PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

GOBERNACION DE NORTE DE SANTANDER.

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

Tabla de contenido

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Gobernación de Norte de Santander tiene como propósito establecer las acciones estratégicas, técnicas, organizacionales y operativas necesarias para garantizar la protección adecuada de los activos de información institucionales. Este plan constituye el instrumento operativo mediante el cual se materializa la aplicación de la Política de Seguridad y Privacidad de la Información, en cumplimiento de los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano.

En un entorno digital cada vez más complejo, donde la información representa uno de los principales activos estratégicos de la administración pública, resulta indispensable fortalecer las capacidades institucionales para proteger su confidencialidad, integridad, disponibilidad, privacidad y trazabilidad. En este contexto, el presente plan proporciona un marco integral para gestionar riesgos, establecer controles, responder a incidentes y fomentar una cultura organizacional orientada a la seguridad digital.

Este documento se alinea con el marco normativo nacional vigente, incluyendo la Ley 1581 de 2012 sobre Protección de Datos Personales, la Ley 1712 de 2014 de Transparencia y Acceso a la Información Pública, la Ley 1273 de 2009 sobre delitos informáticos, así como los estándares internacionales reconocidos como ISO/IEC 27001, ISO/IEC 27701 y las disposiciones del Gobierno Digital.

Asimismo, el plan establece mecanismos para asegurar el cumplimiento institucional de las políticas derivadas del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), promoviendo la mejora continua y garantizando que todos los actores involucrados (funcionarios, contratistas, proveedores y partes interesadas) actúen con responsabilidad y compromiso frente al uso seguro y ético de la información institucional.

Este plan es de aplicación obligatoria para todas las secretarias, dependencias, áreas, procesos y actores que interactúan con los activos de información de la Gobernación, y será revisado periódicamente para adaptarse a los cambios tecnológicos, normativos y organizacionales que impacten la seguridad y privacidad de la información.

1. JUSTIFICACIÓN

La información se ha consolidado como un activo estratégico fundamental para la operación, la toma de decisiones y la generación de valor público en las entidades del Estado. En este contexto, la Gobernación de Norte de Santander reconoce la importancia de establecer mecanismos integrales para proteger sus activos de información frente a riesgos internos y externos que puedan comprometer su confidencialidad, integridad, disponibilidad, trazabilidad y privacidad.

El creciente uso de tecnologías de la información y la digitalización de los procesos institucionales, junto con la necesidad de garantizar el cumplimiento del marco normativo vigente en materia de protección de datos personales, transparencia, seguridad digital y gobierno abierto, exige la adopción de medidas estructuradas que aseguren una gestión responsable y segura de la información institucional.

En este sentido, el Plan de Seguridad y Privacidad de la Información constituye un instrumento técnico y estratégico que permite la implementación efectiva de los lineamientos establecidos en la Política de Seguridad y Privacidad de la Información, bajo los principios y dimensiones del Modelo de Seguridad y Privacidad de la Información (MSPI), promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Este plan responde a la necesidad de establecer acciones sistemáticas que permitan mitigar los riesgos asociados a la gestión de la información, fortalecer las capacidades institucionales, garantizar la continuidad operativa, asegurar el cumplimiento normativo y fomentar una cultura organizacional orientada a la seguridad y privacidad digital en todas las dependencias de la Gobernación de Norte de Santander.

Además, permite disponer de un marco estructurado para la coordinación, asignación de responsabilidades, capacitación del talento humano, implementación de controles, atención de incidentes y mejora continua de los procesos asociados a

la seguridad de la información, garantizando así la confianza institucional y la protección de los derechos de los ciudadanos.

2. OBJETIVO

Establecer las acciones, mecanismos y controles necesarios para garantizar la protección integral de los activos de información de la Gobernación de Norte de Santander, mediante la implementación de medidas técnicas, organizacionales y procedimentales que aseguren su confidencialidad, integridad, disponibilidad, trazabilidad y privacidad, fomentando además una cultura institucional orientada a la gestión responsable de la información, en cumplimiento del marco normativo vigente y en armonía con los principios del Modelo de Seguridad y Privacidad de la Información (MSPI).

1.1 OBJETIVOS ESPECÍFICOS

- Establecer controles técnicos, organizacionales y procedimentales que permitan proteger los activos de información institucional frente a amenazas internas y externas, garantizando su confidencialidad, integridad, disponibilidad, trazabilidad y privacidad.
- Implementar un modelo de gestión de riesgos de seguridad de la información, que permita identificar, evaluar, tratar y monitorear los riesgos asociados a los activos de información y los procesos institucionales.
- Fortalecer las capacidades institucionales de respuesta ante incidentes de seguridad, mediante la adopción de procedimientos para su detección, análisis, tratamiento, documentación y prevención.
- Promover la cultura organizacional de seguridad y privacidad de la información, mediante programas de formación, sensibilización y concienciación dirigidos a funcionarios, contratistas y demás partes interesadas.
- Asegurar el cumplimiento del marco normativo vigente en materia de protección de datos personales, transparencia, delitos informáticos y seguridad digital, conforme a las leyes nacionales, el MSPI y estándares internacionales como ISO/IEC 27001.
- Establecer políticas derivadas y procedimientos específicos que regulen el tratamiento de la información en todas las etapas de su ciclo de vida, desde su generación hasta su disposición final.
- Garantizar la continuidad operativa institucional y la recuperación ante desastres, mediante la integración de lineamientos de seguridad en los planes de continuidad del negocio y recuperación de la información.
- Implementar mecanismos de auditoría, monitoreo y evaluación continua, que permitan verificar el cumplimiento del plan, identificar desviaciones y generar acciones de mejora.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Gobernación de Norte de Santander aplica a todos los activos de información, procesos, personas, tecnologías, infraestructura y servicios que intervienen en la gestión, almacenamiento, procesamiento, transmisión y disposición final de la información institucional, sin importar su formato o medio de almacenamiento.

