PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI)

Vigencia 2026

TABLA DE CONTENIDO

1. Introducción

El Plan de Seguridad y Privacidad de la Información (PSPI) de Empresas Públicas de Cundinamarca S.A. E.S.P. constituye el marco institucional para la gestión integral de la seguridad digital, orientado a proteger los activos de información, garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y asegurar la continuidad de los procesos misionales, estratégicos y de apoyo de la entidad.

El PSPI se adopta como un instrumento de gestión transversal, alineado con el Plan Integrado de Planeación y Gestión (MIPG), el Plan Estratégico Institucional, el Plan Estratégico de Tecnologías de la Información (PETI) y el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), en cumplimiento de lo dispuesto en el Decreto 612 de 2018, que establece la integración de los planes institucionales y su articulación con la planeación estratégica.

Este Plan responde a la necesidad de fortalecer la confianza institucional y ciudadana en el manejo de la información, considerando que Empresas Públicas de Cundinamarca S.A. E.S.P, en su calidad de entidad prestadora de servicios públicos, administra información sensible relacionada con usuarios, proyectos de infraestructura, operación técnica, gestión contractual, financiera y administrativa, cuya afectación podría impactar la continuidad del servicio, el cumplimiento normativo y la reputación institucional.

El PSPI se fundamenta en la normatividad colombiana vigente en materia de seguridad digital, protección de datos personales, transparencia y gestión documental, así como en los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de manera complementaria, adopta estándares internacionales reconocidos en gestión de la seguridad de la información, gestión de riesgos y continuidad del negocio, que permiten fortalecer la resiliencia institucional frente a incidentes tecnológicos, fallas operativas y amenazas cibernéticas.

Desde el punto de vista organizacional, el PSPI se desarrolla bajo el esquema de gobernanza definido por Empresas Públicas de Cundinamarca S.A. E.S.P, en el cual el Proceso de Tecnologías de la Información se encuentra adscrito a la Dirección de Planeación, como un proceso de apoyo estratégico con alcance transversal institucional, en este contexto, la seguridad y privacidad de la información no se conciben como una función aislada de carácter técnico, sino como un componente integral de la planeación, la gestión y el control institucional.

El Plan incorpora un enfoque de mejora continua, basado en el ciclo Planear, Hacer, Verificar y Actuar (PHVA), que permite evaluar periódicamente el nivel de madurez en seguridad digital, gestionar los riesgos asociados a los activos de información, implementar controles proporcionales al nivel de criticidad y atender los hallazgos derivados de auditorías internas, externas y ejercicios de autoevaluación.

El PSPI se consolida como un instrumento institucional obligatorio, orientado a garantizar una gestión de la información segura, confiable, transparente y sostenible, en coherencia con los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A. E.S.P y con las políticas públicas nacionales en materia de Gobierno Digital y seguridad de la información.

2. Objetivo

2.1 Objetivo General

Establecer el PSPI como el marco institucional para la gestión integral de la seguridad y privacidad de la información, que permita proteger los activos de información, garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y asegurar la continuidad de los procesos estratégicos, misionales y de apoyo, en cumplimiento de la normatividad vigente y de los lineamientos de Gobierno Digital del Estado colombiano.

2.2 Objetivos Específicos

- Definir los lineamientos, responsabilidades y controles necesarios para la gestión de la seguridad y privacidad de la información, de manera articulada con el MIPG, el Plan Estratégico Institucional, el PETI y el PESI.
- Implementar un enfoque de gestión de riesgos que permita identificar, analizar, valorar, tratar y monitorear los riesgos asociados a los activos de información, en coherencia con el Mapa de Riesgos Institucionales y las metodologías adoptadas por la entidad.
- Fortalecer la gobernanza de la seguridad de la información mediante la asignación clara de roles y responsabilidades, asegurando la participación de la alta dirección, las direcciones estratégicas, las áreas misionales y los procesos de apoyo.
- Establecer directrices para la prevención, detección, gestión y atención de incidentes de seguridad de la información, garantizando la trazabilidad, la

mejora continua y la adecuada articulación con los procesos de control interno y auditoría.

- Asegurar la protección de los datos personales tratados, en cumplimiento de la normatividad vigente, garantizando los derechos de los titulares y la aplicación de medidas técnicas, administrativas y organizacionales proporcionales al nivel de riesgo.
- Integrar la seguridad y privacidad de la información a los procesos de planeación, seguimiento y evaluación institucional, conforme a lo establecido en el Decreto 612 de 2018, facilitando el reporte de avances, la rendición de cuentas y el fortalecimiento de la confianza institucional y ciudadana.

3. Alcance

El PSPI aplica de manera transversal a todos los procesos, dependencias, funcionarios, contratistas, proveedores y terceros que gestionen, accedan, administren o custodien activos de información y recursos tecnológicos, independientemente del medio, formato o soporte en el que se encuentren.

El alcance del PSPI comprende la totalidad del ciclo de vida de la información, desde su generación, recolección y almacenamiento, hasta su uso, transmisión, conservación y disposición final, garantizando la aplicación de controles proporcionales al nivel de criticidad y riesgo asociado.

De manera específica, el PSPI cubre las siguientes dimensiones institucionales:

3.1 Activos de información: Incluye la identificación, clasificación, valoración y protección de los activos de información, tales como información física y digital, bases de datos, documentos, sistemas de información, aplicaciones, servicios tecnológicos y conocimiento institucional, conforme a los principios de confidencialidad, integridad, disponibilidad y privacidad.

