

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 1 de 23

TABLA DE CONTENIDO

INTRODUCCIÓN	2
OBJETIVO	3
OBJETIVO GENERAL	3
OBJETIVOS ESPECÍFICOS	3
ALCANCE.....	3
MARCO NORMATIVO Y DE REFERENCIA	5
PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	6
DIAGNÓSTICO DE MADUREZ EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	8
INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	9
GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	10
PLAN DE TRATAMIENTO DE RIESGOS.....	12
DIRECTRICES ESTRATÉGICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ...	13
ROLES Y RESPONSABILIDADES.....	15
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17
CAPACITACIÓN Y CULTURA ORGANIZACIONAL EN SEGURIDAD DIGITAL.....	18
INDICADORES DE SEGUIMIENTO Y EVALUACIÓN	19
VERIFICACIÓN, REVISIÓN Y ACTUALIZACIÓN DEL PESI	21
DISPOSICIONES FINALES	22



	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 2 de 23

Introducción

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) constituye un instrumento fundamental para garantizar la adecuada gestión de los riesgos asociados a los recursos tecnológicos y activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC), su diseño responde a la necesidad de asegurar que la información institucional, en cualquiera de sus formas, sea protegida bajo los principios de confidencialidad, integridad, disponibilidad y privacidad, pilares que soportan la confianza de los ciudadanos, el cumplimiento normativo y la continuidad de los procesos misionales de la entidad.

Este documento se enmarca en la normatividad nacional y los estándares internacionales en materia de seguridad digital, a nivel normativo, recoge lo establecido en el Decreto 338 de 2022, que reglamenta la Política de Gobierno Digital; la Ley 1581 de 2012, que establece disposiciones generales para la protección de datos personales; la Ley 1712 de 2014, sobre transparencia y acceso a la información pública; la Ley 1273 de 2009, que tipifica los delitos informáticos; y las directrices contenidas en la Guía de Administración del Riesgo del DAFP (versión 7), en el ámbito internacional, se fundamenta en estándares de la familia ISO/IEC 27000, especialmente 27001, 27005, 27017 y 27018, que proporcionan marcos de referencia para la gestión de la seguridad de la información, la gestión de riesgos, la seguridad en servicios en la nube y la protección de datos personales.

La justificación de este plan radica en la necesidad de fortalecer la seguridad digital de la entidad, atendiendo las observaciones realizadas por auditorías internas y externas, los compromisos derivados del FURAG, y las recomendaciones de entes de control y organismos de supervisión, el PESI permite consolidar una visión estratégica y coordinada que oriente tanto las acciones preventivas como las de respuesta ante incidentes, asegurando la trazabilidad y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

El PESI se articula de manera directa con el Objetivo y Alcance institucionalmente aprobados para la Gestión de Tecnologías de la Información, que son transversales a todos los planes y políticas de la entidad, este plan se integra con los instrumentos institucionales como el Plan Estratégico de Tecnologías de la Información (PETI), el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política General de Seguridad de la Información, el Mapa de Riesgos TI y la

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 3 de 23

Matriz de Partes Interesadas, consolidando un ecosistema de gestión tecnológica seguro, eficiente y orientado a resultados.

En este sentido, el PESI se convierte en una herramienta estratégica que no solo responde a los requerimientos normativos y de control, sino que también proyecta la transformación digital de EPC bajo principios de sostenibilidad, confianza digital y gobernanza, garantizando la protección de la información como activo esencial para la prestación de servicios públicos de calidad.

Objetivo

Objetivo General

Definir y consolidar las estrategias institucionales que orienten la gestión integral de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC), garantizando la confidencialidad, integridad, disponibilidad y privacidad de los activos de información, en cumplimiento del marco normativo colombiano, los lineamientos del MinTIC y los estándares internacionales de referencia.

Objetivos Específicos

- Asegurar la incorporación de la seguridad y privacidad de la información en la planeación estratégica institucional, mediante la articulación del PESI con el PETI, el Plan Estratégico Institucional y el MIPG.
- Implementar programas y controles que fortalezcan la gestión de riesgos, la protección de infraestructuras críticas cibernéticas y la capacidad de respuesta ante incidentes, en coherencia con el MSPI y las normas internacionales.
- Promover una cultura organizacional de seguridad digital, mediante la capacitación continua de funcionarios y contratistas, la adopción de buenas prácticas de ciberseguridad y el fomento de la sostenibilidad tecnológica.

Alcance

Aplica a todos los procesos, dependencias, funcionarios, contratistas, proveedores y terceros que interactúan con los activos de información y los recursos

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 4 de 23

tecnológicos de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC), su cobertura es transversal, institucional y de carácter obligatorio.