Este plan abarca de manera integral los siguientes componentes:

- **Procesos institucionales:** Misionales, estratégicos, de apoyo y de evaluación, en los cuales se gestiona información que requiere ser protegida.
- **Activos de información:** Documentos, bases de datos, sistemas de información, aplicaciones, plataformas tecnológicas, redes, equipos informáticos y demás recursos que contienen o gestionan información institucional.
- **Usuarios:** Funcionarios públicos, contratistas, pasantes, proveedores, terceros y cualquier parte interesada que tenga acceso, gestione o interactúe con los activos de información de la Gobernación.
- **Sistemas tecnológicos:** Equipos de cómputo, servidores, redes, aplicaciones, sistemas operativos, dispositivos móviles, plataformas digitales y servicios en la nube que soportan los procesos institucionales.
- **Entornos físicos y virtuales:** Instalaciones, oficinas, centros de datos y ambientes tecnológicos donde se procesan, resguardan o consultan activos de información.
- **Fases del ciclo de vida de la información:** Desde su creación o recolección, almacenamiento, procesamiento, consulta, distribución, transferencia, hasta su eliminación o disposición final.

Este plan tiene aplicación obligatoria para todas las dependencias, secretarías, áreas, unidades administrativas y personal vinculado a la Gobernación de Norte de Santander, y deberá ser también atendido por las partes externas contratadas o asociadas que tengan relación con los activos de información institucionales.

Asimismo, el alcance del plan será objeto de revisión periódica para garantizar su alineación con los cambios organizacionales, tecnológicos, normativos o de contexto que puedan impactar la seguridad y privacidad de la información.

4. MARCO NORMATIVO Y REFERENCIAL

Norma / Referencia	Descripción
Ley 1581 de 2012	Establece disposiciones generales para la protección de datos personales en Colombia. Define principios, derechos, deberes y procedimientos aplicables al tratamiento de datos.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012, especialmente sobre la autorización para el tratamiento de datos recolectados antes de su expedición.
Ley 1712 de 2014	Ley de Transparencia y Acceso a la Información Pública. Establece el deber de garantizar el acceso ciudadano a la información institucional bajo condiciones de seguridad.
Ley 1266 de 2008	Regula el habeas data financiero, aplicable al tratamiento de información relacionada con el historial crediticio y datos financieros.
Ley 1273 de 2009	Establece el marco penal para la protección de la información y los sistemas informáticos, tipificando delitos informáticos y sanciones.
Modelo de Seguridad y Privacidad de la	Modelo orientador del Estado colombiano que define principios, dimensiones y acciones para garantizar la

Información (MSPI)	seguridad y privacidad de la información en entidades públicas.
Decreto 1008 de 2018 / CONPES 3920 de 2018	Política de Gobierno Digital que establece lineamientos para la transformación digital del Estado, incluyendo la dimensión de seguridad digital.
ISO/IEC 27001	Norma internacional que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) estructurado y eficaz.
ISO/IEC 27701:2022	Extensión de la norma ISO/IEC 27001 enfocada en la gestión de la privacidad de la información y el tratamiento de datos personales.
Ley 1341 de 2009 / Ley 1978 de 2019	Marco regulatorio para las TIC en Colombia, define principios orientadores, derechos digitales y deberes del Estado en materia de conectividad y transformación digital.
Ley 1437 de 2011	Código de Procedimiento Administrativo. Define disposiciones sobre el manejo, archivo, confidencialidad y acceso a la información administrativa.
Circular 005 de 2020 – SIC	Establece orientaciones sobre medidas técnicas, administrativas y jurídicas para garantizar el cumplimiento de la Ley 1581 de 2012 y la protección de datos personales.

5. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Para la implementación del Plan de Seguridad y Privacidad de la Información de la Gobernación de Norte de Santander, se adopta la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistema) como marco de referencia técnico para la identificación, clasificación, valoración y tratamiento de los activos de información y los riesgos asociados.

MAGERIT se justifica como metodología principal por las siguientes razones:

- **Alineación con el enfoque de gestión del riesgo del MSPI:** El Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano promueve el análisis estructurado de riesgos sobre los activos de información. MAGERIT permite operacionalizar esta dimensión de forma metódica y verificable.
- **Cobertura integral de los activos de información:** MAGERIT proporciona una clasificación jerárquica y estructurada de los activos primarios y de soporte (información, servicios, aplicaciones, infraestructuras, personal, etc.), lo cual facilita una visión completa del ecosistema tecnológico y documental institucional.
- **Valoración objetiva de los impactos sobre los principios CID:** La metodología permite evaluar cada activo según su nivel de Confidencialidad, Integridad y Disponibilidad, facilitando el diseño de controles proporcionales al nivel de riesgo detectado.
- **Facilidad de integración con sistemas de gestión normativos:** MAGERIT es compatible con marcos de referencia internacionales como ISO/IEC 27001, ISO/IEC 27005 e incluso con lineamientos del Gobierno Digital, facilitando el cumplimiento normativo y la integración con auditorías o sistemas de calidad.
- **Priorización de riesgos y optimización de recursos:** La metodología permite focalizar esfuerzos en aquellos activos y riesgos que representan mayor impacto institucional, mejorando la eficiencia en la asignación de controles y recursos de protección.
- **Facilidad de documentación, trazabilidad y mejora continua:** MAGERIT proporciona herramientas para mantener inventarios, fichas de activos y matrices de valoración actualizadas, apoyando la trazabilidad de las decisiones y la revisión periódica de los riesgos.

- **Adopción institucional progresiva:** La metodología permite una implementación progresiva y adaptable a las capacidades organizacionales de la Gobernación, siendo viable su incorporación por fases, sin que se comprometa su robustez metodológica.

6. IDENTIFICACIÓN

En el marco del análisis de riesgos bajo la metodología MAGERIT, los activos de información se identifican como aquellos elementos que tienen valor para la Gobernación de Norte de Santander y que son fundamentales para el cumplimiento de sus funciones, el soporte a los procesos institucionales y la prestación de servicios a la ciudadanía.