3.2 Infraestructura tecnológica y servicios TI: Abarca la infraestructura tecnológica que soporta los procesos institucionales, incluyendo equipos de cómputo, servidores, redes, sistemas de almacenamiento, aplicaciones institucionales, servicios en la nube autorizados y el sitio web institucional, bajo un enfoque realista, operativo y evidenciable.

3.3 Gestión de riesgos de seguridad y privacidad de la información: Comprende la identificación, análisis, valoración, tratamiento y monitoreo de los riesgos asociados a los activos de información, articulados con el Mapa de Riesgos Institucionales y el

sistema de gestión del riesgo adoptado por Empresas Públicas de Cundinamarca S.A. E.S.P, asegurando su integración con los procesos de planeación, seguimiento y control.

3.4 Controles de seguridad de la información: Incluye la definición e implementación de controles técnicos, administrativos, organizacionales y contractuales orientados a prevenir, detectar y responder a incidentes de seguridad de la información, sin sobredimensionar capacidades ni incorporar tecnologías no existentes.

3.5 Gestión de incidentes de seguridad de la información: Cubre los procedimientos para la detección, registro, análisis, atención, cierre y documentación de incidentes de seguridad de la información, así como la incorporación de lecciones aprendidas al proceso de mejora continua del PSPI.

3.6 Continuidad del negocio y recuperación tecnológica: Comprende la articulación del PSPI con los planes de continuidad del negocio y recuperación tecnológica, garantizando la disponibilidad de los procesos y servicios críticos ante eventos disruptivos, conforme a la normatividad vigente y a la capacidad real de Empresas Públicas de Cundinamarca S.A. E.S.P.

3.7 Protección de datos personales y privacidad: Incluye todas las actividades de tratamiento de datos personales realizadas por Empresas Públicas de Cundinamarca S.A. E.S.P, asegurando el cumplimiento de los principios, derechos y obligaciones establecidos en la normatividad vigente, así como la aplicación de medidas de seguridad acordes con el nivel de riesgo.

3.8 Relación con terceros y proveedores: Aplica a los proveedores, contratistas y terceros que presten servicios o suministren bienes tecnológicos, quienes deberán cumplir con las obligaciones de seguridad y privacidad de la información establecidas contractualmente y en el PSPI.

3.9 Articulación institucional y control: El PSPI se integra a los procesos de planeación institucional, control interno, auditoría, seguimiento y evaluación, sirviendo como insumo para la toma de decisiones, el reporte de avances y la mejora continua, en cumplimiento del Decreto 612 de 2018 y del MIPG.

El alcance del PSPI garantiza que la seguridad y privacidad de la información sean gestionadas como un componente estratégico, transversal y obligatorio de la gestión institucional.

4. Marco Normativo y de Referencia

El PSPI de Empresas Públicas de Cundinamarca S.A. E.S.P se fundamenta en la normatividad colombiana vigente, en los lineamientos emitidos por las entidades rectoras del Estado y en marcos técnicos de referencia internacional, los cuales orientan la gestión de la seguridad y privacidad de la información, la continuidad de los procesos institucionales y el fortalecimiento de la confianza digital.

Este marco normativo y de referencia garantiza que el PSPI se integre de manera coherente al sistema de planeación, gestión, control y auditoría institucional, conforme a lo establecido en el Decreto 612 de 2018 y el MIPG.

4.1 Normatividad nacional aplicable

- Decreto 612 de 2018: establece la integración de los planes institucionales al Plan Integrado de Planeación y Gestión (MIPG), y orienta la articulación del PSPI con la planeación estratégica, el seguimiento y la mejora continua.
- Decreto 338 de 2022: define la Política de Gobierno Digital, incluyendo los componentes de seguridad digital, servicios ciudadanos digitales y confianza en el uso de las tecnologías de la información.
- Ley 1581 de 2012 y sus decretos reglamentarios: regulan la protección de datos personales y los derechos de los titulares de la información.
- Ley 1712 de 2014: establece el régimen de transparencia y acceso a la información pública.
- Ley 594 de 2000: regula la función archivística del Estado y la gestión documental.
- Decreto 2157 de 2017: reglamenta la gestión de la continuidad del negocio en las entidades públicas.
- Ley 1273 de 2009: tipifica los delitos informáticos y protege la información y los datos.
- Plan Integrado de Planeación y Gestión (MIPG): marco de referencia para la gestión pública, dentro del cual se articula el PSPI.
- Guía del Plan de Seguridad y Privacidad de la Información – PSPI, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), vigente para la entidad.

4.2 Normatividad y lineamientos institucionales

- Plan Estratégico Institucional de Empresas públicas de Cundinamarca S.A. E.S.P.
- Plan Estratégico de Tecnologías de la Información (PETI).
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).

- Sistema Integrado de Gestión (SIG).
- Mapa de Riesgos Institucionales y de TI.
- Tablas de Retención Documental (TRD) y demás instrumentos archivísticos vigentes.
- Procedimientos y formatos del Proceso de Tecnologías de la Información.

4.3 Marcos y estándares internacionales de referencia

- ISO/IEC 27001:2022: Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27005: Gestión de riesgos de seguridad de la información.
- ISO/IEC 27031: Continuidad del negocio y recuperación tecnológica en entornos TIC.
- ISO 22301:2019: Sistemas de gestión de continuidad del negocio.
- ISO 31000:2018: Gestión del riesgo.
- ISO/IEC 27035: Gestión de incidentes de seguridad de la información.

Estos estándares se adoptan como marcos de referencia, sin que ello implique la certificación automática de Empresas Públicas de Cundinamarca S.A. E.S.P, sino como apoyo técnico para el diseño, implementación, seguimiento y mejora del PSPI, de acuerdo con la capacidad real y el contexto institucional.

