TABLA DE CONTENIDO

Introducción

La presente Política General de Seguridad de la Información establece el marco institucional que orienta la protección de los activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) y la gestión integral de la seguridad digital en el desarrollo de sus funciones misionales, su propósito es garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la continuidad de los servicios y procesos soportados por tecnologías de la información, en coherencia con las obligaciones del sector público colombiano y con las mejores prácticas nacionales e internacionales.

Esta política se fundamenta en la normatividad colombiana vigente, incluyendo, entre otras, la Ley 1581 de 2012 (protección de datos personales) y su reglamentación, la Ley 1712 de 2014 (transparencia y acceso a la información pública), la Ley 1273 de 2009 (delitos informáticos), el Decreto 1008 de 2018 y el Decreto 338 de 2022 (Política de Gobierno Digital), así como la Resolución MinTIC 500 de 2021 y sus actualizaciones, mediante las cuales se adopta y fortalece el Modelo de Seguridad y Privacidad de la Información (MSPI), como referentes técnicos, EPC adopta los lineamientos de ISO/IEC 27001:2022, ISO/IEC 27002, ISO/IEC 27005, ISO 22301 (continuidad de negocio) y el NIST Cybersecurity Framework 2.0, en calidad de marcos de buenas prácticas.

EPC reconoce que, por la naturaleza de sus funciones y la prestación de servicios públicos, administra infraestructuras y procesos críticos que deben operar con altos estándares de resiliencia, confiabilidad y seguridad digital, por ello, esta política articula la gestión de la seguridad de la información con la gestión del riesgo institucional, la continuidad de negocio, la contratación con componentes tecnológicos, la supervisión de proveedores (incluida la nube) y el cumplimiento de las exigencias de Gobierno Digital y de los Servicios Ciudadanos Digitales.

En coherencia con el Modelo Integrado de Planeación y Gestión (MIPG) y con el Sistema Integrado de Gestión de la entidad, la política se implementa bajo el ciclo de mejora continua (PHVA) y se integra con el Plan Estratégico de Tecnologías de la Información (PETI) y el Plan Estratégico de Seguridad y Privacidad de la Información (PESI). La gestión de activos de información (inventario y clasificación) se asume como eje transversal para priorizar controles, orientar la continuidad y soportar la gestión del riesgo.

La gobernanza de esta política se adecúa al tamaño organizacional de EPC: el Coordinador TI lidera técnica y administrativamente su implementación; la Mesa de Ayuda (MDA) ejecuta las actividades operativas y de soporte; la Dirección de Planeación asegura la alineación con la planeación institucional; el Equipo de Gestión de Calidad sirve como instancia de articulación y aprobación; y Control Interno ejerce la evaluación independiente en el marco del Sistema de Control Interno y del MIPG. Los demás actores (jurídica, contratación, talento humano, proveedores) participan como apoyos transversales según sus competencias.

Como mecanismo formal de verificación, EPC realizará anualmente (y cuando resulte necesario por cambios normativos, incidentes relevantes o auditorías) el Autodiagnóstico del MSPI dispuesto por el MinTIC, sus resultados serán insumo para la revisión por la dirección, la actualización del PESI y del PETI, la gestión de riesgos, y el reporte al Comité de Gestión y Desempeño Institucional, garantizando trazabilidad y mejora continua.

Finalmente, esta política incorpora criterios de sostenibilidad y mitigación del cambio climático en la gestión de TI, promoviendo la digitalización y reducción de papel, el uso responsable de servicios en la nube, la eficiencia energética, el teletrabajo cuando aplique y la gestión adecuada de residuos de aparatos eléctricos y electrónicos (RAEE); todo ello orientado a una operación segura, eficiente y responsable con el entorno. Esta política es de cumplimiento obligatorio para todos los funcionarios, contratistas y terceros que accedan o traten información de EPC.

Objetivo

Objetivo General

Fortalecer la gestión de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P., mediante la implementación de lineamientos, controles y prácticas que garanticen la confidencialidad, integridad, disponibilidad y privacidad de los activos de información, en cumplimiento de la normatividad colombiana vigente, los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y los marcos internacionales de referencia.

Objetivos Específicos

1. Asegurar el cumplimiento normativo y regulatorio en materia de seguridad digital, protección de datos personales, transparencia, acceso a la información y delitos informáticos, integrando los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y del Gobierno Digital.
2. Implementar una gestión integral de riesgos de seguridad de la información, orientada a la protección de infraestructuras críticas cibernéticas, la continuidad de negocio y la resiliencia tecnológica de la entidad, mediante el uso de controles preventivos, correctivos y de detección.
3. Fomentar la cultura organizacional de seguridad digital en funcionarios, contratistas y terceros, promoviendo la capacitación, el uso responsable de los recursos tecnológicos, la adopción de buenas prácticas, y el compromiso con la mejora continua y la sostenibilidad digital.