Los activos se agrupan en categorías jerárquicas, según la estructura lógica establecida por MAGERIT:

Categoría de Activo	Descripción
Activos Primarios	Información y servicios directamente relacionados con los procesos misionales, estratégicos y de apoyo de la Gobernación.
Activos de Soporte	Recursos que dan soporte al funcionamiento de los activos primarios, tales como aplicaciones, infraestructuras tecnológicas, comunicaciones, instalaciones, personal, etc.

7. TIPOLOGÍA DE ACTIVOS

Tipo de Activo	Descripción
Información	Documentos físicos y electrónicos, bases de datos, expedientes, registros históricos, formularios digitales.
Servicios	Trámites en línea, sistemas de gestión financiera, gestión documental, servicios al ciudadano.
Aplicaciones	Software institucional, herramientas ofimáticas, plataformas web.
Equipos	Servidores, estaciones de trabajo, portátiles, impresoras, dispositivos móviles.
Infraestructura	Cableado estructurado, centros de datos, dispositivos de red, sistemas de energía y climatización.
Comunicaciones	Internet, redes LAN/WAN, correo electrónico, VPN.

Personal	Funcionarios, contratistas, técnicos operativos y administrativos.
Instalaciones	Oficinas, archivos físicos, centros de cómputo, áreas restringidas.

8. CLASIFICACIÓN DE ACTIVOS SEGÚN VALORACIÓN DE SEGURIDAD

Cada activo identificado será valorado con base en los tres principios fundamentales de seguridad de la información: Confidencialidad, Integridad y Disponibilidad (CID). MAGERIT propone utilizar una escala de valoración (Alta, Media, Baja) para cada criterio.

Criterio	Definición
Confidencialidad	Grado en que la información debe ser protegida frente al acceso no autorizado.
Integridad	Grado de importancia en la exactitud, veracidad y completitud de la información.

Disponibilidad	Grado en que la información debe estar disponible en tiempo y forma cuando se requiera.

9. RELACIÓN CON PROCESOS CRÍTICOS

Cada activo deberá asociarse a los procesos que apoya, identificando su criticidad y permitiendo así establecer medidas de protección proporcionales a su importancia para la continuidad del servicio.

10. ANÁLISIS Y GESTIÓN DE RIESGOS

11. ENFOQUE GENERAL

La Gestión de Riesgos de Seguridad y Privacidad de la Información en la Gobernación de Norte de Santander tiene como propósito identificar, valorar y tratar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información institucional, garantizando la continuidad de los procesos y el cumplimiento del marco normativo vigente.

Para tal fin, se adopta como referencia metodológica el enfoque propuesto por MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), que permite desarrollar un proceso estructurado, sistemático y trazable para el análisis, evaluación, control y seguimiento de los riesgos.

12. ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS

Etapa	Descripción
1. Identificación de Activos	Determinar qué activos (información, servicios, aplicaciones, infraestructuras, personal) deben ser protegidos.
2. Valoración de Activos	Estimar la importancia de cada activo en función de su Confidencialidad, Integridad y Disponibilidad (CID).

3. Identificación de Amenazas y Vulnerabilidades	Establecer los posibles escenarios que pueden explotar debilidades en los activos identificados.
4. Valoración del Riesgo	Evaluar el impacto potencial y la probabilidad de ocurrencia, permitiendo calcular el nivel de riesgo.
5. Evaluación y Tratamiento del Riesgo	Definir medidas preventivas, correctivas o compensatorias, priorizando los controles según el nivel de riesgo.
6. Aceptación del Riesgo Residual	Documentar los riesgos que, después de aplicar controles, se consideran aceptables bajo el criterio institucional.
7. Monitoreo y Revisión	Verificar periódicamente la evolución del riesgo y la efectividad de los controles implementados.

13. CLASIFICACIÓN DE RIESGOS

Se establecerá una matriz de valoración de riesgos con criterios como:

- Probabilidad de ocurrencia: Baja / Media / Alta
- Impacto potencial: Bajo / Medio / Alto
- Nivel de riesgo: Bajo / Medio / Alto / Crítico

14. TRATAMIENTO DEL RIESGO

Las opciones de tratamiento que se considerarán son:

- Mitigar: Implementar controles para reducir la probabilidad o impacto.
- Transferir: Derivar el riesgo a un tercero (ej. seguros o outsourcing).
- Evitar: Eliminar la causa del riesgo (cambio en el proceso).
- Aceptar: Reconocer el riesgo y asumirlo bajo control.

15. HERRAMIENTAS Y DOCUMENTACIÓN APOYADA

- Inventario y clasificación de activos.
- Matriz de riesgos y controles.
- Ficha de tratamiento del riesgo.
- Registro de incidentes.
- Indicadores de efectividad de los controles.

16. RESPONSABILIDADES

- El Equipo de Seguridad de la Información coordinará el proceso de gestión de riesgos.
- Cada líder de dependencia de la Gobernación será responsable de identificar y reportar riesgos propios del proceso que administra.
- La Secretaría de Tecnologías de la Información y las Comunicaciones brindará soporte técnico y metodológico.

17. ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN

La Gobernación de Norte de Santander, en el marco de su Política de Seguridad y Privacidad de la Información, adopta un conjunto de estrategias estructuradas e integrales orientadas a proteger los activos de información institucional y reducir los riesgos que puedan afectar su confidencialidad, integridad, disponibilidad, trazabilidad y privacidad.

Estas estrategias se definen con base en los principios del Modelo de Seguridad y Privacidad de la Información (MSPI) y están alineadas con el proceso de análisis y gestión de riesgos desarrollado bajo la metodología MAGERIT.

18. ESTRATEGIAS TÉCNICAS

- Implementación de controles de acceso físico y lógico a los sistemas de información y recursos tecnológicos.
- Uso de herramientas de autenticación robusta, cifrado de datos y mecanismos de respaldo.
- Protección perimetral mediante firewalls, antivirus, sistemas de detección y prevención de intrusos (IDS/IPS) y monitoreo continuo.
- Aplicación de actualizaciones y parches de seguridad de manera oportuna en sistemas y aplicaciones.
- Control de dispositivos externos y medios de almacenamiento removibles.
- Seguridad en redes, protocolos y canales de transmisión de información.