5. Principios

El PSPI se rige por un conjunto de principios que orientan la gestión integral de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P, garantizando que las decisiones, controles y acciones se adopten de manera coherente con la normatividad vigente, el contexto institucional y la capacidad real de la entidad.

Estos principios constituyen la base para el diseño, implementación, seguimiento y mejora continua del PSPI, y son de obligatorio cumplimiento para todos los actores que gestionen o accedan a los activos de información.

5.1 Confidencialidad: La información debe ser protegida frente a accesos, divulgaciones o usos no autorizados, Empresas Públicas de Cundinamarca S.A. E.S.P aplica controles de acceso basados en el principio de mínimo privilegio, mecanismos de autenticación acordes con el nivel de riesgo y acuerdos de confidencialidad con funcionarios, contratistas y proveedores.

5.2 Integridad: La información debe mantenerse completa, exacta y protegida frente a alteraciones no autorizadas, Empresas Públicas de Cundinamarca S.A. E.S.P

implementa controles que permiten asegurar la trazabilidad, el control de cambios y la consistencia de la información a lo largo de su ciclo de vida.

5.3 Disponibilidad: La información, los sistemas y los servicios tecnológicos deben estar disponibles para los usuarios autorizados cuando sean requeridos. Este principio se garantiza mediante la gestión de respaldos, la continuidad del negocio, la recuperación tecnológica y la gestión adecuada de incidentes.

5.4 Privacidad: El tratamiento de datos personales se realiza en cumplimiento de la normatividad vigente, garantizando los derechos de los titulares y la aplicación de medidas técnicas, administrativas y organizacionales proporcionales al nivel de riesgo asociado al tratamiento de la información.

5.5 Cumplimiento normativo: Todas las actividades del PSPI deben ajustarse a las disposiciones legales, reglamentarias y técnicas aplicables, así como a los lineamientos institucionales, el cumplimiento se verifica mediante auditorías internas, ejercicios de autoevaluación y revisiones de control interno.

5.6 Gestión del riesgo: La seguridad y privacidad de la información se gestionan bajo un enfoque basado en riesgos, que permite identificar, analizar, valorar, tratar y monitorear las amenazas y vulnerabilidades que puedan afectar los activos de información, priorizando aquellos de mayor impacto institucional.

5.7 Responsabilidad compartida: La seguridad de la información no es una función exclusiva del Proceso de Tecnologías de la Información, todos los funcionarios, contratistas, proveedores y terceros que interactúan con los activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P son responsables de cumplir las políticas, procedimientos y controles establecidos en el PSPI.

5.8 Mejora continua: El PSPI se fortalece de manera permanente mediante la aplicación del ciclo Planear, Hacer, Verificar y Actuar (PHVA), incorporando los resultados de indicadores, auditorías, gestión de incidentes y cambios en el entorno normativo, tecnológico u organizacional.

5.9 Transparencia y confianza institucional: La gestión de la información y la provisión de servicios digitales deben ejecutarse bajo esquemas de seguridad que fortalezcan la confianza institucional y ciudadana, garantizando el acceso a la información pública en condiciones de integridad, disponibilidad y trazabilidad.

5.10 Sostenibilidad digital: La gestión de la seguridad y privacidad de la información incorpora prácticas responsables orientadas al uso eficiente de los recursos tecnológicos, la reducción del impacto ambiental de las TIC y la alineación con los principios de sostenibilidad institucional.

6. Justificación y Articulación

La adopción del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P se justifica como una necesidad institucional para asegurar que la gestión de la información y de los recursos tecnológicos se realice de manera segura, controlada y alineada con los objetivos estratégicos de la entidad, garantizando la continuidad de los procesos misionales y el cumplimiento de la normatividad vigente.

El PSPI no se concibe como un instrumento aislado de carácter técnico, sino como un componente transversal de la planeación, la gestión y el control institucional, integrado al Plan Integrado de Planeación y Gestión (MIPG), conforme a lo establecido en el Decreto 612 de 2018, que orienta la articulación de los planes institucionales y su seguimiento bajo un enfoque de resultados y mejora continua.

Desde la perspectiva del MIPG, el PSPI se articula principalmente con las dimensiones de Direccionamiento Estratégico y Planeación, Gestión con Valores para Resultados, Evaluación de Resultados y Control Interno, aportando insumos para la toma de decisiones, la gestión de riesgos y el fortalecimiento de la transparencia y la confianza institucional.

En el marco del Plan Estratégico Institucional, el PSPI contribuye al cumplimiento de los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A. E.S.P mediante la protección de los activos de información, la reducción de riesgos asociados a la seguridad digital, la prevención de incidentes que puedan afectar la operación y la garantía de la disponibilidad de la información para la gestión y la prestación de los servicios públicos.

La articulación del PSPI con la planeación institucional se materializa a través de su integración con el Plan Estratégico de Tecnologías de la Información (PETI) y el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), asegurando que los proyectos tecnológicos, las inversiones en TIC y las acciones de fortalecimiento de la seguridad digital se encuentren alineadas con las prioridades estratégicas y cuenten con criterios de riesgo, control y sostenibilidad.

Adicionalmente, el PSPI se integra a los procesos de seguimiento y evaluación institucional, sirviendo como insumo para el reporte de avances en el Formulario Único de Reporte de Avances de la Gestión (FURAG), así como para la atención de auditorías internas y externas, los resultados del autodiagnóstico del PSPI, los indicadores de desempeño y los planes de mejoramiento derivados de hallazgos de control interno se incorporan al ciclo de planeación y mejora continua de la entidad.