Alcance

Esta política aplica a todos los procesos, dependencias, funcionarios, contratistas, proveedores y terceros que interactúan con los recursos tecnológicos y los activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC). Su cobertura es institucional, transversal y de carácter obligatorio.

El alcance comprende:

- **Activos de información:** Identificación, clasificación, registro, administración y protección de activos físicos, digitales y de soporte tecnológico, contenidos en el Inventario Institucional de Activos, considerando su nivel de criticidad en términos de confidencialidad, integridad, disponibilidad y privacidad (CIDP).
- **Infraestructura tecnológica:** Equipos de cómputo, servidores, dispositivos de red, servicios en la nube, sistemas de almacenamiento, aplicaciones, bases de datos y redes de telecomunicaciones que soportan los procesos institucionales.
- **Gestión de riesgos:** Identificación, análisis, valoración, tratamiento y monitoreo de riesgos de seguridad de la información y ciberseguridad, articulados con el Mapa de Riesgos Institucionales, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Controles de seguridad:** Definición, implementación y seguimiento de controles de carácter técnico (cifrado, autenticación, firewalls, antivirus, SIEM, respaldos), organizacional (políticas, procedimientos, roles y

responsabilidades), jurídico (cumplimiento normativo, cláusulas contractuales, protección de datos personales) y operativo (soporte, monitoreo, continuidad y recuperación ante desastres).

- **Relación con terceros:** Interacción con contratistas, proveedores y aliados estratégicos que suministren bienes o servicios tecnológicos, quienes deberán cumplir con cláusulas de seguridad de la información, continuidad y confidencialidad.
- **Procesos institucionales:** Sistemas de información, trámites, servicios digitales y procesos internos que hagan uso de tecnologías de la información, incluyendo aquellos asociados a Gobierno Digital, Servicios Ciudadanos Digitales, Transparencia y Acceso a la Información Pública.
- **Gestión de incidentes y continuidad:** Prevención, detección, reporte, análisis, respuesta y aprendizaje frente a incidentes de seguridad digital, junto con planes de continuidad de negocio y recuperación ante desastres, conforme a la ISO 22301 y al Decreto 2157 de 2017.
- **Ámbito normativo:** Cumplimiento de la Ley 1581 de 2012 (protección de datos personales), la Ley 1712 de 2014 (transparencia), la Ley 1273 de 2009 (delitos informáticos), el Decreto 338 de 2022 (Gobierno Digital), la Resolución 500 de 2021 y sus actualizaciones (MSPI), así como marcos internacionales (ISO/IEC 27001:2022, ISO/IEC 27002, ISO/IEC 27005, NIST Cybersecurity Framework 2.0).

En síntesis, el alcance cubre tanto la operación tecnológica interna de EPC como la interacción con actores externos y partes interesadas, garantizando que la seguridad de la información sea un eje estratégico que soporte la misión institucional, la confianza ciudadana, la transparencia y la sostenibilidad digital.

Marco Normativo y de Referencia

La presente política se sustenta en la normatividad colombiana vigente, los lineamientos expedidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y en marcos internacionales de buenas prácticas de seguridad de la información y ciberseguridad.

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**: establecen 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 sus actualizaciones, incluida la **Resolución 2277 de 2025**: lineamientos para la implementación del **Modelo de Seguridad y Privacidad de la Información (MSPI)**.
- **Conpes 3920 de 2018**: Política Nacional de Transformación Digital e Inteligencia Artificial.
- **Conpes 3995 de 2020**: Política Nacional de Confianza y Seguridad Digital.

Normatividad institucional de referencia:

- Plan Estratégico de Tecnologías de la Información (PETI).
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Plan de Seguridad y Privacidad de la Información.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Mapa de Riesgos Institucionales y de Gestión TI.
- Inventario y Clasificación de Activos de Información.
- Matriz de Partes Interesadas en TI.
- Matriz de Contexto Estratégico en TI.

Normas y marcos internacionales de referencia:

- **ISO/IEC 27001:2022**: sistemas de gestión de seguridad de la información.
- **ISO/IEC 27002:2022**: código de prácticas para 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 en la nube.
- **NIST Cybersecurity Framework 2.0**: marco de gestión de riesgos de ciberseguridad.
- **COBIT 2019**: gobernanza y gestión de tecnologías de la información.