El alcance comprende la gestión integral de la seguridad digital en las siguientes dimensiones:

- **Activos de información:** identificación, clasificación, administración y protección de los activos físicos, digitales y tecnológicos contenidos en el Inventario Institucional de Activos, con base en criterios de confidencialidad, integridad, disponibilidad y privacidad (CIDP).
- **Infraestructura tecnológica:** equipos de cómputo, servidores, dispositivos de red, aplicaciones, bases de datos, servicios en la nube, sistemas de almacenamiento y telecomunicaciones que soportan los procesos institucionales.
- **Gestión de riesgos:** identificación, valoración, tratamiento y monitoreo de riesgos relacionados con la seguridad y privacidad de la información, integrados al Mapa de Riesgos Institucionales y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- **Controles de seguridad:** definición e implementación de medidas técnicas (cifrado, autenticación multifactor, respaldos, firewalls, SIEM), organizacionales (roles, políticas y procedimientos), contractuales (cláusulas de seguridad en contratación) y operativas (monitoreo, continuidad y recuperación).
- **Relación con terceros:** supervisión de proveedores y aliados estratégicos que presten servicios tecnológicos, asegurando que cumplan con los requisitos contractuales y con los lineamientos del MinTIC sobre seguridad digital y servicios en la nube.
- **Procesos institucionales:** aplicación del PESI a todos los sistemas de información, trámites y servicios digitales, en cumplimiento de la Política de Gobierno Digital, los Servicios Ciudadanos Digitales y las disposiciones de transparencia y acceso a la información pública.
- **Gestión de incidentes y continuidad:** prevención, reporte, atención y cierre de incidentes de seguridad de la información, así como la ejecución de planes de continuidad de negocio y recuperación ante desastres, de acuerdo con la ISO 22301:2019 y el Decreto 2157 de 2017.
- **Ámbito normativo:** cumplimiento de las leyes nacionales, decretos, resoluciones del MinTIC y estándares internacionales en materia de seguridad digital, protección de datos personales, delitos informáticos y gestión de riesgos.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 5 de 23

Este plan se integra con el PETI, el Plan Estratégico Institucional y el Sistema Integrado de Gestión, asegurando que la seguridad y privacidad de la información se gestionen como un eje estratégico de la operación institucional.

Marco Normativo y de Referencia

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se fundamenta en la normatividad nacional vigente, en los lineamientos expedidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en marcos internacionales de referencia en ciberseguridad y gestión de riesgos.

Normatividad nacional aplicable

- Ley 1273 de 2009: tipifica los delitos informáticos y la protección de la información y de los datos.
- Ley 1581 de 2012 y Decreto 1377 de 2013: regulan la protección de datos personales y los derechos de los titulares.
- Ley 1712 de 2014 y Decreto 103 de 2015: establecen el derecho de acceso a la información pública y la transparencia.
- Ley 594 de 2000: Ley General de Archivos, que regula la función archivística del Estado.
- Decreto 1008 de 2018 y Decreto 338 de 2022: regulan la Política de Gobierno Digital y sus lineamientos.
- Decreto 2157 de 2017: reglamenta la gestión de continuidad de negocio en entidades públicas y privadas.
- Resolución MinTIC 500 de 2021 y Resolución 2277 de 2025: lineamientos para la implementación y fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Conpes 4070 de 2021: Política Nacional de Confianza y Seguridad Digital.
- Estrategia Nacional de Confianza y Seguridad Digital 2025–2027: hoja de ruta más reciente para fortalecer la seguridad digital y la resiliencia cibernética en Colombia.

Normatividad institucional de referencia

- Plan Estratégico de Tecnologías de la Información (PETI).
- Política General de Seguridad de la Información.
- Plan de Seguridad y Privacidad de la Información.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 6 de 23

- Mapas de Riesgos de Gestión y Corrupción – TI.
- Inventario y Clasificación de Activos de Información.
- Matrices de Contexto Estratégico y Partes Interesadas en TI.
- Normograma de Gestión de TI.

Marcos y estándares internacionales de referencia

- ISO/IEC 27001:2022: sistemas de gestión de seguridad de la información.
- ISO/IEC 27002:2022: controles de seguridad de la información.
- ISO/IEC 27005: gestión de riesgos de seguridad de la información.
- ISO 22301:2019: sistemas de gestión de continuidad de negocio.
- ISO 31000:2018: gestión del riesgo.
- ISO/IEC 27017 y 27018: seguridad y privacidad en servicios de nube.
- NIST Cybersecurity Framework 2.0: gestión de riesgos de ciberseguridad.
- COBIT 2019: gobernanza y gestión de TI.

Este marco normativo asegura que la ejecución del PESI se realice bajo un enfoque integral, en cumplimiento de la legislación colombiana, alineada con los lineamientos del MinTIC y soportada en estándares internacionales reconocidos.

Principios de la Política de Seguridad y Privacidad de la Información

El presente Plan Estratégico de Seguridad y Privacidad de la Información se fundamenta en principios que orientan el diseño, implementación y evaluación de todas las acciones relacionadas con la protección de los activos tecnológicos y de información, estos principios aseguran coherencia con la normativa nacional, las políticas institucionales y los estándares internacionales de seguridad digital:

Confidencialidad

Garantizar que la información sea accesible únicamente para las personas autorizadas, evitando su divulgación o exposición no autorizada, la confidencialidad aplica a toda la información institucional, incluyendo datos personales, datos sensibles, información contractual y datos de carácter estratégico.