En este contexto, el PSPI fortalece la gobernanza institucional al definir roles, responsabilidades y mecanismos de articulación entre la alta dirección, la Dirección de Planeación, el Proceso de Tecnologías de la Información, las direcciones estratégicas y misionales, y los órganos de control, garantizando coherencia, trazabilidad y responsabilidad en la gestión de la seguridad y privacidad de la información.

7. Glosario y Términos de Referencia

Para efectos de la correcta interpretación y aplicación del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, se adoptan las siguientes definiciones y términos de referencia, los cuales deberán ser utilizados de manera consistente en los documentos, procedimientos y registros asociados a la gestión de la seguridad y privacidad de la información.

Activo de información: Recurso que tiene valor para Empresas Públicas de Cundinamarca S.A. E.S.P y que debe ser protegido, incluyendo información, datos, documentos, sistemas, aplicaciones, infraestructura tecnológica, servicios, personas y conocimiento institucional.

Autodiagnóstico PSPI: Herramienta definida por la entidad rectora para evaluar el nivel de madurez de la gestión de la seguridad y privacidad de la información, identificar brechas y orientar acciones de mejora continua.

Confidencialidad: Principio que garantiza que la información solo sea accesible a personas, procesos o sistemas debidamente autorizados.

Disponibilidad: Principio que asegura que la información, los sistemas y los servicios tecnológicos estén accesibles y utilizables por los usuarios autorizados cuando sean requeridos.

Gestión de riesgos de seguridad de la información: Proceso sistemático para identificar, analizar, valorar, tratar y monitorear los riesgos que puedan afectar los activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P.

Gestión de incidentes de seguridad de la información: Conjunto de actividades orientadas a la detección, registro, análisis, atención, cierre y documentación de eventos que afecten o puedan afectar la seguridad y privacidad de la información.

Integridad: Principio que garantiza que la información sea completa, exacta, consistente y protegida frente a modificaciones no autorizadas.

Mesa de Ayuda (MDA): Instancia operativa del Proceso de Tecnologías de la Información responsable del soporte técnico, la atención de incidentes, la gestión de cambios y la operación diaria de los servicios tecnológicos.

PSPI: Marco institucional que define los lineamientos, principios, roles y controles para la gestión integral de la seguridad y privacidad de la información.

Privacidad: Principio orientado a garantizar el tratamiento adecuado de los datos personales, protegiendo los derechos de los titulares y aplicando medidas de seguridad proporcionales al nivel de riesgo.

Proceso de Tecnologías de la Información: Proceso de apoyo estratégico adscrito a la Dirección de Planeación, responsable de habilitar, soportar y asegurar el uso adecuado de las tecnologías de la información.

Respaldo de información: Copia de seguridad de la información crítica, realizada con el fin de garantizar su recuperación en caso de pérdida, daño o incidente de seguridad.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre los activos de información, los procesos institucionales o el cumplimiento de los objetivos de Empresas Públicas de Cundinamarca S.A. E.S.P.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de controles técnicos, administrativos y organizacionales.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión, conforme a la normatividad vigente.

Usuario autorizado: Funcionario, contratista o tercero que cuenta con autorización formal para acceder y utilizar activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P, en el marco de sus funciones o actividades contractuales.

8. Contexto Estratégico y Partes Interesadas

La gestión de la seguridad y privacidad de la información en se desarrolla en un contexto institucional, normativo y operativo que exige un enfoque estratégico, transversal y articulado con los objetivos misionales y de apoyo de la entidad, en este escenario, el PSPI se constituye como un instrumento fundamental para la protección de los activos de información y para la garantía de la continuidad y confiabilidad de los servicios públicos prestados por Empresas Públicas de Cundinamarca S.A. E.S.P.

8.1 Contexto estratégico

Empresas Públicas de Cundinamarca S.A. E.S.P administra información crítica asociada a la planeación, estructuración y ejecución de proyectos, la operación y aseguramiento de la prestación de los servicios, la gestión financiera, contractual, jurídica, administrativa y de talento humano, así como información relacionada con ciudadanos, usuarios, entes territoriales y organismos de control, La pérdida, alteración, indisponibilidad o uso indebido de esta información puede generar impactos operativos, legales, financieros y reputacionales para la entidad.

En este contexto, el PSPI se articula con los instrumentos de planeación institucional, en especial con el Plan Estratégico Institucional, el PETI y el PESI, asegurando que la seguridad y privacidad de la información se integren a la toma de decisiones, a la priorización de inversiones y a la gestión de riesgos institucionales.

El PSPI se desarrolla bajo un esquema de gobernanza en el cual el Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, actúa como habilitador estratégico de la gestión institucional, garantizando que los controles de seguridad de la información respondan a las necesidades reales de los procesos misionales y de apoyo, sin sobredimensionar capacidades ni incorporar soluciones no evidenciables.

8.2 Partes interesadas

La gestión de la seguridad y privacidad de la información debe responder a las expectativas y requerimientos de las partes interesadas internas y externas con las que Empresas Públicas de Cundinamarca S.A. E.S.P interactúa, las cuales influyen o se ven afectadas por el uso y protección de la información institucional.