Este marco normativo asegura que la gestión de la seguridad de la información en EPC se realice de forma integral, en cumplimiento de la ley, alineada con los lineamientos de MinTIC y soportada en estándares internacionales reconocidos.

Principios de la Política de Seguridad de la Información

La gestión de la seguridad de la información en **Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC)** se rige por principios que buscan garantizar una protección integral de los activos institucionales, considerando dimensiones técnicas, organizacionales, jurídicas y de gobernanza.

Confidencialidad: La información debe estar protegida contra accesos, divulgaciones o usos no autorizados, este principio se implementa mediante mecanismos de control de acceso, autenticación robusta, cifrado de datos en tránsito y en reposo, segmentación de redes y acuerdos de confidencialidad en contratos con funcionarios, contratistas y proveedores.

Integridad: Se asegura que la información mantenga su exactitud y consistencia a lo largo de todo su ciclo de vida, para ello se aplican controles como la gestión de cambios en sistemas, el uso de firmas digitales, el versionamiento de documentos, el control de registros y la aplicación de políticas de respaldo que permitan verificar la recuperación de datos sin alteraciones.

Disponibilidad: Los sistemas, servicios y datos deben estar accesibles de manera oportuna para los usuarios autorizados, este principio se garantiza a través de planes de continuidad de negocio, redundancia de infraestructuras críticas, mecanismos de recuperación ante desastres, acuerdos de niveles de servicio con proveedores y monitoreo en tiempo real de la infraestructura tecnológica.

Privacidad: El tratamiento de datos personales se realiza en estricto cumplimiento de la **Ley 1581 de 2012** y sus decretos reglamentarios, asegurando el respeto a los derechos de los titulares, se aplican medidas como la modificación o eliminación de datos, la gestión de autorizaciones, el registro de incidentes de seguridad que involucren datos personales y la adopción de buenas prácticas de privacidad en servicios en la nube.

Legalidad y cumplimiento: Todas las actividades relacionadas con la seguridad de la información deben ajustarse al marco normativo nacional, a los lineamientos

del MinTIC y a los estándares internacionales adoptados por la entidad, el cumplimiento incluye auditorías internas, evaluaciones de control, revisiones por la dirección y la aplicación anual del autodiagnóstico MSPI como herramienta de verificación oficial.

Gestión del riesgo: Se fundamenta en la identificación, análisis, valoración y tratamiento de los riesgos que puedan afectar los activos de información, incluyendo amenazas cibernéticas, vulnerabilidades técnicas, errores humanos y fallas de proveedores, se adoptan metodologías alineadas con la ISO/IEC 27005 y con el Mapa de Riesgos Institucionales, integrando controles preventivos, predictivos y correctivos.

Responsabilidad compartida: La protección de la información no es exclusiva del área de TI, sino que compromete a todos los funcionarios, contratistas y terceros vinculados. Cada usuario es responsable del uso seguro de los recursos tecnológicos y del cumplimiento de las políticas internas, el Coordinador TI lidera la gestión técnica, la Mesa de Ayuda (MDA) ejecuta controles operativos, y las demás áreas apoyan desde sus competencias.

Mejora continua: El sistema de gestión de la seguridad de la información se fortalece permanentemente mediante la aplicación del ciclo PHVA (Planear, Hacer, Verificar, Actuar), la revisión periódica de los documentos internos, la actualización de controles frente a nuevas amenazas y la incorporación de recomendaciones derivadas de auditorías, incidentes y resultados del autodiagnóstico MSPI.

Transparencia y confianza ciudadana: La apertura de datos y la provisión de servicios digitales deben realizarse bajo esquemas seguros que protejan la integridad de la información pública, generando confianza en los usuarios y en los entes de control, esto incluye el cumplimiento de la Ley 1712 de 2014, la publicación de información en medios oficiales y la habilitación de canales seguros de atención digital.

Sostenibilidad digital: La gestión de la seguridad de la información también incorpora criterios de responsabilidad ambiental, promoviendo la reducción del uso de papel mediante la digitalización de procesos, la eficiencia energética en los centros de datos, el teletrabajo como práctica institucional y la adecuada disposición de residuos electrónicos (RAEE), en coherencia con los Objetivos de Desarrollo Sostenible (ODS).

Directrices Generales de Seguridad de la Información

La implementación de la seguridad digital se desarrolla bajo directrices que garantizan la protección integral de los activos de información y la operación continua de los servicios institucionales.