19. ESTRATEGIAS ORGANIZACIONALES

- Establecimiento de roles y responsabilidades claras en la gestión de la seguridad de la información.
- Creación y fortalecimiento del Equipo de Seguridad de la Información, coordinado por la Secretaría TIC.

- Inclusión de cláusulas de seguridad en contratos con terceros y proveedores de servicios tecnológicos.
- Diseño de políticas derivadas específicas que regulen el ciclo de vida de la información y los controles asociados.

20. ESTRATEGIAS DE GESTIÓN DEL RIESGO

- Aplicación sistemática de la metodología MAGERIT para el análisis y tratamiento de riesgos.
- Priorización de los activos críticos de información y aplicación proporcional de medidas de protección.
- Registro, valoración y tratamiento de riesgos residuales.

21. ESTRATEGIAS DE CONCIENCIACIÓN Y FORMACIÓN

- Desarrollo de programas permanentes de capacitación y sensibilización para funcionarios, contratistas y partes interesadas.
- Promoción de una cultura organizacional basada en buenas prácticas de seguridad digital.
- Realización de simulacros, pruebas de phishing, campañas educativas y difusión de guías institucionales.

22. ESTRATEGIAS DE GESTIÓN DE INCIDENTES Y CONTINUIDAD

- Implementación de un procedimiento estructurado para la gestión de incidentes de seguridad.
- Documentación, análisis, reporte y seguimiento de los eventos que afecten o puedan afectar los activos de información.
- Integración de la seguridad de la información en los planes de continuidad del negocio y recuperación ante desastres.

23. ESTRATEGIAS DE EVALUACIÓN Y MEJORA CONTINUA

- Realización periódica de auditorías internas sobre el cumplimiento del SGSPI.
- Definición de indicadores de gestión y mecanismos de control para evaluar la eficacia de las medidas implementadas.
- Revisión continua de políticas, procedimientos y controles, en función de los cambios normativos, tecnológicos y organizacionales.

24. PROTECCIÓN DE DATOS PERSONALES

La Gobernación de Norte de Santander, en cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y el marco establecido en la Política de Seguridad y Privacidad de la Información, adopta las medidas necesarias para garantizar el adecuado tratamiento y protección de los datos personales de los ciudadanos, funcionarios, contratistas y demás titulares cuyos datos sean gestionados por la entidad.

25. PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales en la Gobernación se realizará de conformidad con los siguientes principios:

- **Legalidad:** Todo tratamiento debe realizarse conforme a la ley.
- **Finalidad:** El uso de los datos debe obedecer a una finalidad legítima, informada y específica.
- **Libertad:** El tratamiento solo podrá realizarse con el consentimiento, autorización o mandato legal.
- **Transparencia:** El titular puede conocer en todo momento el uso de su información.
- **Seguridad:** Se adoptarán medidas técnicas, humanas y administrativas para proteger los datos.
- **Acceso y Circulación Restringida:** El acceso solo será permitido a quienes cuenten con autorización.
- **Confidencialidad:** Todos los que intervienen en el tratamiento están obligados a mantener reserva.

26. MEDIDAS DE PROTECCIÓN IMPLEMENTADAS

La Gobernación adopta medidas de protección conforme a los siguientes aspectos:

- Controles de acceso a bases de datos y sistemas que gestionan datos personales.
- Cifrado de información y protocolos seguros para transmisión de datos.
- Políticas y procedimientos específicos para el almacenamiento, tratamiento y disposición final de los datos.
- Mecanismos de autorización informada para la recolección y tratamiento de datos.
- Análisis de riesgos y controles específicos sobre los activos que contienen información personal.

27. DERECHOS DE LOS TITULARES DE DATOS

Los titulares de los datos personales tienen derecho a:

- Conocer, actualizar y rectificar sus datos.
- Solicitar prueba de autorización.
- Ser informados sobre el uso de sus datos.
- Presentar quejas ante la SIC.
- Revocar la autorización y/o solicitar la supresión de los datos.
- Acceder gratuitamente a sus datos personales.

28. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

La Gobernación de Norte de Santander a través de la política de tratamiento de datos estableció como responsable del Tratamiento de Datos Personales a la oficina de Relacionamiento con la ciudadanía, quien coordinará las acciones necesarias para el cumplimiento normativo, la atención de solicitudes de los titulares y el seguimiento a las medidas de seguridad asociadas al tratamiento de datos.

29. PROCEDIMIENTOS Y ATENCIÓN DE SOLICITUDES

Se garantizará a los titulares el acceso a canales formales y procedimientos claros para ejercer sus derechos, conforme a lo establecido para el Tratamiento de Datos Personales, el cual forma parte de las políticas derivadas del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

30. GESTIÓN DE INCIDENTES DE SEGURIDAD

La Gestión de Incidentes de Seguridad de la Información en la Gobernación de Norte de Santander tiene como propósito establecer un procedimiento sistemático, oportuno y eficaz para la detección, análisis, notificación, tratamiento y documentación de eventos o incidentes que comprometan la seguridad, privacidad o disponibilidad de los activos de información institucional.

Esta gestión es un componente fundamental del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y se encuentra alineada con los principios del Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas internacionales (ISO/IEC 27035 – Gestión de Incidentes).

31. DEFINICIÓN DE INCIDENTE DE SEGURIDAD

Se entiende por incidente de seguridad de la información cualquier evento confirmado o sospechoso que afecte, o pueda afectar, la confidencialidad, integridad, disponibilidad, privacidad o trazabilidad de los activos de información institucionales. Estos incidentes pueden ser provocados por errores humanos, fallos técnicos, accesos no autorizados, malware, ataques externos, entre otros.

32. TIPOLOGÍA DE INCIDENTES COMUNES

- Accesos no autorizados a sistemas o datos.
- Pérdida, fuga o divulgación no autorizada de información.
- Daños o alteraciones no autorizadas a bases de datos o archivos.
- Robo o extravío de dispositivos con información institucional.
- Ataques informáticos (phishing, malware, ransomware, etc.).
- Fallos en la infraestructura tecnológica que comprometan la información.
- Incumplimiento de las políticas de seguridad por parte de usuarios.