Integridad

Asegurar que los datos y sistemas de información mantengan su exactitud, consistencia y fiabilidad a lo largo de todo su ciclo de vida, la integridad implica proteger la información frente a modificaciones indebidas, pérdidas accidentales o manipulaciones malintencionadas.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 7 de 23

Disponibilidad

Velar por que la información, los sistemas y servicios tecnológicos estén accesibles y en funcionamiento cuando los usuarios autorizados lo requieran, esto incluye la adopción de medidas de continuidad, recuperación ante desastres y redundancia tecnológica.

Privacidad

Resguardar los datos personales y sensibles de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios, asegurando que su tratamiento se limite a las finalidades autorizadas y que se respeten los derechos de los titulares de la información.

Responsabilidad compartida

Promover la corresponsabilidad en la gestión de la seguridad digital entre todos los funcionarios, contratistas y terceros vinculados a la entidad, cada actor debe cumplir con las políticas, lineamientos y controles definidos para garantizar un entorno digital seguro.

Mejora continua

Fomentar la actualización permanente de controles, procesos y capacidades institucionales, asegurando que la seguridad y privacidad de la información evolucionen conforme a los cambios tecnológicos, normativos y de riesgos emergentes.

Sostenibilidad digital y reducción de huella ambiental

Incorporar un enfoque de sostenibilidad en la gestión de tecnologías de la información, favoreciendo el uso eficiente de recursos energéticos, la optimización de infraestructura, la migración a soluciones digitales que reduzcan el consumo de papel y la adecuada disposición de residuos electrónicos (RAEE), contribuyendo así a los compromisos institucionales frente al cambio climático.

Transparencia y rendición de cuentas

Garantizar que la gestión de seguridad y privacidad de la información esté alineada con los principios de transparencia pública, trazabilidad de decisiones y rendición de cuentas a ciudadanos, entes de control y partes interesadas.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 8 de 23

Diagnóstico de Madurez en Seguridad y Privacidad de la Información

El nivel de madurez en seguridad digital ha sido evaluado mediante la aplicación del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), herramienta oficial definida por el MinTIC.

Los resultados obtenidos en el último ejercicio evidencian que la entidad se encuentra en un nivel de madurez 2 – Repetible, con un puntaje del 48 %, lo que indica que existen prácticas implementadas de manera parcial, aunque con oportunidades significativas de fortalecimiento en materia de seguridad digital.

Hallazgos principales

- La política de seguridad de la información se encuentra definida y en proceso de actualización, pero requiere mayor difusión y apropiación por parte de funcionarios y contratistas.
- El inventario de activos de información está consolidado, aunque se requiere profundizar en la clasificación por criticidad y en la relación de activos con riesgos específicos.
- Se han implementado controles básicos de seguridad (respaldos, antivirus, firewall, accesos restringidos), pero aún se requiere fortalecer la gestión de incidentes, la supervisión a proveedores tecnológicos y los mecanismos de continuidad de negocio.
- El proceso de capacitación en seguridad digital se realiza de manera parcial y debe institucionalizarse como parte de la inducción, reinducción y formación anual obligatoria.
- La integración del PESI con el PETI y con la planeación institucional debe fortalecerse, para asegurar que la seguridad digital sea un eje transversal en los proyectos de TI.

Recomendaciones estratégicas derivadas del autodiagnóstico

- Consolidar un programa de gestión de riesgos de seguridad de la información, alineado con la ISO/IEC 27005 y con el Mapa de Riesgos Institucionales.
- Fortalecer el proceso de gestión de incidentes, incluyendo registro, análisis de causa raíz, respuesta oportuna y aprendizaje organizacional.
- Ampliar la cobertura de capacitación en seguridad digital para todos los funcionarios, contratistas y terceros con acceso a los sistemas institucionales.
- Implementar herramientas de monitoreo y análisis de eventos de seguridad (SIEM) que permitan mejorar la detección temprana de amenazas.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 9 de 23

- Reforzar la supervisión de contratos tecnológicos, asegurando la inclusión de cláusulas de seguridad y continuidad en todos los acuerdos.

El diagnóstico de madurez constituye la base para la definición de los objetivos, directrices y acciones del presente PESI, y servirá como punto de referencia para medir los avances en cada ciclo de implementación y mejora continua.

Inventario y Clasificación de Activos de Información

La protección de la información institucional depende de una adecuada identificación, clasificación y gestión de los activos que la componen, para ello, se mantiene un Inventario Institucional de Activos de Información, que constituye la base para la aplicación de controles, la gestión de riesgos y la continuidad de negocio.

Inventario institucional

El inventario incluye activos en las siguientes categorías:

- Información: documentos físicos y digitales, bases de datos, reportes, comunicaciones oficiales.
- Tecnológicos: hardware, software, aplicaciones, servicios en la nube, sistemas de almacenamiento, dispositivos de red.
- Servicios: sistemas críticos de operación, aplicaciones de soporte institucional, telecomunicaciones.
- Recurso humano: funcionarios, contratistas y terceros que acceden o administran los activos de información.