Gestión de activos de información

- Mantener actualizado el Inventario Institucional de Activos, identificando propietario, custodio, usuarios, criticidad y riesgos asociados.
- Clasificar los activos conforme a criterios de confidencialidad, integridad, disponibilidad y privacidad (CIDP).
- Establecer medidas de protección diferenciadas para los activos críticos, en coherencia con el MSPI y la normativa nacional.

Protección de infraestructuras críticas cibernéticas (ICC)

- Identificar y proteger los sistemas tecnológicos esenciales para la operación y prestación de servicios públicos.
- Implementar controles de seguridad física y lógica, redundancia tecnológica y mecanismos de recuperación rápida.
- Cumplir con lo dispuesto en el Decreto 338 de 2022 y lineamientos de MinTIC sobre ICC.

Seguridad en el uso de tecnologías y servicios en la nube

- Contratar servicios en la nube bajo cláusulas contractuales que aseguren protección de datos, continuidad y confidencialidad.
- Adoptar controles recomendados en las normas ISO/IEC 27017 (seguridad en la nube) y ISO/IEC 27018 (privacidad en la nube).
- Supervisar a los proveedores conforme a lo establecido en los lineamientos del MinTIC.

Gestión de riesgos de seguridad de la información

- Identificar, valorar y tratar riesgos de seguridad digital en el marco del Mapa de Riesgos Institucionales y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Priorizar riesgos que puedan comprometer los activos críticos, la continuidad del negocio o el cumplimiento normativo.
- Mantener coherencia con la ISO/IEC 27005 y con los lineamientos del CONPES 3995 de 2020 – Confianza y Seguridad Digital.

Seguridad en el acceso y uso de la información

- Implementar controles de autenticación robusta, gestión de contraseñas, segregación de funciones y registros de auditoría.
- Aplicar el principio de mínimo privilegio, permitiendo el acceso solo a quienes lo requieren para el cumplimiento de sus funciones.
- Garantizar el uso responsable y ético de la información institucional por parte de funcionarios, contratistas y terceros.

Prevención y gestión de incidentes de seguridad

- Establecer un procedimiento formal de reporte y atención de incidentes, incluyendo clasificación, registro, análisis, respuesta y cierre.
- Asegurar que los incidentes de seguridad de la información se documenten y sirvan como insumo para planes de mejora.
- Incorporar pruebas periódicas de respuesta a incidentes y continuidad de negocio.

Cumplimiento legal y contractual

- Observar lo dispuesto en la Ley 1581 de 2012 (protección de datos personales), la Ley 1712 de 2014 (transparencia), la Ley 1273 de 2009 (delitos informáticos) y las normas de contratación pública (Ley 80 de 1993 y Ley 1150 de 2007).
- Verificar que los contratos con proveedores incluyan cláusulas específicas sobre seguridad de la información, confidencialidad y continuidad.
- Asegurar la trazabilidad y registro documental en el Sistema Integrado de Gestión de EPC.

Capacitación y cultura de seguridad digital

- Desarrollar programas de sensibilización y formación en seguridad digital para funcionarios y contratistas.
- Promover la cultura de uso responsable de las tecnologías, prevención de incidentes y reporte oportuno de irregularidades.
- Incorporar en la inducción y reinducción institucional los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

Transparencia y sostenibilidad digital

- Publicar información en medios oficiales conforme a la Ley 1712 de 2014 y a los principios de Gobierno Digital.
- Fomentar la reducción del uso de papel, el teletrabajo, la eficiencia energética y la adecuada disposición de residuos electrónicos.

- Articular las prácticas de seguridad con los Objetivos de Desarrollo Sostenible (ODS), en particular los relacionados con innovación, instituciones sólidas y acción climática.

Roles y Responsabilidades

La implementación de la Política General de Seguridad de la Información requiere una distribución clara de funciones y responsabilidades que aseguren el cumplimiento de los lineamientos institucionales y normativos. En EPC, estas responsabilidades se organizan de la siguiente manera:

Coordinador de Tecnologías de la Información (Coordinador TI)

- Liderar la planeación, implementación y seguimiento de la política y de los planes estratégicos asociados (PETI y PESI).
- Coordinar la ejecución de controles técnicos y organizacionales de seguridad digital.
- Gestionar los riesgos de seguridad de la información y presentar informes periódicos al Comité de Gestión y Desempeño Institucional.
- Supervisar la relación con proveedores tecnológicos, garantizando el cumplimiento de cláusulas contractuales en materia de seguridad.

