Mesa de Servicios Tecnológicos Formato Acuerdo de confidencialidad	**10.** Realizar la gestión y control de acceso a sistemas de información	Administradores de Sistemas de información	Ejecutar el Protocolo de Gestión de Acceso a Usuarios (periodicidad por demanda)		Registro de la gestión de casos en la mesa de servicios tecnológicos Formato Acuerdo de confidencialidad diligenciado	Procesos Direcciones Territoriales Entidades Externas con acuerdo de intercambio de información - SRNI
Alertas Ciberseguridad ColCERT Requerimientos y Eventos registrados en la Mesa de Servicios Tecnológicos	**11.** Gestionar plataformas de seguridad	Oficina de Tecnologías de la Información	Gestionar las herramientas de Seguridad de la Infraestructura Tecnológica de la Entidad (periodicidad semanal)		Informes técnicos de plataformas Gestión de casos en la mesa de servicios tecnológicos	Oficina de Tecnologías de la Información
Alertas Ciberseguridad ColCERT Requerimientos y Eventos registrados en la Mesa de Servicios Tecnológicos	**12.** Gestionar requerimientos o eventos de seguridad de la información	Oficina de Tecnologías de la Información	Atender casos reportados en la Mesa de Servicios Tecnológicos (periodicidad semanal)		Registro de la gestión de casos en la mesa de servicios tecnológicos	Procesos Direcciones Territoriales ColCERT del MinTIC
Alertas Ciberseguridad ColCERT Eventos registrados en la Mesa de Servicios Tecnológicos Formato de Registro de Incidentes de Seguridad diligenciado parcialmente	**13.** Gestionar los incidentes SGSI	Oficina de Tecnologías de la Información	Ejecutar el Procedimiento de Gestión de Incidentes (periodicidad por demanda)		Documentación de acciones en correo electrónico y/o mesa de servicios tecnológicos.	Procesos Direcciones Territoriales ColCERT del MinTIC Superintendencia de Industria y Comercio – SIC, en caso de involucrar Datos Personales