Cada activo registrado se documenta con información sobre su propietario, custodio, usuarios autorizados, ubicación, soporte (físico o digital), clasificación archivística y dependencias responsables.

Clasificación por criticidad

Los activos se valoran conforme a criterios de confidencialidad, integridad, disponibilidad y privacidad (CIDP), asignando un nivel de criticidad alto, medio o bajo, que determina la prioridad de protección y los controles aplicables.

- Alta criticidad: activos cuya afectación comprometería la prestación de servicios públicos, la continuidad de negocio o la legalidad de la operación institucional.
- Media criticidad: activos necesarios para el funcionamiento de procesos internos, cuyo impacto por pérdida o alteración es controlable pero relevante.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 10 de 23

- Baja criticidad: activos de soporte cuya afectación tendría impacto menor o fácilmente recuperable.

Relación con riesgos y controles

Cada activo debe estar vinculado a los riesgos identificados en el Mapa de Riesgos de TI y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, asegurando la trazabilidad entre activos, amenazas, vulnerabilidades y controles.

Responsabilidades

- El Coordinador TI es responsable de administrar el inventario, definir criterios de clasificación y coordinar la protección de activos críticos.
- La Mesa de Ayuda (MDA) realiza el registro, actualización y monitoreo de los activos, reportando cambios o incidencias.
- Los propietarios de la información deben garantizar el uso adecuado de los activos y cumplir con los controles establecidos.

Revisión y actualización

El inventario será revisado y actualizado al menos una vez al año, y de manera extraordinaria cuando se incorporen nuevos activos, se realicen cambios tecnológicos relevantes o se presenten incidentes de seguridad, este inventario constituye un insumo esencial para el autodiagnóstico MSPI, el PETI y el presente PESI, garantizando la integración entre la gestión de activos, la seguridad digital y la planeación estratégica de la entidad.

Gestión de Riesgos de Seguridad y Privacidad de la Información

La gestión de riesgos constituye un eje central y se desarrolla en coherencia con el Mapa de Riesgos Institucionales, el Mapa de Riesgos de TI y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Identificación de riesgos

La identificación considera amenazas internas y externas que puedan comprometer los activos de información, la infraestructura tecnológica y la prestación de servicios institucionales. Los riesgos se clasifican en las siguientes categorías:

- Tecnológicos: fallas de hardware, software, telecomunicaciones y servicios en la nube.
- Organizacionales: errores humanos, falta de controles, procesos ineficientes.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 11 de 23

- Exógenos: ataques cibernéticos, desastres naturales, interrupción de proveedores.
- Jurídicos y regulatorios: incumplimiento de la normatividad en protección de datos personales, transparencia y delitos informáticos.

Valoración de riesgos

Cada riesgo se analiza bajo criterios de probabilidad de ocurrencia e impacto, determinando un nivel de riesgo inherente y un riesgo residual luego de aplicar controles. La metodología utilizada se fundamenta en la ISO/IEC 27005 y en la ISO 31000:2018, garantizando trazabilidad y consistencia.

Tratamiento de riesgos

Las opciones de manejo incluyen:

- Mitigar: implementar controles preventivos, predictivos o correctivos.
- Transferir: trasladar el riesgo a terceros mediante acuerdos o seguros.
- Aceptar: reconocer el riesgo cuando su impacto es mínimo y controlable.
- Eliminar: suprimir el riesgo mediante la eliminación del activo o proceso que lo origina.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información documenta las acciones específicas, responsables, plazos y controles aplicables para cada riesgo identificado.

Controles asociados

- Técnicos: cifrado, autenticación multifactor, segmentación de redes, sistemas de respaldo y monitoreo.
- Organizacionales: procedimientos, roles y responsabilidades claras, acuerdos de confidencialidad.
- Contractuales: inclusión de cláusulas de seguridad y continuidad en contratos tecnológicos.
- Operativos: simulacros de incidentes, auditorías internas y pruebas de recuperación ante desastres.

Monitoreo y reporte

El seguimiento se realiza mediante:

- Indicadores de gestión definidos en el PESI.
- Reportes periódicos de incidentes y riesgos emergentes.
- Resultados del autodiagnóstico MSPI.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 12 de 23

- Auditorías internas y revisiones por la dirección en el Comité de Gestión y Desempeño Institucional.

De esta manera, la gestión de riesgos asegura que la seguridad y privacidad de la información en EPC sea administrada de forma integral, anticipando amenazas, reduciendo vulnerabilidades y fortaleciendo la resiliencia institucional.

Plan de Tratamiento de Riesgos

Define las acciones estratégicas y operativas necesarias para reducir la probabilidad e impacto de los riesgos identificados en el Mapa de Riesgos de TI y en el Mapa de Riesgos Institucionales.

Objetivo del plan

Implementar medidas preventivas, predictivas y correctivas que fortalezcan la seguridad de la información, protejan los activos críticos y aseguren la continuidad de los servicios institucionales.