Mesa de Ayuda (MDA)

- Ejecutar las acciones operativas de soporte, administración de sistemas, atención de incidentes y mantenimiento de infraestructura tecnológica.
- Reportar de forma inmediata los incidentes de seguridad detectados o informados por los usuarios.
- Apoyar el registro y actualización del inventario de activos de información.
- Implementar las medidas de seguridad definidas por el Coordinador TI y documentar su cumplimiento.

Dirección de Planeación

- Asegurar la alineación de la política con el Plan Estratégico Institucional y con el MIPG.
- Coordinar el reporte de los avances de seguridad digital en los instrumentos de planeación y seguimiento (FURAG, informes de gestión).

Equipo de Gestión de Calidad

- Revisar y aprobar los documentos asociados a la política, garantizando su coherencia con el Sistema Integrado de Gestión.
- Promover la articulación de la seguridad digital en los demás procesos institucionales.

Comité de Gestión y Desempeño Institucional

- Actuar como instancia de decisión y seguimiento de la política y de los riesgos de seguridad de la información.
- Analizar los resultados del autodiagnóstico MSPI, auditorías internas y evaluaciones de control, definiendo las acciones de mejora correspondientes.
- Aprobar los planes y estrategias de seguridad digital presentados por el Coordinador TI.

Oficina de Control Interno

- Realizar auditorías internas y evaluaciones de cumplimiento de la política, en el marco del Sistema de Control Interno y del MIPG.
- Emitir recomendaciones y verificar la implementación de acciones correctivas y preventivas.

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

- Incorporar cláusulas de seguridad en contratos y convenios.
- Verificar que las normas de protección de datos, confidencialidad y continuidad se cumplan en la contratación pública.
- Apoyar procesos de formación y sensibilización en seguridad digital.
- Garantizar el cumplimiento de obligaciones en materia de seguridad y privacidad de la información durante la ejecución de contratos y servicios.

La responsabilidad de la seguridad de la información es compartida, todos los funcionarios, contratistas y terceros que accedan a los activos de información de EPC deben cumplir con esta política y reportar de forma oportuna cualquier incidente o vulnerabilidad detectada.

Gestión de Activos de Información

La información constituye uno de los activos más valiosos, por lo que su adecuada identificación, clasificación, administración y protección es fundamental para garantizar la continuidad de las operaciones y el cumplimiento normativo.

Inventario y clasificación

- Se debe mantener actualizado el Inventario Institucional de Activos de Información, que incluye datos, documentos, aplicaciones, servicios tecnológicos, infraestructura, hardware, software, redes y personal asociado.
- Cada activo se identifica con su propietario, custodio, usuarios autorizados, ubicación y soporte (físico o digital).
- Los activos deben clasificarse conforme a criterios de confidencialidad, integridad, disponibilidad y privacidad (CIDP), asignando un nivel de criticidad (alto, medio, bajo) que permita priorizar controles.

Propiedad y responsabilidades

- Todo activo debe tener un propietario responsable, quien asegura su correcto uso y determina los controles requeridos.
- El Coordinador TI administra los activos tecnológicos y la Mesa de Ayuda (MDA) ejecuta las tareas de registro, actualización y monitoreo de dichos activos.
- Los usuarios institucionales son responsables del uso adecuado y seguro de los activos a los que tengan acceso.

Protección y controles

- Los activos críticos deben contar con medidas de seguridad físicas (controles de acceso a instalaciones, resguardo de equipos), técnicas (cifrado, autenticación, respaldos, alta disponibilidad) y organizacionales (protocolos, políticas, acuerdos de confidencialidad).
- Los controles se seleccionan con base en el nivel de criticidad del activo, los riesgos asociados y lo definido en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- En los contratos con proveedores se deben incluir cláusulas específicas para la protección de activos, en especial aquellos alojados en servicios en la nube o gestionados por terceros.

Riesgos asociados

- Pérdida de disponibilidad de sistemas críticos.
- Acceso no autorizado a información sensible.
- Fuga, alteración o destrucción de datos.
- Obsolescencia tecnológica y vulnerabilidades en software o hardware.
- Riesgos derivados de proveedores que no cumplan con estándares de seguridad digital.

Revisión y actualización

- El inventario de activos de información debe revisarse mínimo una vez al año, y de forma extraordinaria cada vez que se incorporen nuevos activos, se realicen cambios tecnológicos significativos o se presenten incidentes de seguridad relevantes.
- La información consolidada será insumo para el autodiagnóstico MSPI, el Mapa de Riesgos de TI, el PETI y el PESI, garantizando la integración entre seguridad digital, planeación estratégica y gestión de riesgos.