Partes interesadas internas

- Gerencia General y Subgerencias: responsables de la dirección estratégica y de la toma de decisiones basadas en información confiable y oportuna.
- Dirección de Planeación: responsable de la articulación del PSPI con la planeación institucional, el MIPG y el seguimiento a la gestión.
- Direcciones estratégicas y de apoyo: responsables de la gestión, uso y custodia de la información asociada a sus procesos.
- Direcciones misionales: responsables de la información relacionada con la estructuración, ejecución y operación de proyectos y servicios.
- Proceso de Tecnologías de la Información y Mesa de Ayuda: responsables de habilitar, operar y asegurar los servicios tecnológicos y los controles de seguridad de la información.
- Dirección de Control Interno: responsable de evaluar la efectividad del PSPI y emitir recomendaciones de mejora.

Partes interesadas externas

- Ciudadanos y usuarios: titulares de información personal y beneficiarios de los servicios prestados por Empresas Públicas de Cundinamarca S.A. E.S.P, quienes esperan un manejo seguro, transparente y confiable de su información.
- Entidades territoriales y entidades del orden nacional: actores con los que Empresas Públicas de Cundinamarca S.A. E.S.P intercambia información para la planeación, ejecución y seguimiento de proyectos.
- Entes de control y organismos de supervisión: responsables de verificar el cumplimiento normativo, la gestión de riesgos y la adecuada protección de la información.
- Proveedores y contratistas: terceros que acceden o gestionan información de Empresas Públicas de Cundinamarca S.A. E.S.P en el marco de relaciones contractuales y que deben cumplir las obligaciones de seguridad y privacidad establecidas.

La identificación y gestión de las partes interesadas permite asegurar que el PSPI se implemente de manera coherente con el contexto institucional, fortaleciendo la confianza, la transparencia y la responsabilidad en el manejo de la información.

9. Diagnóstico de Madurez

El diagnóstico de madurez en seguridad digital constituye un insumo fundamental para la gestión del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, al permitir evaluar de manera objetiva el nivel de desarrollo de los controles, procesos y prácticas asociadas a la seguridad y privacidad de la información, así como identificar brechas y oportunidades de mejora.

El autodiagnóstico se aplica conforme a la metodología y lineamientos definidos por la entidad rectora en materia de seguridad digital, y sus resultados se integran al ciclo de planeación, seguimiento y mejora continua de la entidad, en coherencia con el MIPG y el Decreto 612 de 2018.

9.1 Metodología del autodiagnóstico

El autodiagnóstico del PSPI se desarrolla a partir de la evaluación de los dominios y criterios establecidos en la guía vigente, considerando aspectos de gobernanza, gestión de riesgos, controles de seguridad, gestión de incidentes, continuidad del negocio, protección de datos personales y cultura organizacional.

La evaluación se realiza con base en evidencia documental y operativa verificable, evitando la sobrevaloración del nivel de madurez y garantizando que los resultados reflejen la capacidad real de Empresas Públicas de Cundinamarca S.A. E.S.P.

9.2 Nivel de madurez institucional

De acuerdo con la última aplicación del autodiagnóstico, Empresas Públicas de Cundinamarca S.A. E.S.P presenta un nivel de madurez que evidencia la existencia de políticas, lineamientos y prácticas definidas para la gestión de la seguridad y privacidad de la información, con avances progresivos en su formalización e integración a los procesos institucionales.

Este nivel de madurez indica que Empresas Públicas de Cundinamarca S.A. E.S.P cuenta con una base estructurada para la gestión del PSPI, aunque persisten oportunidades de fortalecimiento en aspectos como la estandarización de controles,

la gestión sistemática de riesgos, la cultura organizacional y la trazabilidad de la información.

9.3 Principales hallazgos

Como resultado del autodiagnóstico, se identifican, entre otros, los siguientes aspectos relevantes:

- Existencia de lineamientos institucionales para la seguridad y privacidad de la información, articulados con la planeación institucional.
- Avances en la identificación y clasificación de activos de información, con necesidad de fortalecer su vinculación con los riesgos asociados.
- Implementación de controles básicos de seguridad de la información, con oportunidades de mejora en su documentación y seguimiento.
- Procedimientos definidos para la gestión de incidentes, que requieren fortalecimiento en términos de registro, análisis y lecciones aprendidas.
- Necesidad de ampliar y sistematizar las acciones de capacitación y sensibilización en seguridad digital.

9.4 Oportunidades de mejora

Los resultados del autodiagnóstico permiten definir acciones de mejora orientadas a:

- Fortalecer la integración del PSPI con el PETI, el PESI y el Plan Estratégico Institucional.
- Mejorar la gestión de riesgos de seguridad de la información, asegurando su alineación con el Mapa de Riesgos Institucionales.
- Incrementar la trazabilidad y documentación de los controles de seguridad implementados.
- Consolidar una cultura organizacional en seguridad y privacidad de la información, mediante programas de capacitación y sensibilización.

9.5 Articulación con la mejora continua

Los resultados del autodiagnóstico del PSPI constituyen insumo para la definición de planes de mejoramiento, el ajuste de controles y la priorización de acciones estratégicas, los cuales se incorporan al ciclo Planear, Hacer, Verificar y Actuar (PHVA), garantizando la evolución progresiva del nivel de madurez en seguridad digital de Empresas Públicas de Cundinamarca S.A. E.S.P.

10. Inventario y Clasificación de Activos de Información

La gestión adecuada de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P parte del conocimiento y control de los activos de información que soportan los procesos estratégicos, misionales y de apoyo, el PSPI establece la obligación de identificar, registrar, clasificar y mantener actualizado el inventario institucional de activos de información, como base para la gestión de riesgos y la aplicación de controles de seguridad.