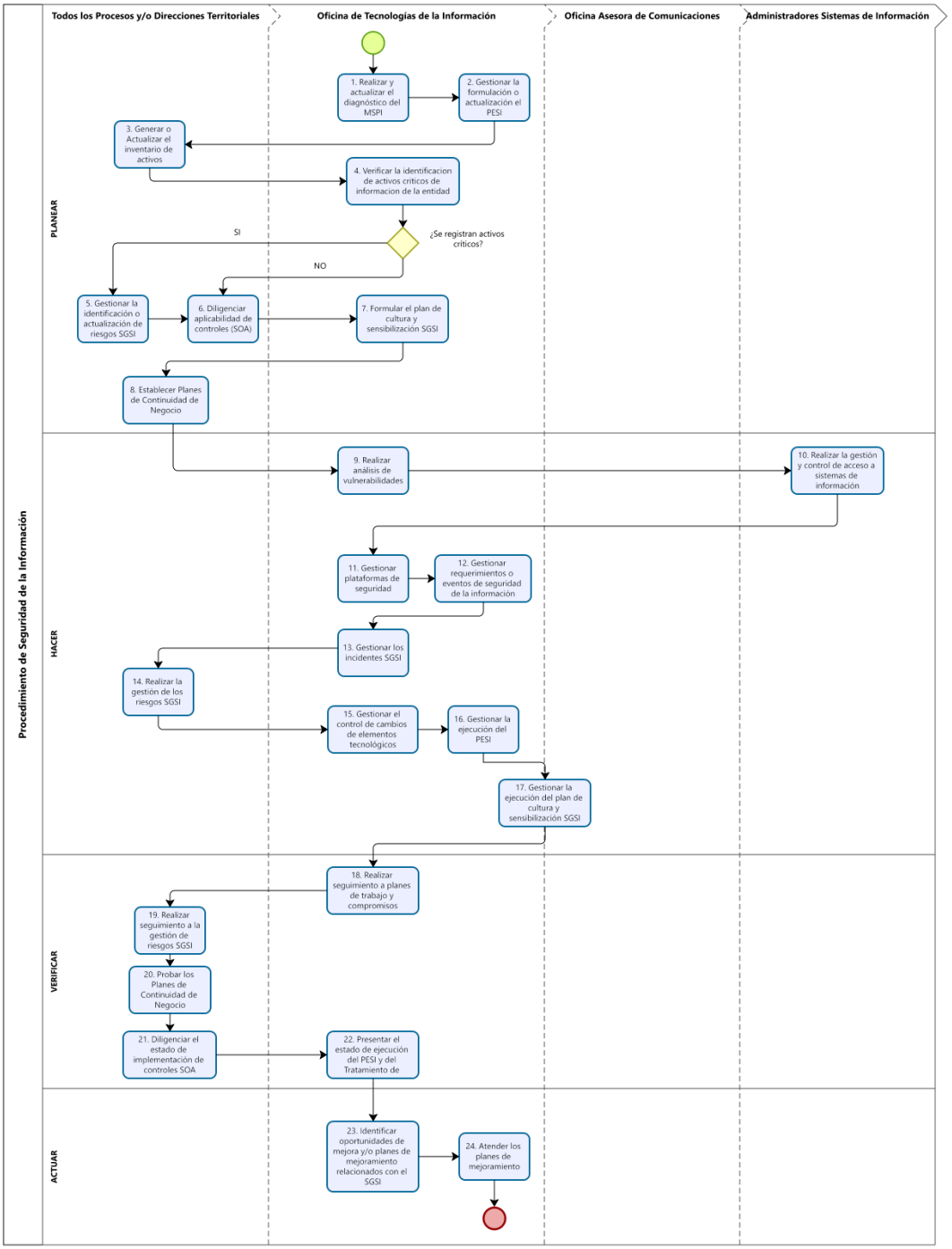
Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
Matriz de riesgos SGSI por Proceso y Riesgo tipo para las Direcciones Territoriales	**14.** Realizar la gestión de los riesgos SGSI	Todos los procesos y/o Direcciones Territoriales	Ejecutar controles y planes de tratamiento de los Riesgos SGSI (periodicidad cuatrimestral)		Soportes de ejecución de controles y planes de tratamiento a los riesgos SGSI	Oficina de Tecnologías de la Información Oficina de Control Interno
Solicitudes de cambio con Registro en la Mesa de Servicios Tecnológicos	**15.** Gestionar el control de cambios de elementos tecnológicos	Oficina de Tecnologías de la Información	Ejecutar el Protocolo de Gestión de Cambios de Tecnologías de la Información (periodicidad por demanda)		Formato de Gestión de cambios	Oficina de Tecnologías de la Información
Plan Estratégico de Seguridad de la información - PESI	**16.** Gestionar la ejecución del PESI	Oficina de Tecnologías de la Información	Gestionar la ejecución del Plan Estratégico de Seguridad de la Información PESI (Operación y Proyectos) (actividad permanente)		Soportes de ejecución del PESI: - Reporte indicador Plan de Acción - Soportes de ejecución Proyectos de Seguridad de la Información	Comité Institucional de Gestión y Desempeño Entes de Control Procesos y Direcciones Territoriales Departamento Administrativo para la Prosperidad Social
Plan de cultura y sensibilización en Seguridad de la Información (SGSI)	**17.** Gestionar la ejecución del plan de cultura y sensibilización SGSI	Oficina de Tecnologías de la Información Oficina Asesora de Comunicaciones	Ejecutar las actividades establecidas en el plan de cultura y sensibilización SGSI		Listas de asistencia a charlas de Seguridad de la información Flashes informativos o infografías enviadas en articulación con la Oficina Asesora de Comunicaciones	Procesos y Direcciones Territoriales
VERIFICAR						
Soportes de ejecución del PESI: Reporte indicador Plan de Acción	**18.** Realizar seguimiento a planes de trabajo y compromisos	Oficina de Tecnologías de la Información	Realizar seguimiento a las actividades ejecutadas relacionadas con el PESI, definición de controles y Plan de Cultura en Seguridad de la Información.		Actas de seguimiento en reuniones de Gobierno TI y en Seguimiento al PETI (Plan Estratégico de Tecnologías de la Información)	Comité Institucional de Gestión y Desempeño Entes de Control

Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
Soportes de ejecución Proyectos de Seguridad de la Información						Oficina de Control Interno
Soportes de ejecución de controles y planes de tratamiento a los riesgos SGSI	**19.** Realizar seguimiento a la gestión de riesgos SGSI	Todos los procesos y/o Direcciones Territoriales	Realizar la consolidación de evidencias generadas a partir de la ejecución de controles y planes de tratamiento de riesgos del SGSI (periodicidad cuatrimestral)		Informes de seguimiento periódico del tratamiento de riesgos de seguridad y privacidad de la información	Comité Institucional de Gestión y Desempeño Oficina de Tecnologías de la Información Oficina de Control Interno
Planes de continuidad BCP por proceso (Documento interno Clasificado) Plan de recuperación ante desastres tecnológicos DRP (Documento interno Clasificado)	**20.** Probar los Planes de Continuidad de Negocio	Todos los procesos y/o Direcciones Territoriales	Realizar y documentar las pruebas de continuidad de negocio, incluyendo las pruebas del Plan de Recuperación ante desastres tecnológicos – DRP (periodicidad por demanda)		Informes de ejecución de pruebas	Comité Institucional de Gestión y Desempeño Oficina de Tecnologías de la Información Oficina de Control Interno
Formato de declaración de aplicabilidad de controles SOA – El cual documenta la inclusión o exclusión de controles, asimismo la asignación de controles a Procesos y DTs	**21.** Diligenciar el estado de implementación de controles SOA	Todos los procesos y/o Direcciones Territoriales	Diligenciar la Declaración de aplicabilidad de controles, en cuanto al estado de implementación de cada control aplicable al proceso a la Dirección Territorial. Adicionalmente, consolidar los soportes de ejecución de los controles aplicables (periodicidad anual)		Formato de declaración de aplicabilidad de controles SOA – diligenciamiento del estado de implementación aplicable a cada Proceso y Dirección Territorial Formato de Bitácora Acceso Centro Cableado o Cómputo	Oficina de Control Interno Oficina de Tecnologías de la Información
Soportes de ejecución del PESI: Reporte indicador Plan de Acción	**22.** Presentar el estado de ejecución del PESI y del Tratamiento de Riesgos SGSI	Oficina de Tecnologías de la Información	Presentar los avances de la ejecución del PESI y del Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información ante el		Acta de comité	Comité Institucional de Gestión y Desempeño

Entradas	Actividad	Responsable	Descripción	PC*	Salidas	Cliente
Soportes de ejecución Proyectos de Seguridad de la Información			Comité Institucional de Gestión y Desempeño (periodicidad bimensual)			
ACTUAR						
Soportes de ejecución del PESI: Reporte indicador Plan de Acción Soportes de ejecución Proyectos de Seguridad de la Información	**23.** Identificar oportunidades de mejora y/o planes de mejoramiento relacionados con el SGSI	Oficina de Tecnologías de la Información	A partir de auditorías internas (Oficina de Control Interno) a mediante la verificación del cumplimiento de los controles aplicables en el SOA (periodicidad anual)		Informes de seguimiento o Auditorías técnicas internas Oportunidades de mejora Plan de mejoramiento	Oficina de Control Interno Oficina de Tecnologías de la Información Entes de Control
Informes de seguimiento o Auditorías técnicas internas Oportunidades de mejora Plan de mejoramiento	**24.** Atender los planes de mejoramiento	Oficina de Tecnologías de la Información	Ejecutar los planes de mejoramiento establecidos en el marco del SGSI (periodicidad anual)		Soportes de ejecución de las oportunidades de mejora y del plan de tratamiento	Oficina de Control Interno