Gestión de Riesgos de Seguridad de la Información

La gestión de riesgos busca identificar, analizar, valorar, tratar y monitorear las amenazas que puedan comprometer la seguridad de la información y la ciberseguridad institucional, este proceso se desarrolla de manera articulada con el Mapa de Riesgos Institucionales, el Mapa de Riesgos de Gestión y de Corrupción – TI, y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Identificación de riesgos

- Se consideran riesgos de origen tecnológico (fallas de hardware, software, redes, nube), organizacional (errores humanos, debilidades en procesos, falta de controles), externo (ataques cibernéticos, desastres naturales, interrupción de proveedores) y jurídico–regulatorio (incumplimiento de leyes y lineamientos del MinTIC).
- Todo riesgo identificado debe asociarse a uno o varios activos de información del inventario institucional.

Valoración de riesgos

- Los riesgos se analizan considerando probabilidad de ocurrencia e impacto sobre los activos y procesos institucionales.
- Se determina un nivel de riesgo inherente, con base en amenazas y vulnerabilidades, y un riesgo residual después de aplicar controles existentes.
- La valoración se realiza aplicando metodologías alineadas con la ISO/IEC 27005 y la ISO 31000:2018.

Tratamiento de riesgos

- Las opciones de manejo incluyen: mitigar, aceptar, transferir o eliminar el riesgo.

- Las decisiones se documentan en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, estableciendo responsables, acciones, plazos y controles específicos.
- El tratamiento debe priorizar riesgos de alto impacto sobre la confidencialidad, integridad, disponibilidad y privacidad (CIDP) de la información.

Controles aplicables

- Técnicos: autenticación multifactor, cifrado, respaldos periódicos, segmentación de redes, firewalls, SIEM, antivirus.
- Organizacionales: políticas y procedimientos internos, acuerdos de confidencialidad, segregación de funciones, planes de continuidad.
- Jurídicos y contractuales: cláusulas de seguridad en contratos, supervisión a proveedores, cumplimiento normativo (Ley 1581, Ley 1712, Ley 1273, Decreto 338 de 2022, Resolución 2277 de 2025).
- Operativos: pruebas de recuperación, simulacros de incidentes, auditorías internas y revisiones por la dirección.

Monitoreo y reporte

- El seguimiento a los riesgos se realiza mediante indicadores de gestión, informes trimestrales y reportes de incidentes.
- Los resultados se presentan al Comité de Gestión y Desempeño Institucional y se incluyen en la revisión anual de la política.
- Los hallazgos de auditoría, los resultados del autodiagnóstico MSPI y las evaluaciones de control interno se utilizan como insumos para fortalecer la gestión de riesgos.

Con este enfoque, EPC asegura que los riesgos de seguridad digital sean gestionados de manera integral, preventiva y correctiva, protegiendo tanto sus activos de información como la confianza de los ciudadanos y partes interesadas.

Relación con PETI, PESI y el Modelo de Seguridad y Privacidad de la Información (MSPI)

La Política General de Seguridad de la Información se articula directamente con los instrumentos estratégicos de Tecnologías de la Información, garantizando coherencia, continuidad y alineación normativa entre los diferentes planes que orientan la gestión tecnológica en EPC.

Plan Estratégico de Tecnologías de la Información (PETI)
El PETI constituye la hoja de ruta institucional para la gestión y modernización de los recursos tecnológicos de la entidad, esta política se integra al PETI con el fin de asegurar que toda iniciativa de inversión o proyecto tecnológico incorpore de manera transversal criterios de seguridad de la información, gestión de riesgos, sostenibilidad digital y cumplimiento normativo, asimismo, el PETI define los programas y proyectos que fortalecen la infraestructura tecnológica, el desarrollo de aplicaciones, la conectividad y los servicios digitales, bajo un enfoque de seguridad y confianza digital.

Plan Estratégico de Seguridad y Privacidad de la Información (PESI)
El PESI define las acciones específicas para implementar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPI), la presente política constituye el marco de referencia del PESI, orientando que los controles, lineamientos y planes de acción se encuentren alineados con la normativa nacional, los lineamientos del MinTIC, el Conpes 4070 de 2021 y los estándares internacionales de seguridad, el PESI permite materializar en acciones concretas la gestión de incidentes, la capacitación en seguridad digital, la supervisión de proveedores y la atención de auditorías internas y externas.

Integración con la planeación institucional
El PETI y el PESI se encuentran integrados al Plan Estratégico Institucional (PEI) y al Modelo Integrado de Planeación y Gestión (MIPG), asegurando que la seguridad de la información no sea un componente aislado, sino un eje transversal de la gestión pública, los resultados del autodiagnóstico MSPI, de los mapas de riesgos, de los planes de acción y de las auditorías institucionales constituyen insumos obligatorios para la actualización permanente de estos instrumentos estratégicos.