Acciones estratégicas

- Mitigación de riesgos tecnológicos: fortalecer la infraestructura de seguridad perimetral, implementar autenticación multifactor, gestionar parches de software y habilitar plataformas de monitoreo de eventos de seguridad (SIEM).
- Continuidad del negocio y recuperación: ejecutar planes de respaldo, replicación de datos y pruebas de recuperación ante desastres, en cumplimiento con la ISO 22301:2019.
- Protección de datos personales: garantizar el cumplimiento de la Ley 1581 de 2012, mediante la anonimización de información sensible, auditorías de privacidad y gestión de incidentes que involucren datos personales.
- Supervisión de proveedores: exigir cláusulas contractuales de seguridad y continuidad, realizar auditorías periódicas a proveedores tecnológicos y monitorear su cumplimiento frente a los acuerdos de nivel de servicio.
- Fortalecimiento de la cultura de seguridad: institucionalizar programas de capacitación, sensibilización y campañas permanentes sobre seguridad digital para funcionarios, contratistas y terceros.
- Gestión documental y transparencia: integrar controles de seguridad en la publicación de información, en cumplimiento de la Ley 1712 de 2014 y de la Política de Gobierno Digital.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 13 de 23

Responsables de la ejecución

- El Coordinador TI lidera la implementación y seguimiento del plan, asegurando la alineación con el MSPI y con los lineamientos del MinTIC.
- La Mesa de Ayuda (MDA) ejecuta las acciones operativas, como la gestión de incidentes, los respaldos, el control de accesos y la aplicación de medidas técnicas.
- El Comité de Gestión y Desempeño Institucional aprueba los avances y define acciones adicionales según la evolución de los riesgos.
- Control Interno verifica la efectividad de las medidas adoptadas y el cumplimiento de las obligaciones normativas.

Seguimiento y actualización

El plan será evaluado consolidando informes de cumplimiento y soportes documentales, los resultados servirán de insumo para la revisión anual del PESI y para la actualización del Mapa de Riesgos y del Plan de Tratamiento de Riesgos.

Con este enfoque, EPC asegura que los riesgos de seguridad y privacidad de la información no solo sean identificados, sino también gestionados de manera efectiva y sostenible en el tiempo.

Directrices Estratégicas de Seguridad y Privacidad de la Información

La implementación del PESI se fundamenta en un conjunto de directrices estratégicas que orientan las acciones de seguridad digital, en coherencia con los lineamientos del MinTIC, el MSPI, la normativa nacional y los estándares internacionales adoptados.

Gestión de activos de información

Mantener actualizado el inventario institucional, garantizando la clasificación por niveles de confidencialidad, integridad, disponibilidad y privacidad (CIDP), y aplicando controles diferenciados para los activos de mayor criticidad.

Protección de infraestructuras críticas cibernéticas (ICC)

Identificar los sistemas y servicios esenciales para la prestación de los servicios públicos y asegurar su continuidad mediante medidas de seguridad física, lógica, redundancia tecnológica y planes de recuperación rápida.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 14 de 23

Seguridad en el uso de tecnologías y servicios en la nube

Contratar y operar servicios en la nube bajo cláusulas contractuales de seguridad y confidencialidad, aplicando controles definidos en las normas ISO/IEC 27017 y 27018, y supervisando permanentemente el cumplimiento de los proveedores.

Gestión de riesgos

Aplicar de manera continua la metodología de gestión de riesgos establecida en la ISO/IEC 27005, en articulación con el Mapa de Riesgos Institucional y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Gestión de accesos y control de usuarios

Implementar políticas de control de accesos basadas en el principio de mínimo privilegio, autenticación multifactor, segregación de funciones y registro de auditoría para todas las cuentas críticas.

Prevención y gestión de incidentes

Definir y operar un procedimiento formal de reporte, análisis, atención y cierre de incidentes de seguridad de la información, incluyendo la identificación de causas raíz, la comunicación a las partes interesadas y la implementación de medidas correctivas.

Cumplimiento normativo y contractual

Garantizar la observancia de las leyes nacionales, en especial la Ley 1581 de 2012 (protección de datos personales), la Ley 1712 de 2014 (transparencia) y la Ley 1273 de 2009 (delitos informáticos), así como el cumplimiento de cláusulas contractuales de seguridad y continuidad en la contratación pública.

Cultura organizacional de seguridad digital

Institucionalizar programas de capacitación, sensibilización y formación en seguridad y privacidad de la información, como parte de la inducción, reinducción y capacitaciones anuales de funcionarios y contratistas.

Monitoreo y continuidad de negocio

Fortalecer los mecanismos de detección y análisis de amenazas mediante plataformas de monitoreo (SIEM), pruebas de vulnerabilidades, actualizaciones de software y planes de continuidad del negocio alineados con la norma ISO 22301:2019.

Transparencia y sostenibilidad digital

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 15 de 23

Integrar la seguridad digital con las estrategias de apertura de datos y acceso a la información pública, y promover el uso eficiente de los recursos tecnológicos, el teletrabajo, la reducción del consumo de papel y la disposición responsable de residuos electrónicos (RAEE).