33. ETAPAS DEL PROCESO DE GESTIÓN DE INCIDENTES

Etapa	Descripción
• **1. Detección**	Identificación de un posible incidente a través de alertas, reportes o monitoreo.
• **2. Notificación**	Comunicación inmediata del incidente al Equipo de Seguridad de la Información o al canal designado.
• **3. Análisis y Clasificación**	Verificación del evento, determinación del tipo de incidente y su criticidad.
4. Contención	Medidas para limitar la propagación o impacto del incidente.
• **5. Resolución y Recuperación**	Aplicación de acciones correctivas y restauración de los servicios afectados.
• **6. Documentación y Registro**	Consolidación del incidente en el registro oficial, lecciones aprendidas y evidencias.
• **7. Mejora y Prevención**	Análisis post-incidente, identificación de causas raíz y recomendaciones de mejora.

34. ROLES Y RESPONSABLES

- Usuarios: Identificar y reportar de inmediato cualquier incidente de seguridad.
- Líderes de dependencia: Apoyar la atención del incidente y facilitar el flujo de información.
- Equipo de Seguridad de la Información: Coordinar el tratamiento, análisis y documentación de los incidentes.
- Secretaría de Tecnologías de la Información y las Comunicaciones (SETIC): Aplicar medidas técnicas de respuesta y recuperación.
- Comité de Seguridad de la Información: Evaluar incidentes críticos y validar medidas de mejora.

35. REGISTRO Y SEGUIMIENTO DE INCIDENTES

Todos los incidentes deben ser registrados en el formato MA-TC-PR04-FO-01 Registro de Incidentes de Seguridad de la Información, el cual debe contener al menos:

- Fecha y hora del incidente.
- Área y sistema afectado.
- Descripción del incidente.
- Clasificación de la gravedad (bajo, medio, alto, crítico).
- Acciones tomadas.
- Responsables.
- Estado del incidente (abierto, en análisis, resuelto).
- Lecciones aprendidas y acciones preventivas.

36. EVALUACIÓN Y MEJORA CONTINUA

La Gobernación evaluará periódicamente la gestión de incidentes para:

- Identificar tendencias o patrones recurrentes.
- Mejorar los controles preventivos.
- Actualizar procedimientos y fortalecer la cultura de reporte y respuesta.

37. PLAN DE FORMACIÓN Y SENSIBILIZACIÓN

El Plan de Formación y Sensibilización en Seguridad y Privacidad de la Información tiene como propósito promover una cultura organizacional orientada a la protección de los activos de información de la Gobernación de Norte de Santander, asegurando que todos los funcionarios, contratistas, proveedores y demás partes interesadas comprendan y apliquen buenas prácticas en el uso seguro y responsable de los recursos tecnológicos e informáticos.

Este plan se enmarca en los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Seguridad y Privacidad de la Información y los estándares internacionales como ISO/IEC 27001 y 27002, en lo que respecta a concienciación y capacitación continua.

38. OBJETIVOS DEL PLAN

- Desarrollar competencias en los funcionarios sobre los principios, normativas y prácticas de seguridad de la información.
- Sensibilizar sobre los riesgos asociados al manejo inadecuado de la información institucional.
- Fomentar el cumplimiento de la política institucional y el uso adecuado de los activos tecnológicos.
- Promover el reporte oportuno de incidentes y el autocuidado de la información.
- Disminuir los riesgos derivados del factor humano en los procesos institucionales.

39. PÚBLICO OBJETIVO

- Funcionarios de planta y provisionales.
- Contratistas administrativos y técnicos.
- Pasantes y personal en misión.
- Proveedores de servicios tecnológicos.
- Partes interesadas externas con acceso a sistemas de información.

40. CONTENIDOS FORMATIVOS PROPUESTOS

Temática	Descripción
Introducción a la Seguridad y Privacidad de la Información	Conceptos fundamentales, políticas institucionales y responsabilidades.
Manejo adecuado de contraseñas y autenticación segura	Recomendaciones prácticas y políticas institucionales.
Buenas prácticas en el uso de correo electrónico y navegación segura	Prevención del phishing, malware y pérdida de información.
Protección de datos personales	Principios de la Ley 1581 de 2012 y procedimientos institucionales.
Reporte y gestión de incidentes de seguridad	Procedimiento institucional y canales de atención.
Clasificación y tratamiento de la información	Niveles de sensibilidad y controles aplicables.
Seguridad en dispositivos móviles y trabajo remoto	Medidas de protección en entornos fuera de oficina.

41. ESTRATEGIAS DE FORMACIÓN Y SENSIBILIZACIÓN

- Jornadas presenciales y virtuales de capacitación.
- Cursos auto-formativos en plataformas institucionales.
- Boletines digitales, infografías y material divulgativo.
- Campañas temáticas periódicas (ej. mes de la ciberseguridad).
- Simulacros y ejercicios de concienciación (phishing simulado, cuestionarios, etc.).
- Incorporación de módulos de seguridad en inducciones institucionales.

42. EVALUACIÓN Y SEGUIMIENTO

- Registro de participación y cumplimiento de capacitaciones.
- Evaluación de conocimientos mediante pruebas cortas o encuestas.
- Indicadores de gestión como: tasa de cobertura, nivel de satisfacción y mejora en el reporte de incidentes.
- Retroalimentación periódica para ajustar contenidos y metodologías.

43. RESPONSABLES

- **Secretaría de Tecnologías de la Información y las Comunicaciones (SETIC):** Coordinación general del plan y diseño de contenidos.
- **Equipo de Seguridad de la Información:** Apoyo técnico y seguimiento.
- **Líderes de proceso / jefes de dependencia:** Socialización interna y verificación de participación.
- **Comité de Seguridad y Privacidad de la Información:** Monitoreo del cumplimiento y alineación con el SGSPI.

44. PLAN DE AUDITORÍA Y SEGUIMIENTO

El Plan de Auditoría y Seguimiento tiene como objetivo establecer los mecanismos que permitan verificar el cumplimiento, efectividad y mejora continua de la Política de Seguridad y Privacidad de la Información, así como de los controles, procedimientos y actividades implementadas en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de la Gobernación de Norte de Santander.