De esta manera, la política asegura que la gestión de la seguridad de la información en EPC disponga de un sustento normativo, estratégico y operativo, con trazabilidad directa entre la planeación tecnológica, la gestión de riesgos y los objetivos misionales de la entidad.

Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) y uso de resultados

El autodiagnóstico del MSPI es la herramienta oficial definida por el MinTIC para evaluar el nivel de madurez de la seguridad digital en entidades públicas., en EPC se adopta como mecanismo central de verificación, seguimiento y mejora continua de la gestión de la seguridad y privacidad de la información.

Periodicidad y obligatoriedad

El autodiagnóstico será aplicado anualmente de acuerdo con los lineamientos del MinTIC y, de manera extraordinaria, en los siguientes casos: incidentes críticos de seguridad, cambios normativos significativos o auditorías externas que así lo requieran.

Alcance del autodiagnóstico

La evaluación comprende las dimensiones organizacionales, de personas, físicas, tecnológicas y de cumplimiento normativo, permite medir el grado de implementación de controles, la eficacia de la política institucional y la alineación con estándares internacionales como ISO/IEC 27001, 27005 y 27018, asimismo, considera la revisión de documentos internos como el Inventario de Activos de Información, el Mapa de Riesgos TI, el Plan de Tratamiento de Riesgos, el PETI y el PESI.

Uso de los resultados

Los hallazgos se consolidan en un informe oficial presentado al Comité de Gestión y Desempeño Institucional y a la Dirección de Planeación, dichos resultados son insumo obligatorio para la revisión por la dirección, la formulación de planes de acción correctivos y la actualización de los instrumentos estratégicos, adicionalmente, el autodiagnóstico se integra con el Mapa de Riesgos Institucionales, el Sistema de Control Interno y los reportes del FURAG, garantizando trazabilidad y fortalecimiento de la gestión.

Responsables

El Coordinador TI lidera la aplicación del autodiagnóstico y consolida la información; la Mesa de Ayuda (MDA) suministra registros operativos y evidencias de los controles; el Equipo de Gestión de Calidad valida la coherencia con el Sistema Integrado de Gestión; y la Oficina de Control Interno verifica los resultados, asegurando independencia y su incorporación en el ciclo de mejora continua.

Con la adopción de este instrumento, EPC asegura una medición objetiva, estandarizada y alineada con la Política de Gobierno Digital, el Conpes 4070 de 2021 y las mejores prácticas internacionales en ciberseguridad.

Seguimiento, Verificación del Cumplimiento e Indicadores

El cumplimiento de la política será evaluado periódicamente mediante indicadores, auditorías internas, revisiones por la dirección y el autodiagnóstico anual del MSPI, garantizando trazabilidad, objetividad y transparencia en la gestión de la seguridad de la información.

Mecanismos de verificación

- Autodiagnóstico MSPI: medición anual del nivel de madurez de la seguridad digital según lineamientos del MinTIC.
- Auditorías internas y de control interno: verificación de cumplimiento normativo, contractual y de procedimientos internos.
- Revisión por la dirección: análisis de resultados, riesgos y planes de acción en el Comité de Gestión y Desempeño Institucional.
- FURAG (Formulario Único de Reporte de Avances de la Gestión): reporte oficial de indicadores de Gobierno Digital y Seguridad de la Información ante Función Pública.
- Indicadores internos de gestión: seguimiento a metas y acciones definidas en el PETI y el PESI.

Indicadores sugeridos

- Porcentaje de incidentes de seguridad atendidos dentro del tiempo establecido.
- Nivel de avance en la implementación del PESI.
- Grado de cumplimiento de las actividades definidas en el PETI con enfoque en seguridad digital.
- Disponibilidad promedio de los sistemas de información críticos.
- Porcentaje de funcionarios y contratistas capacitados en seguridad de la información.
- Número de auditorías internas realizadas y porcentaje de hallazgos cerrados.
- Porcentaje de acciones de mejora implementadas derivadas de auditorías internas, externas y del FURAG.

- Porcentaje de dispositivos tecnológicos gestionados bajo normatividad ambiental (RAEE) y soluciones que reduzcan impacto ambiental.

Revisión y Actualización de la Política

La Política General de Seguridad de la Información será revisada y actualizada de forma periódica y extraordinaria, garantizando su pertinencia frente a cambios organizacionales, normativos y tecnológicos.