Roles y Responsabilidades

La ejecución requiere la participación articulada de diferentes actores institucionales, con responsabilidades claramente definidas para garantizar la efectividad de la gestión de seguridad digital.

Coordinador de Tecnologías de la Información (Coordinador TI)

Es el responsable principal de liderar la implementación del PESI, sus funciones incluyen:

- Coordinar la ejecución de las estrategias, directrices y planes de acción en materia de seguridad digital.
- Administrar los activos tecnológicos y supervisar la clasificación y protección de la información crítica.
- Presentar informes periódicos al Comité de Gestión y Desempeño Institucional sobre avances, incidentes y riesgos emergentes.
- Asegurar que los contratos tecnológicos incluyan cláusulas de seguridad y supervisar su cumplimiento.

Mesa de Ayuda (MDA)

Actúa como el equipo operativo encargado de ejecutar controles y medidas técnicas. Entre sus responsabilidades se encuentran:

- Administrar los accesos a sistemas y redes bajo los lineamientos del Coordinador TI.
- Atender y registrar incidentes de seguridad, escalando aquellos que tengan impacto crítico.
- Mantener actualizados los respaldos, aplicar parches de seguridad y realizar monitoreos rutinarios.
- Apoyar la actualización del inventario de activos de información y la aplicación de controles.

Comité de Gestión y Desempeño Institucional

Es la instancia de decisión y supervisión en materia de seguridad digital. Entre sus funciones destacan:

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 16 de 23

- Aprobar el PESI y sus actualizaciones.
- Revisar los resultados del autodiagnóstico MSPI, auditorías y seguimientos de riesgos.
- Definir acciones estratégicas frente a incidentes o hallazgos de alto impacto.

Dirección de Planeación

Asegura la alineación del PESI con el Plan Estratégico Institucional y el MIPG, incorporando metas y acciones de seguridad digital en la planeación institucional.

Equipo de Gestión de Calidad

Valida la coherencia del PESI con el Sistema Integrado de Gestión y coordina su publicación en los canales oficiales.

Oficina de Control Interno

Ejecuta auditorías y evaluaciones independientes sobre la efectividad del PESI, emite recomendaciones y verifica la implementación de las acciones de mejora.

Áreas de apoyo transversales (Jurídica, Contratación, Talento Humano)

Contribuyen en la incorporación de cláusulas de seguridad en los contratos, en la capacitación institucional, en la definición de obligaciones legales y en la supervisión del cumplimiento de requisitos por parte de terceros.

La responsabilidad de la seguridad digital es compartida, todos los funcionarios, contratistas y terceros que accedan a los activos de información de EPC deben cumplir las disposiciones del PESI y reportar oportunamente cualquier incidente o vulnerabilidad.

La implementación del PESI se articula con el esquema de las tres líneas de defensa del Modelo Integrado de Planeación y Gestión (MIPG):

- **Primera línea de defensa:** El Coordinador de TI y la Mesa de Ayuda (MDA) son responsables de la ejecución operativa del plan, la implementación de controles, la gestión de incidentes y la administración de los recursos tecnológicos.
- **Segunda línea de defensa:** Las áreas de Planeación Estratégica, Jurídica, Contratación, Talento Humano y Control Interno brindan apoyo estratégico y realizan funciones de monitoreo, supervisión y orientación, asegurando el cumplimiento normativo y contractual.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 17 de 23

- **Tercera línea de defensa:** La Oficina de Control Interno ejerce la función de aseguramiento independiente, evaluando la efectividad de los controles, la gestión de riesgos y el cumplimiento de los lineamientos del PESI.

Gestión de Incidentes de Seguridad de la Información

La gestión de incidentes constituye un proceso clave para garantizar la protección de los activos de información y la continuidad de los servicios institucionales, su finalidad es detectar, registrar, analizar, atender y cerrar los incidentes de seguridad digital de manera oportuna, reduciendo su impacto y generando aprendizajes para fortalecer la resiliencia organizacional.

Definición de incidente

Se entiende como incidente de seguridad de la información cualquier evento que afecte o pueda afectar la confidencialidad, integridad, disponibilidad o privacidad (CIDP) de los activos de información, esto incluye accesos no autorizados, pérdida o robo de información, malware, fallas en sistemas críticos, interrupciones de servicios tecnológicos y violaciones de datos personales.

Etapas del proceso de gestión de incidentes

- Detección y reporte: cualquier funcionario, contratista o tercero debe informar inmediatamente un incidente al Coordinador TI o a la Mesa de Ayuda (MDA), utilizando los canales definidos (correo institucional, sistema de tickets o formato oficial).
- Registro y clasificación: la MDA documentará el incidente, asignando nivel de criticidad (alto, medio o bajo) y relacionándolo con los activos afectados.
- Análisis e investigación: el Coordinador TI determinará la causa raíz, evaluará el impacto y definirá las medidas inmediatas de contención.
- Respuesta y mitigación: se implementarán controles correctivos para restaurar los servicios afectados, proteger los datos y contener la propagación del incidente.
- Cierre y documentación: una vez resuelto, el incidente será cerrado con la elaboración de un informe que incluya las acciones aplicadas, el tiempo de respuesta y las lecciones aprendidas.
- Retroalimentación y mejora: los resultados del análisis alimentarán los planes de acción, el Plan de Tratamiento de Riesgos y la actualización de controles.