Este plan se desarrolla en concordancia con las recomendaciones del Modelo de Seguridad y Privacidad de la Información (MSPI) y los controles de auditoría definidos en la norma ISO/IEC 27001, garantizando una gestión transparente, medible y sostenible de la seguridad de la información.

45. OBJETIVOS DEL PLAN DE AUDITORÍA Y SEGUIMIENTO

- Evaluar el grado de cumplimiento de la Política y los planes derivados del SGSPI.
- Verificar la implementación y efectividad de los controles técnicos, organizacionales y procedimentales.
- Identificar brechas, vulnerabilidades, no conformidades y oportunidades de mejora.
- Garantizar la trazabilidad, actualización y mejora continua del sistema.
- Facilitar la preparación de auditorías externas, inspecciones o evaluaciones institucionales.

46. TIPOS DE AUDITORÍA Y EVALUACIÓN

Tipo de Evaluación	Descripción
Auditoría interna	Ejercicio periódico realizado por personal designado o equipos independientes, con enfoque preventivo y correctivo.
Autoevaluaciones	Evaluaciones internas realizadas por los responsables de las dependencias, mediante listas de verificación o formularios.
Auditoría externa	Evaluación especializada realizada por terceros, ya sea por entes de control, entidades certificadoras o auditores contratados.
Seguimiento de acciones correctivas	Verificación del cierre efectivo de hallazgos o recomendaciones derivadas de auditorías anteriores.

47. ÁMBITOS DE EVALUACIÓN

- Cumplimiento normativo (Leyes 1581, 1712, 1273, etc.).
- Cumplimiento de las políticas derivadas del SGSPI.
- Gestión de riesgos e incidentes.
- Protección de datos personales.
- Clasificación y tratamiento de la información.
- Controles de acceso, monitoreo y trazabilidad.

- Formación y concienciación del personal.
- Planes de continuidad y recuperación ante desastres.

48. INSTRUMENTOS DE SEGUIMIENTO

- Listas de verificación / checklists.
- Indicadores de cumplimiento.
- Formatos de hallazgos y acciones correctivas.
- Informes periódicos al Comité de Seguridad y Privacidad de la Información.
- Registros de auditorías internas y externas.

49. PERIODICIDAD

Las auditorías internas deberán programarse al menos una vez al año, o cuando se identifiquen cambios relevantes en los procesos, infraestructura tecnológica, estructura organizacional o marco normativo. Las autoevaluaciones podrán realizarse de forma trimestral o semestral, según la dinámica institucional.

50. RESPONSABLES

- **Equipo de Seguridad de la Información:** Coordinación del proceso de auditoría y seguimiento.
- **SETIC:** Apoyo técnico y gestión de evidencias.
- **Líderes de proceso:** Autoevaluación y soporte en auditorías.
- **Comité de Seguridad y Privacidad de la Información:** Análisis de resultados y toma de decisiones.
-

51. MEJORA CONTINUA

Los resultados de las auditorías serán insumo para la actualización de políticas, procedimientos y controles. Se deberá implementar un plan de mejora continua, con acciones priorizadas, responsables y fechas de cumplimiento, lo cual permitirá mantener vigente y eficaz el SGSPI.

52. PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES (BCP / DRP)

El Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP) de la Gobernación de Norte de Santander establece las estrategias, procedimientos y recursos necesarios para asegurar la disponibilidad de los procesos críticos, la recuperación de los activos de información y la restauración de los servicios institucionales ante eventos que interrumpan su funcionamiento normal.

Este plan forma parte integral del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y busca garantizar la resiliencia institucional frente a amenazas tecnológicas, físicas, humanas o naturales.

53. OBJETIVOS DEL BCP / DRP

- Asegurar la continuidad operativa de los procesos críticos de la Gobernación.
- Minimizar el impacto institucional, legal y reputacional ante incidentes disruptivos.
- Garantizar la disponibilidad y recuperación de los activos de información afectados.
- Proteger los derechos de los ciudadanos y partes interesadas.
- Reducir los tiempos de inactividad y facilitar la toma de decisiones ante emergencias.

54. ALCANCE DEL PLAN

Este plan aplica a:

- Procesos misionales, estratégicos y de apoyo.

- Activos de información críticos (sistemas, bases de datos, servidores).
- Infraestructura tecnológica y comunicaciones.
- Personal clave y recursos de soporte institucional.

55. FASES DEL BCP / DRP

Fase	Descripción
Análisis de Impacto al Negocio (BIA)	Identificación de procesos críticos, tiempos máximos de interrupción (MTD) y recursos necesarios para su recuperación.
Evaluación de riesgos	Identificación de amenazas que pueden afectar la disponibilidad de los procesos y activos tecnológicos.
Estrategias de continuidad	Definición de procedimientos alternos, redundancias tecnológicas, recursos de respaldo y planes de contingencia.
Plan de recuperación ante desastres	Procedimientos para recuperar sistemas, datos e infraestructura tras una contingencia (incluye backups, DRP y reinicio de operaciones).
Pruebas y simulacros	Ejecución periódica de simulaciones para validar los tiempos, recursos y protocolos definidos.
Mantenimiento y actualización	Revisión regular del plan ante cambios en procesos, tecnologías o estructura organizacional.

56. COMPONENTES ESENCIALES DEL PLAN

- Inventario de procesos y activos críticos.
- Asignación de roles y responsabilidades.
- Documentación de procedimientos alternos.
- Mecanismos de respaldo (backups) y recuperación.
- Protocolos de comunicación institucional ante incidentes.
- Planes de evacuación y contingencia física.

57. ROLES Y RESPONSABLES

Rol	Responsabilidades
Equipo de Continuidad / Seguridad de la Información	Coordinación general del plan y ejecución de procedimientos ante incidentes.
Secretaría TIC	Recuperación tecnológica, respaldo de sistemas y activación del DRP.
Líderes de proceso	Implementación de procedimientos alternos para asegurar la continuidad operativa.
Comité de Seguridad de la Información	Aprobación, seguimiento y evaluación del plan.