El inventario de activos de información constituye un insumo transversal para la planeación institucional, la gestión del riesgo, la continuidad del negocio, la atención de incidentes y los procesos de auditoría y control.

10.1 Identificación de activos de información

Empresas Públicas de Cundinamarca S.A. E.S.P identifica como activos de información todos aquellos recursos que tienen valor para la entidad y cuya afectación puede generar impactos operativos, legales, financieros o reputacionales, estos activos incluyen, entre otros:

- Información en cualquier formato o soporte.
- Sistemas de información, aplicaciones y bases de datos.
- Infraestructura tecnológica y servicios asociados.
- Servicios tecnológicos que soportan procesos críticos.
- Talento humano con conocimiento crítico para la operación institucional.

La identificación de activos se realiza de manera articulada con las direcciones estratégicas, misionales y de apoyo, garantizando una visión integral y actualizada del ecosistema de información de Empresas Públicas de Cundinamarca S.A. E.S.P.

10.2 Inventario institucional de activos de información

Empresas Públicas de Cundinamarca S.A. E.S.P mantiene un inventario institucional de activos de información debidamente documentado, el cual debe incluir como mínimo la descripción del activo, su ubicación, el responsable o custodio, el proceso asociado y su relación con los servicios institucionales.

El inventario es administrado por el Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, con el apoyo de la Mesa de Ayuda, y debe estar disponible como evidencia para ejercicios de control interno, auditoría y seguimiento institucional.

10.3 Clasificación de activos de información

Los activos de información se clasifican de acuerdo con su nivel de criticidad, considerando los principios de confidencialidad, integridad, disponibilidad y privacidad, esta clasificación permite priorizar la aplicación de controles y la gestión de riesgos, conforme a la capacidad real de Empresas Públicas de Cundinamarca S.A. E.S.P.

De manera general, se establecen los siguientes niveles de clasificación:

- Alta criticidad: activos cuya afectación puede comprometer la continuidad de los servicios, el cumplimiento normativo o la toma de decisiones estratégicas.
- Media criticidad: activos cuya afectación genera impactos operativos relevantes, pero con capacidad de recuperación en plazos razonables.
- Baja criticidad: activos de apoyo cuya afectación tiene impacto limitado y controlable.

10.4 Relación de activos con riesgos y controles

Cada activo de información debe estar asociado a los riesgos identificados en el Mapa de Riesgos Institucionales y de TI, así como a los controles definidos para su protección. Esta relación permite asegurar que los esfuerzos de seguridad se orienten a los activos de mayor impacto y riesgo para Empresas Públicas de Cundinamarca S.A. E.S.P.

La información derivada del inventario y la clasificación de activos alimenta la gestión de riesgos, el plan de tratamiento de riesgos, la continuidad del negocio y la atención de incidentes de seguridad de la información.

10.5 Revisión y actualización del inventario

El inventario y la clasificación de activos de información deben revisarse y actualizarse de manera periódica, y de forma extraordinaria cuando se presenten cambios relevantes en los procesos, la infraestructura tecnológica, la normatividad aplicable o como resultado de incidentes de seguridad o hallazgos de auditoría.

La actualización del inventario constituye una responsabilidad compartida entre el Proceso de Tecnologías de la Información y las áreas propietarias de la información, bajo la supervisión de la Dirección de Planeación.

11. Gestión de Riesgos de Seguridad y Privacidad de la Información

La gestión de riesgos de seguridad y privacidad de la información es un componente central del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, orientado a identificar, analizar, valorar, tratar y monitorear los riesgos que puedan afectar los activos de información y la continuidad de los procesos institucionales.

11.1 Enfoque y metodología de gestión del riesgo: Empresas Públicas de Cundinamarca S.A. E.S.P adopta un enfoque de gestión del riesgo basado en estándares y buenas prácticas reconocidas, que permite evaluar de manera sistemática las amenazas y vulnerabilidades asociadas a los activos de información, considerando la probabilidad de ocurrencia y el impacto potencial sobre los objetivos institucionales.

La metodología de gestión del riesgo se integra a los lineamientos institucionales vigentes y se desarrolla bajo criterios de proporcionalidad, evidencia y capacidad real, evitando la sobreestimación del nivel de madurez tecnológica.

11.2 Identificación de riesgos: La identificación de riesgos se realiza a partir del análisis de los activos de información, los procesos asociados, las amenazas internas y externas, y las vulnerabilidades existentes, este ejercicio involucra a las áreas propietarias de la información y al Proceso de Tecnologías de la Información, garantizando una visión integral del contexto de riesgo.

Los riesgos identificados incluyen, entre otros, aquellos de naturaleza tecnológica, organizacional, legal, operativa y relacionados con terceros.

11.3 Análisis y valoración de riesgos: Una vez identificados, los riesgos son analizados y valorados considerando su probabilidad de ocurrencia y el impacto potencial sobre la confidencialidad, integridad, disponibilidad y privacidad de la información.

La valoración permite clasificar los riesgos en niveles que facilitan la priorización de acciones y la asignación de controles, asegurando que los recursos institucionales se orienten a los riesgos de mayor impacto para Empresas Públicas de Cundinamarca S.A. E.S.P.

11.4 Tratamiento de riesgos: El tratamiento de los riesgos se define a partir de las opciones establecidas en la metodología adoptada por Empresas Públicas de

Cundinamarca S.A. E.S.P, que pueden incluir la mitigación, aceptación, transferencia o eliminación del riesgo.

Las decisiones de tratamiento se documentan y se integran al plan de tratamiento de riesgos de seguridad y privacidad de la información, asegurando coherencia con la planeación institucional, el PETI y el PESI.