Responsabilidades

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 18 de 23

- El Coordinador TI lidera la gestión de incidentes, coordina la respuesta y presenta informes consolidados al Comité de Gestión y Desempeño Institucional.
- La MDA recibe, registra, clasifica y atiende operativamente los incidentes de acuerdo con los protocolos definidos.
- Los usuarios institucionales tienen la obligación de reportar inmediatamente cualquier anomalía o sospecha de incidente.
- Control Interno podrá verificar la gestión de incidentes como parte de las auditorías internas.

Documentación y trazabilidad

Cada incidente debe contar con un registro formal que documente fecha, descripción, activos afectados, nivel de criticidad, responsables, acciones aplicadas, tiempos de respuesta y resultados obtenidos. Dichos registros constituyen insumo para auditorías, revisiones de la dirección y actualizaciones del PESI.

Pruebas y simulacros

El proceso de gestión de incidentes será fortalecido mediante la realización de simulacros y pruebas de respuesta al menos una vez al año, con el fin de evaluar la efectividad de los procedimientos y mejorar la capacidad de reacción institucional.

Capacitación y Cultura Organizacional en Seguridad Digital

La seguridad digital requiere no solo controles técnicos y organizacionales, sino también una cultura institucional orientada a la protección de la información. Por esta razón, la formación y sensibilización en seguridad digital se establece como un componente obligatorio del presente PESI.

Programas de capacitación

Todos los funcionarios, contratistas y terceros con acceso a los activos de información deberán participar en programas de capacitación diseñados para:

- Sensibilizar sobre la importancia de la confidencialidad, integridad, disponibilidad y privacidad (CIDP) de la información.
- Instruir en el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y la Ley 1273 de 2009 de delitos informáticos.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 19 de 23

- Promover buenas prácticas en el uso seguro del correo electrónico, contraseñas, navegación en internet, dispositivos móviles y servicios en la nube.
- Difundir los protocolos institucionales de reporte y gestión de incidentes de seguridad de la información.

Obligatoriedad y periodicidad

- La capacitación en seguridad digital será obligatoria en los procesos de inducción, reinducción y actualización anual de todos los funcionarios y contratistas.
- El Coordinador TI, en coordinación con Talento Humano, definirá programas especializados de formación para la Mesa de Ayuda (MDA) y el personal con funciones críticas en TI.
- Los proveedores de servicios tecnológicos deberán acreditar programas de formación en seguridad digital para su personal, como requisito contractual.

Cultura organizacional de seguridad digital

La cultura de seguridad se fortalecerá mediante:

- Campañas periódicas de sensibilización sobre riesgos y medidas de prevención.
- Publicación de boletines y alertas de seguridad en medios internos institucionales.
- Inclusión de la seguridad digital en los espacios de comunicación organizacional y en la agenda del Comité de Gestión y Desempeño Institucional.
- Incentivos para los funcionarios y equipos que demuestren buenas prácticas en el uso responsable de las tecnologías.

El fortalecimiento de la cultura organizacional en seguridad digital permitirá reducir los incidentes originados por errores humanos, fomentar el cumplimiento normativo y garantizar la apropiación de los lineamientos del PESI por parte de toda la entidad.

Indicadores de Seguimiento y Evaluación

El cumplimiento del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) será verificado a través de indicadores de gestión y resultados que permitan medir el nivel de implementación de controles, la reducción de riesgos, la

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 20 de 23

efectividad de las acciones emprendidas y la madurez alcanzada en seguridad digital.

Indicadores estratégicos

- Porcentaje de implementación de acciones del PESI respecto al plan anual aprobado.
- Nivel de madurez alcanzado en el autodiagnóstico MSPI, comparado con el ciclo anterior.
- Porcentaje de alineación del PESI con el PETI y el Plan Estratégico Institucional.
- Porcentaje de acciones de mejora implementadas derivadas de auditorías internas, externas y del FURAG.

Indicadores de gestión operativa

- Porcentaje de activos de información clasificados y con controles aplicados según criticidad.
- Porcentaje de incidentes de seguridad atendidos dentro de los tiempos establecidos.
- Tiempo promedio de detección y respuesta a incidentes de seguridad digital.
- Porcentaje de proveedores tecnológicos con cláusulas de seguridad y continuidad incluidas en sus contratos.
- Porcentaje de sistemas críticos con pruebas exitosas de respaldo y recuperación.

Indicadores de capacitación y cultura organizacional

- Porcentaje de funcionarios y contratistas capacitados en seguridad digital en inducción, reinducción y programas anuales.
- Número de campañas de sensibilización realizadas anualmente.
- Nivel de participación en actividades de cultura digital y reportes de buenas prácticas.

Indicadores de sostenibilidad digital

- Porcentaje de dispositivos tecnológicos dispuestos conforme a normatividad ambiental y de RAEE.
- Porcentaje de soluciones tecnológicas implementadas que contribuyen a la reducción del uso de papel y energía.