58. INDICADORES DE EFECTIVIDAD

- Tiempo de respuesta ante incidentes (RTO).
- Nivel de recuperación de datos (RPO).
- Frecuencia de pruebas del plan.
- Grado de cumplimiento del plan ante simulacros.
- Tiempo total de restablecimiento del servicio.

59. RECURSOS NECESARIOS

Para la implementación efectiva del Plan de Seguridad y Privacidad de la Información de la Gobernación de Norte de Santander, se requiere la asignación adecuada de recursos humanos, técnicos, financieros, administrativos y normativos, que garanticen el cumplimiento de las acciones definidas, la sostenibilidad del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), y la consolidación de una cultura organizacional orientada a la protección de los activos de información.

A continuación, se detallan los recursos necesarios:

60. RECURSOS HUMANOS

- Personal técnico especializado en seguridad de la información, infraestructura tecnológica y protección de datos.
- Integración formal del Equipo de Seguridad de la Información, con funciones definidas y dedicación institucional.
- Funcionarios capacitados en buenas prácticas de seguridad, gestión de incidentes, tratamiento de datos personales y continuidad del negocio.
- Apoyo administrativo para la ejecución de planes, capacitaciones y seguimiento.

61. RECURSOS TÉCNICOS

- Sistemas de gestión de incidentes y monitoreo de seguridad (SIEM).
- Herramientas de respaldo y recuperación de datos.
- Infraestructura de red segura (firewalls, IDS/IPS, VPN, controles de acceso).
- Plataformas tecnológicas para formación, gestión documental y seguimiento.
- Software para control de acceso, cifrado, auditoría y cumplimiento normativo.
- Equipamiento adecuado para pruebas, copias de seguridad, contingencias y recuperación ante desastres.

62. RECURSOS FINANCIEROS

- Presupuesto específico para la adquisición, renovación y mantenimiento de soluciones tecnológicas.
- Recursos financieros para el diseño y ejecución de programas de capacitación.
- Recursos destinados a auditorías, consultorías especializadas o certificaciones del SGSPI.
- Asignación presupuestal para contingencias y medidas correctivas ante eventos disruptivos.

63. RECURSOS ADMINISTRATIVOS Y NORMATIVOS

- Políticas, lineamientos y manuales institucionales que respalden el SGSPI.
- Procedimientos aprobados para gestión de riesgos, incidentes, continuidad y protección de datos personales.
- Convenios o acuerdos con proveedores de servicios TIC, ajustados a las políticas de seguridad.
- Inclusión de cláusulas de seguridad en contratos con terceros.

64. RECURSOS DOCUMENTALES Y METODOLÓGICOS

- Plantillas y formatos institucionales para inventario de activos, análisis de riesgos, incidentes, auditorías, entre otros.
- Procedimientos normalizados (POE) para todas las actividades del SGSPI.
- Manuales de usuario, guías de buenas prácticas y material didáctico de apoyo.

65. CRONOGRAMA DE IMPLEMENTACIÓN

Fase / Actividad	Responsable	Inicio Estimado	Fin Estimado	Observaciones
Socialización y aprobación del plan	Equipo de Seguridad / SETIC	Abril 2026	Mayo 2026	Requiere validación del Comité de Seguridad
Identificación y clasificación de activos de información	SETIC / Líderes de proceso	Mayo 2026	Junio 2026	Debe ser documentado y actualizado periódicamente
Análisis y gestión de riesgos (MAGERIT)	Equipo de Seguridad / SETIC	Junio 2026	Julio 2026	Incluye valoración de activos y definición de riesgos residuales
Diseño e implementación de controles técnicos y organizacionales	SETIC / Comité de Seguridad	Julio 2026	Agosto 2026	Controles técnicos y procedimentales según criticidad
Formulación de políticas derivadas del SGSPI	Equipo de Seguridad / Comité de Seguridad	Agosto 2026	Agosto 2026	Debe incluir políticas específicas de acceso, clasificación, incidentes, etc.
Implementación del plan de formación y sensibilización	SETIC / Talento Humano / Líderes de proceso	Agosto 2026	Octubre 2026	Debe ejecutarse de forma periódica durante el año

Diseño e implementación del plan de gestión de incidentes	Equipo de Seguridad / SETIC	Septiembre 2026	Octubre 2026	Debe contar con canales claros y formatos de reporte
Diseño y ejecución del plan de continuidad del negocio (BCP/DRP)	SETIC / Comité de Continuidad	Octubre 2026	Noviembre 2026	Integrar análisis BIA y estrategias de recuperación
Ejecución del plan de auditoría y seguimiento	Equipo de Seguridad / Comité de Seguridad	Noviembre 2026	Diciembre 2026	Incluye auditoría interna y autoevaluaciones
Evaluación de resultados y mejora continua	Equipo de Seguridad / Comité de Seguridad	Diciembre 2026	Diciembre 2026	Debe retroalimentar el ciclo del SGSPI

66. RESPONSABLES DEL PLAN

La ejecución, seguimiento y sostenibilidad del Plan de Seguridad y Privacidad de la Información requiere la participación activa y coordinada de diversas instancias institucionales. Cada actor tiene asignadas responsabilidades específicas según su rol dentro del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), en concordancia con las buenas prácticas del MSPI.

La ejecución, seguimiento y sostenibilidad del Plan de Seguridad y Privacidad de la Información requiere la participación activa y coordinada de diversas instancias institucionales. Cada actor tiene asignadas responsabilidades específicas según su rol dentro del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), en concordancia con las buenas prácticas del MSPI.

Responsable	Funciones Asociadas
Gobernador de Norte de Santander	• Validar el Plan de Seguridad y Privacidad de la Información. • Asignar los recursos necesarios para su implementación. • Garantizar el respaldo institucional y normativo del SGSPI.
Comité de Seguridad y Privacidad de la Información	• Supervisar la implementación del plan. • Validar políticas derivadas, planes complementarios y acciones correctivas. • Evaluar resultados y proponer acciones de mejora.
Secretaría de Tecnologías de la Información y las Comunicaciones (SETIC)	• Coordinar técnica y administrativamente la ejecución del plan. • Implementar los controles tecnológicos definidos.