11.5 Monitoreo y revisión de riesgos: Los riesgos de seguridad y privacidad de la información son objeto de monitoreo y revisión periódica, con el fin de evaluar la efectividad de los controles implementados y detectar cambios en el contexto institucional, tecnológico o normativo.

El monitoreo de riesgos constituye un insumo para la mejora continua del PSPI y para la toma de decisiones por parte de la Dirección de Planeación, la alta dirección y los órganos de control.

12. Plan de Tratamiento de Riesgos

El plan de tratamiento de riesgos constituye el instrumento mediante el cual Empresas Públicas de Cundinamarca S.A. E.S.P define y ejecuta las acciones necesarias para gestionar los riesgos de seguridad y privacidad de la información identificados y valorados en el marco del PSPI, asegurando su integración con la planeación institucional y el sistema de control interno.

Este plan se articula con el Mapa de Riesgos Institucionales, el PETI y el PESI, y se formula bajo los principios de proporcionalidad, viabilidad y capacidad real de la entidad, conforme a lo establecido en el Decreto 612 de 2018.

12.1 Objetivo del plan de tratamiento de riesgos: El objetivo del plan de tratamiento de riesgos es reducir la probabilidad de ocurrencia y el impacto de los riesgos de seguridad y privacidad de la información que puedan afectar los activos de información y la continuidad de los procesos institucionales de Empresas Públicas de Cundinamarca S.A. E.S.P, mediante la aplicación de controles adecuados y verificables.

12.2 Estrategias de tratamiento del riesgo: Para la gestión de los riesgos identificados, Empresas Públicas de Cundinamarca S.A. E.S.P podrá adoptar una o varias de las siguientes estrategias, de acuerdo con el nivel de riesgo y el contexto institucional:

- Mitigación: implementación de controles técnicos, administrativos u organizacionales orientados a reducir la probabilidad o el impacto del riesgo.
- Aceptación: decisión informada de asumir el riesgo cuando su impacto sea bajo o cuando el costo de su tratamiento supere el beneficio esperado, dejando evidencia documentada.
- Transferencia: traslado parcial del riesgo a terceros, mediante mecanismos contractuales, acuerdos de nivel de servicio o seguros, cuando aplique.
- Eliminación: supresión del riesgo mediante la eliminación del activo, proceso o actividad que lo genera, cuando sea viable.

12.3 Definición de acciones de tratamiento: Las acciones de tratamiento de riesgos deben definirse de manera clara y documentada, indicando como mínimo el riesgo asociado, la acción a implementar, el responsable, los recursos requeridos, los plazos de ejecución y los indicadores de seguimiento.

Estas acciones se priorizan con base en el nivel de riesgo, el impacto institucional y la disponibilidad de recursos, asegurando coherencia con los planes y proyectos institucionales.

12.4 Responsables del plan de tratamiento: El Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, es responsable de coordinar la formulación, ejecución y seguimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Las direcciones estratégicas, misionales y de apoyo son responsables de apoyar la implementación de las acciones que involucren activos de información bajo su custodia o gestión, garantizando la corresponsabilidad institucional.

La Dirección de Control Interno realiza seguimiento independiente al cumplimiento y efectividad del plan, en el marco de sus funciones de evaluación y control.

12.5 Seguimiento y actualización del plan: El plan de tratamiento de riesgos debe ser objeto de seguimiento periódico, con el fin de verificar el avance de las acciones, evaluar la efectividad de los controles implementados y realizar los ajustes necesarios ante cambios en el contexto institucional, tecnológico o normativo.

Los resultados del seguimiento alimentan el ciclo de mejora continua del PSPI y constituyen evidencia para los procesos de auditoría interna, externa y los reportes institucionales correspondientes.

13. Directrices Generales

Las directrices generales del PSPI establecen los lineamientos que orientan la gestión de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P, garantizando un enfoque coherente, transversal y alineado con la planeación institucional, la gestión del riesgo y los procesos de control y auditoría.

Estas directrices son de obligatorio cumplimiento para todos los procesos, dependencias, funcionarios, contratistas, proveedores y terceros que gestionen o accedan a los activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P.

13.1 Gestión integral de los activos de información: Empresas Públicas de Cundinamarca S.A. E.S.P debe mantener actualizado el inventario institucional de activos de información, asegurando su adecuada identificación, clasificación y asignación de responsables, los controles de seguridad se aplicarán de manera proporcional al nivel de criticidad y riesgo de cada activo.

13.2 Seguridad en la infraestructura tecnológica y servicios TI: La infraestructura tecnológica y los servicios TI que soportan los procesos institucionales deben gestionarse bajo criterios de disponibilidad, integridad y seguridad, considerando la capacidad real de Empresas Públicas de Cundinamarca S.A. E.S.P y evitando la incorporación de soluciones no evidenciables o no autorizadas.

13.3 Gestión de accesos y control de usuarios: El acceso a los activos de información debe otorgarse únicamente a usuarios autorizados, bajo el principio de mínimo privilegio y de acuerdo con las funciones asignadas, Empresas Públicas de Cundinamarca S.A. E.S.P debe mantener controles para la creación, modificación y revocación de accesos, así como mecanismos de trazabilidad y registro.

13.4 Relación con proveedores y terceros: Los proveedores, contratistas y terceros que accedan o gestionen información de Empresas Públicas de Cundinamarca S.A. E.S.P deben cumplir las obligaciones de seguridad y privacidad definidas contractualmente y en el PSPI, la supervisión de estas obligaciones debe quedar documentada como evidencia de control.