Periodicidad ordinaria

- La revisión se realizará al menos una vez al año, en coherencia con el ciclo de planeación institucional, el PETI, el PESI y el autodiagnóstico del MSPI.
- Los resultados de esta revisión deberán presentarse al Comité de Gestión y Desempeño Institucional para su aprobación.

Circunstancias extraordinarias: La actualización podrá realizarse de manera inmediata cuando se presenten:

- Modificaciones significativas en el marco normativo nacional o en los lineamientos del MinTIC.
- Incidentes críticos de seguridad de la información o ciberseguridad que impacten la operación de la entidad.
- Cambios tecnológicos de alto impacto, como migración de sistemas a la nube, adquisición de infraestructura crítica o adopción de nuevas plataformas digitales.
- Recomendaciones derivadas de auditorías internas, de control interno o de entes de control externos.

Responsables de la revisión

- El Coordinador TI liderará el proceso de revisión y propondrá los ajustes requeridos.
- La Mesa de Ayuda (MDA) aportará información operativa sobre incidentes, controles aplicados y estado de los activos.
- El Equipo de Gestión de Calidad verificará la coherencia con el Sistema Integrado de Gestión y los demás documentos institucionales.
- Control Interno validará la independencia de la revisión y verificará la implementación de mejoras.

Integración con otros instrumentos: Los cambios realizados deberán quedar alineados con el Plan Estratégico Institucional, el Mapa de Riesgos, el PETI, el PESI, el Inventario de Activos de Información, y los documentos complementarios de seguridad digital, con este proceso, EPC asegura que la política se mantenga vigente, aplicable y alineada con las mejores prácticas nacionales e internacionales en seguridad de la información.

Documentos Internos Relacionados

La aplicación de esta política se soporta en un conjunto de documentos internos que desarrollan, complementan y operacionalizan los lineamientos de seguridad de la información, estos documentos forman parte del Sistema Integrado de Gestión y deben revisarse y actualizarse de manera periódica, garantizando coherencia normativa y técnica.

Documentos estratégicos y de planeación

- Plan Estratégico de Tecnologías de la Información (PETI).
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Plan de Seguridad y Privacidad de la Información.

Gestión de riesgos y continuidad

- Mapa de Riesgos de Gestión – Área de TI.
- Mapa de Riesgos de Corrupción – TI.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Plan de Contingencia y Recuperación en Seguridad Informática.

Inventarios y caracterización

- Inventario y Clasificación de Activos de Información.
- GTI-C026 – Caracterización del Proceso de Gestión de Tecnologías de la Información.

Matrices de contexto y partes interesadas

- PDE-F368 – Matriz de Contexto Estratégico – Gestión de TI.
- PDE-F369 – Matriz de Partes Interesadas – Área de TI.

Normograma y políticas asociadas

- GJ-F209 – Normograma de Gestión de TI.
- Política de Operación del Riesgo.

Herramientas de seguimiento y evaluación

- Autodiagnóstico del MSPI.
- Informes de seguimiento de riesgos (trimestrales y anuales).
- Indicadores de gestión de seguridad digital reportados en FURAG.

La revisión de estos documentos debe realizarse en articulación con el ciclo de actualización de la presente política y en coherencia con las exigencias del Modelo de Seguridad y Privacidad de la Información (MSPI) y del Modelo Integrado de Planeación y Gestión (MIPG).

Disposiciones Finales

La Política General de Seguridad de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) es de obligatorio cumplimiento para todos los funcionarios, contratistas, proveedores y terceros que accedan, procesen o administren información institucional, independientemente del medio o soporte en que esta se encuentre, el Coordinador TI, con apoyo de la Mesa de Ayuda (MDA), será el responsable de coordinar la implementación, divulgación y seguimiento de la política, asegurando su integración en los procesos internos y en los contratos que involucren componentes tecnológicos.

La publicación de esta política se realizará a través de los canales institucionales oficiales, incluyendo la página web de la entidad, en cumplimiento de lo establecido en la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública, el Comité de Gestión y Desempeño Institucional actuará como la instancia de decisión y aprobación de sus actualizaciones, garantizando coherencia con el Plan Estratégico Institucional, el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos del MinTIC.

Los incumplimientos a lo dispuesto en este documento darán lugar a las acciones disciplinarias, contractuales o legales que correspondan, conforme a la normatividad vigente y a los procedimientos internos de la entidad, la vigencia de la política inicia a partir de su aprobación y publicación, y su revisión deberá efectuarse de manera anual o extraordinaria cuando ocurran cambios normativos, incidentes críticos, auditorías externas u otras circunstancias que así lo exijan.

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**	**CARGO**
0	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