	• Liderar el proceso de gestión de incidentes, formación, continuidad del negocio y auditoría.
Equipo de Seguridad de la Información	• Ejecutar las actividades operativas del plan. • Coordinar el inventario y clasificación de activos, análisis de riesgos, seguimiento y documentación. • Monitorear el cumplimiento de los controles y apoyar auditorías.
Líderes de Proceso / Jefes de Dependencia	• • Aplicar el plan en su ámbito de responsabilidad. • Asegurar el cumplimiento de las políticas y procedimientos. • Participar activamente en el proceso de formación, reporte de incidentes y mejora continua.
Responsable del Tratamiento de Datos Personales	• Velar por el cumplimiento de la normativa de protección de datos. • Atender solicitudes de titulares y coordinar el registro de bases de datos ante la SIC. • Apoyar el análisis de riesgos sobre información personal.
Usuarios Finales (funcionarios, contratistas, terceros)	• Cumplir las políticas, procedimientos y lineamientos del plan. • Usar los recursos de información de forma segura y responsable. • Reportar oportunamente cualquier incidente de seguridad.

67. MATRIZ DE RESPONSABILIDADES RACI

La Matriz de Responsabilidades RACI (Responsable, Aprobador, Consultado, Informado) es una herramienta estratégica que permite asignar roles y responsabilidades claras a los actores institucionales involucrados en la implementación, ejecución, seguimiento y mejora continua del Plan de Seguridad y Privacidad de la Información.

Esta matriz facilita la coordinación interinstitucional, promueve la rendición de cuentas, y permite mantener una trazabilidad efectiva de las tareas clave, alineando las acciones con la estructura del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y con las buenas prácticas de gobernanza digital.

68. SIGNIFICADO DEL MODELO RACI:

Letra	Significado
R – Responsable	Quien ejecuta la tarea o actividad. Tiene la responsabilidad operativa.
A – Aprobador (Accountable)	Quien tiene la autoridad final sobre la actividad. Toma decisiones y valida resultados.
C – Consultado	Quien debe ser consultado antes o durante la ejecución. Su conocimiento o aprobación es clave.
I – Informado	Quien debe ser informado del avance o resultado de la actividad, aunque no participe directamente.

Actividad / Componente del Plan	Gobernador	Comité de Seguridad	SETIC	Equipo de Seguridad de la Información	Líderes de Proceso	Responsable de Tratamiento de Datos Personales	Usuarios Finales
Aprobación del Plan de Seguridad y Privacidad	A	C	I	I	I	I	I
Asignación de recursos para el SGSPI	R	C	C	C	I	I	I
Supervisión general del plan	I	R	C	C	C	I	I
Ejecución técnica del plan	I	I	R	R	C	C	I
Gestión de riesgos y clasificación de activos	I	C	C	R	C	C	I
Implementación de controles tecnológicos	I	C	R	C	I	I	I
Gestión de incidentes de seguridad	I	C	R	R	C	C	C
Ejecución del plan de formación y sensibilización	I	C	R	C	C	I	I
Desarrollo del plan de continuidad del negocio (BCP/DRP)	I	C	R	C	C	I	I
Auditorías internas y seguimiento	I	R	C	R	C	C	I
Atención de derechos de titulares de datos personales	I	I	I	C	I	R	I
Cumplimiento de políticas y procedimientos	I	C	C	C	R	C	R

69. MECANISMOS DE MEJORA CONTINUA

El Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de la Gobernación de Norte de Santander debe evolucionar continuamente para responder de manera eficiente a los cambios tecnológicos, normativos, organizacionales y de riesgos. Por esta razón, se implementan mecanismos de mejora continua que aseguren su vigencia, eficacia y adaptabilidad.

La mejora continua permite fortalecer los controles existentes, cerrar brechas identificadas, y elevar el nivel de madurez institucional en seguridad de la información, en concordancia con los principios del Modelo de Seguridad y Privacidad de la Información (MSPI) y los estándares como ISO/IEC 27001.

70. CICLO DE MEJORA CONTINUA (PHVA)

La Gobernación aplicará el enfoque PHVA (Planear – Hacer – Verificar – Actuar) como metodología para la gestión y mejora del SGSPI:

Fase	Actividades Clave
Planear (Plan)	Definición de políticas, objetivos, análisis de riesgos, planificación de controles y recursos.
Hacer (Do)	Ejecución de acciones y controles definidos en el plan. Implementación operativa.
Verificar (Check)	Auditorías, indicadores, seguimiento, revisión del desempeño y evaluación de cumplimiento.
Actuar (Act)	Implementación de acciones correctivas, lecciones aprendidas y ajustes al plan.

71. ACCIONES PARA GARANTIZAR LA MEJORA CONTINUA

- Revisión periódica del Plan de Seguridad y Privacidad de la Información.

- Evaluación de los resultados del análisis de riesgos y actualización de controles.
- Aplicación y análisis de los indicadores de cumplimiento y desempeño.
- Implementación de planes de acción correctiva y preventiva tras auditorías y autoevaluaciones.
- Incorporación de lecciones aprendidas de los incidentes de seguridad gestionados.
- Actualización de las políticas derivadas y documentos del SGSPI.
- Retroalimentación permanente del Comité de Seguridad y Privacidad de la Información.

72. HERRAMIENTAS DE MEJORA CONTINUA

- Auditorías internas y externas.
- Encuestas de satisfacción sobre capacitación y cultura de seguridad.
- Simulacros de incidentes y pruebas de continuidad.
- Evaluación de madurez del SGSPI.
- Análisis de tendencias de incidentes, riesgos y no conformidades.

73. RESPONSABLES DEL PROCESO DE MEJORA

- **Equipo de Seguridad de la Información:** Coordinación y seguimiento.
- **Comité de Seguridad y Privacidad:** Toma de decisiones y validación de acciones.
- **SETIC y líderes de proceso:** Implementación de ajustes y retroalimentación continua.

SONIA ARANGO MEDINA
Secretaria de las Tecnologías de la Información y las Comunicaciones