Fuentes de información

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 21 de 23

Los indicadores se alimentarán de los registros de la Mesa de Ayuda (MDA), informes del Coordinador TI, resultados del autodiagnóstico MSPI, reportes de auditoría interna y externa, matrices de riesgos, reportes de seguimiento de proveedores y evidencias de gestión ambiental en TIC.

Seguimiento y reporte

El seguimiento a los indicadores y sus resultados se presentará al Comité de Gestión y Desempeño Institucional y, de manera consolidada, en los informes institucionales al FURAG y a los entes de control, con este sistema de indicadores, EPC asegura la trazabilidad y objetividad en la evaluación de la implementación del PESI, garantizando la mejora continua de la seguridad digital, la confianza ciudadana y la sostenibilidad de los procesos tecnológicos.

Verificación, Revisión y Actualización del PESI

La verificación y actualización del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) es un proceso permanente que garantiza su vigencia, pertinencia y efectividad frente a los cambios normativos, tecnológicos y organizacionales.

Periodicidad ordinaria

El PESI será revisado y actualizado anualmente, en coherencia con el ciclo de planeación institucional, el PETI, el Mapa de Riesgos y los resultados del autodiagnóstico MSPI. Los ajustes y avances se presentarán al Comité de Gestión y Desempeño Institucional, instancia que aprueba las modificaciones y actualizaciones.

Circunstancias extraordinarias

La revisión podrá realizarse en cualquier momento cuando se presenten:

- Cambios relevantes en la normatividad nacional o en los lineamientos del MinTIC.
- Incidentes críticos de seguridad de la información que impacten los activos institucionales.
- Transformaciones tecnológicas significativas, como migraciones de sistemas a la nube, implementación de nuevas plataformas o modernización de infraestructura crítica.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 22 de 23

- Recomendaciones derivadas de auditorías internas, entes de control o revisiones por la dirección.

Responsables de la verificación y revisión

- El Coordinador TI lidera el proceso de verificación y propone los ajustes necesarios.
- La Mesa de Ayuda (MDA) suministra información operativa sobre incidentes, controles y gestión de activos.
- El Equipo de Gestión de Calidad valida la coherencia con el Sistema Integrado de Gestión y coordina la publicación de actualizaciones en los canales institucionales.
- Control Interno garantiza la independencia de la revisión y verifica la implementación de las acciones de mejora.

Integración con la planeación institucional

Las actualizaciones del PESI deben estar alineadas con el Plan Estratégico Institucional, el PETI y el MIPG, asegurando que la seguridad digital permanezca como un eje transversal de la gestión pública, este proceso de verificación y revisión permite que el PESI mantenga un carácter dinámico, adaptable y orientado a la mejora continua, fortaleciendo la capacidad de EPC para enfrentar los retos de la seguridad y privacidad de la información en el entorno digital.

Disposiciones Finales

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) es de cumplimiento obligatorio para todos los funcionarios, contratistas, proveedores y terceros que gestionen, accedan o administren activos de información institucional, su adopción asegura que la seguridad digital se consolide como un eje transversal de la operación y la planeación estratégica de la entidad.

La responsabilidad de coordinar la implementación y seguimiento del PESI recae en el Coordinador TI, con apoyo operativo de la Mesa de Ayuda (MDA), el Comité de Gestión y Desempeño Institucional será la instancia encargada de aprobar las actualizaciones, revisar los avances y definir acciones estratégicas frente a riesgos o incidentes críticos.

	Plan Estratégico de Seguridad y Privacidad de la Información (PESI)	Código: GTI-PI016
		Versión: 0
		Fecha: 27/10/2025
		Página 23 de 23

El plan será publicado en los canales oficiales de la entidad, incluyendo la página web institucional, en cumplimiento de la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública, su revisión será anual y también se actualizará de manera extraordinaria ante cambios normativos, incidentes relevantes, recomendaciones de auditoría o transformaciones tecnológicas significativas, el incumplimiento de las disposiciones establecidas en este plan podrá dar lugar a acciones disciplinarias, contractuales o legales, según la gravedad de la falta y de acuerdo con la normatividad vigente.

Con este instrumento, EPC reafirma su compromiso con la gestión integral de la seguridad y privacidad de la información, la protección de los datos personales, la confianza ciudadana y la sostenibilidad digital, en coherencia con los lineamientos del MinTIC y los estándares internacionales de referencia.

CONTROL DE CAMBIOS				
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	CARGO
1	27/10/2025	Versión inicial	Héctor Gil	Planeación

PROYECTÓ	REVISÓ	APROBÓ
Nombre: Héctor Gil	Nombre: Luis Mendoza	Nombre: Diego Guevara
Cargo: Coordinador TI - Contratista	Cargo: Asesor de Planeación - Contratista	Cargo: director de Planeación
Dirección: Planeación	Subgerencia y/o Dirección: Planeación	Dirección: Planeación
Fecha: 27/10/2025	Fecha: 27/10/2025	Fecha: 27/10/2025