Producto y/o Servicio Generado	Descripción del Producto y/o Servicio
Actualización y aprobación del PESI y seguimiento al cumplimiento de las metas del PESI. Lineamientos para la creación de Usuario en sistemas de información según protocolo, en articulación con procesos responsables. Generación del inventario de activos de información. Gestión de ejecución del plan Tratamiento Riesgos de Seguridad y privacidad de la Información implementado. Atención a incidentes de seguridad. Ejecución del Plan Estratégico de Seguridad de la Información. Pruebas del Plan de Recuperación de desastres tecnológicos.	El actual macro procedimiento de Seguridad de la Información involucra la actualización del Plan Estratégico de Seguridad de la Información. Así mismo, mediante el seguimiento periódico se documenta el avance en el cumplimiento de las metas del PESI establecidas. Por otra parte, este procedimiento integra lo relacionado a la creación de usuarios en sistemas de información, integrando el protocolo establecido tal fin. Adicionalmente, en articulación con los diferentes enlaces del Sistema Integrado de Gestión se realiza la actualización del inventario de activos y la actualización de los riesgos asociados al Sistema de Gestión de Seguridad de la Información – SGSI. Es importante indicar que, también involucra la gestión de ejecución del plan de tratamiento de Riesgos de Seguridad de la Información. Por último, se incluye la gestión de atención a eventos e incidentes de seguridad de la información. Lo anterior, en el marco de la ejecución del Plan Estratégico de Seguridad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Diagrama de flujo Procedimiento



Indicadores de gestión

A continuación, se presentan los indicadores de gestión asociados al procedimiento:

Actividad	Indicador Propuesto	Fórmula / Métrica	Periodicidad	Meta	Responsable
Diagnóstico MSPI	% de avance en el diligenciamiento del instrumento	(Evaluación de efectividad de controles / calificación objetivo) × 100	Semestral	80%	Oficina de Tecnologías de la Información
Ejecución del Plan Estratégico de Seguridad de la Información - PESI	Nivel de cumplimiento del PESI	(Actividades ejecutadas / Actividades planificadas) × 100	Anual	100%	Oficina de Tecnologías de la Información
Inventario de activos	% de activos identificados y clasificados	(Activos clasificados / Total activos) × 100 (Cantidad de procesos que reportan actualización de activos / Total procesos)	Anual	100%	Procesos
Gestión de riesgos	% de riesgos tratados	(Cantidad de controles y planes con evidencia de ejecución / Total de controles y planes) × 100	Cuatrimestral	90%	Procesos y Direcciones Territoriales
Aplicabilidad de controles (SOA)	% de controles implementados	(Controles implementados / Controles aplicables) × 100	Anual	80%	Procesos y Direcciones Territoriales
Cultura y sensibilización	% de participación en actividades	(funcionarios y contratistas que asistieron al menos a una charla de seguridad de la información / Total funcionarios y contratistas) × 100	Anual	20%	Procesos y Direcciones Territoriales
Gestión de incidentes	Tiempo promedio de respuesta a incidentes	Número de eventos o incidentes con atención acorde al ANS establecido / Número de incidentes X 100	Mensual	90%	Oficina de Tecnologías de la Información
Continuidad de negocio	% de pruebas exitosas de BCP y/o DRP	(Pruebas exitosas / Total pruebas realizadas) × 100	Anual	80%	Procesos
Planes de mejoramiento	% de acciones correctivas implementadas	(Acciones ejecutadas / Total acciones planificadas) × 100	Anual	90%	Oficina de Tecnologías de la Información

6. ANEXOS

Anexo 1: Formato Matriz Declaración de Aplicabilidad - SoA.
Anexo 2: Formato Plan de Cultura y Sensibilización en Seguridad de Información.
Anexo 3: Formato de Bitácora Acceso Centro Cableado o Cómputo.
Anexo 4: Procedimiento de Generación del Inventario de Activos de Información.
Anexo 5: Procedimiento de Gestión de Incidentes de Seguridad.
Anexo 6: Protocolo de Gestión de Cambios de Tecnologías de la Información.
Anexo 7: Protocolo de Gestión de Acceso a Usuarios.

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	03/06/2026	Creación del documento