13.5 Gestión de incidentes de seguridad de la información: Empresas Públicas de Cundinamarca S.A. E.S.P debe contar con procedimientos definidos para la detección, registro, análisis, atención y cierre de incidentes de seguridad de la

información, garantizando la trazabilidad de las acciones realizadas y la incorporación de lecciones aprendidas al proceso de mejora continua.

13.6 Continuidad del negocio y recuperación tecnológica: La seguridad y privacidad de la información deben integrarse a los planes de continuidad del negocio y recuperación tecnológica, asegurando la disponibilidad de los procesos y servicios críticos ante eventos disruptivos, conforme a la normatividad vigente y a la capacidad institucional.

13.7 Protección de datos personales y privacidad: El tratamiento de datos personales debe realizarse en cumplimiento de la normatividad vigente, garantizando los derechos de los titulares y la aplicación de medidas de seguridad adecuadas al nivel de riesgo del tratamiento.

13.8 Capacitación y cultura organizacional: Empresas Públicas de Cundinamarca S.A. E.S.P debe promover una cultura institucional de seguridad y privacidad de la información, mediante acciones de capacitación, sensibilización y comunicación dirigidas a funcionarios, contratistas y terceros.

13.9 Monitoreo, seguimiento y mejora continua: El PSPI debe ser objeto de monitoreo y seguimiento permanente, integrando indicadores, auditorías y ejercicios de autoevaluación que permitan identificar oportunidades de mejora y fortalecer la gestión de la seguridad de la información.

14. Roles y Responsabilidades

La implementación, operación, seguimiento y mejora continua del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P requiere la participación coordinada de las instancias institucionales, con roles y responsabilidades claramente definidos, garantizando gobernanza, control, trazabilidad y cumplimiento normativo, conforme al organigrama vigente y al Plan Integrado de Planeación y Gestión (MIPG).

14.1 Gerencia General

- Garantizar la adopción institucional del PSPI y su alineación con los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A. E.S.P.
- Asignar y autorizar los recursos necesarios para la gestión de la seguridad y privacidad de la información.
- Respaldar las decisiones estratégicas relacionadas con la gestión de riesgos de seguridad de la información.

- Conocer los resultados relevantes del PSPI que impacten la continuidad institucional y la toma de decisiones.

14.2 Dirección de Planeación

- Actuar como dueña institucional del Proceso de Tecnologías de la Información y del PSPI.
- Asegurar la articulación del PSPI con el MIPG, el Plan Estratégico Institucional, el PETI y el PESI.
- Realizar seguimiento estratégico al desempeño del PSPI y promover acciones de mejora continua.
- Integrar los resultados del PSPI a los procesos de planeación, seguimiento y evaluación institucional.

14.3 Proceso de Tecnologías de la Información

El Proceso de Tecnologías de la Información es un proceso de apoyo estratégico adscrito a la Dirección de Planeación, encargado de habilitar, soportar y asegurar el uso adecuado, seguro y controlado de las tecnologías de la información en Empresas Públicas de Cundinamarca S.A. E.S.P.

La responsabilidad del Proceso de Tecnologías de la Información recae en el Coordinador de Tecnologías de la Información, quien ejerce la dirección técnica, operativa y de control del proceso, con apoyo de la Mesa de Ayuda (MDA) para la ejecución operativa.

Son responsabilidades del Proceso de Tecnologías de la Información:

- Implementar, operar y mantener el PSPI de manera articulada con la planeación institucional.
- Gestionar los riesgos de seguridad y privacidad de la información asociados a los activos tecnológicos e informacionales.
- Definir, aplicar y documentar controles de seguridad acordes con la capacidad real de Empresas Públicas de Cundinamarca S.A. E.S.P.
- Administrar el inventario y la clasificación de los activos de información.
- Coordinar la gestión de incidentes de seguridad de la información.
- Articular la gestión de TI y del PSPI con las direcciones estratégicas, misionales y de apoyo.

14.4 Coordinador de Tecnologías de la Información

El Coordinador de Tecnologías de la Información es el responsable directo del Proceso de Tecnologías de la Información y de la gestión integral del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P.

En el marco del PSPI, tiene las siguientes responsabilidades:

- Dirigir, coordinar y controlar el Proceso de Tecnologías de la Información.
- Liderar la implementación, operación y mejora continua del PSPI.
- Definir los lineamientos técnicos, operativos y de seguridad de la información.
- Coordinar la gestión de riesgos de seguridad y privacidad de la información.
- Aprobar y supervisar la ejecución del plan de tratamiento de riesgos.
- Coordinar la atención y gestión de incidentes de seguridad de la información, incluyendo la escalación de incidentes críticos.
- Articular el PSPI con la Dirección de Planeación, la Dirección de Control Interno, la Dirección Jurídica y la Dirección de Gestión Contractual.
- Presentar informes de gestión, avances y resultados del PSPI a las instancias institucionales y de control.
- Coordinar auditorías internas y externas relacionadas con TI y seguridad de la información.

14.5 Mesa de Ayuda (MDA)

La Mesa de Ayuda es la instancia operativa del Proceso de Tecnologías de la Información y actúa bajo la coordinación y supervisión directa del Coordinador de Tecnologías de la Información.

En el marco del PSPI, la Mesa de Ayuda (MDA) es responsable de:

- Ejecutar la operación diaria de los servicios tecnológicos institucionales.
- Aplicar los controles técnicos definidos en el PSPI y en los procedimientos del Proceso de Tecnologías de la Información.
- Registrar, clasificar y atender incidentes de seguridad de la información, dejando evidencia verificable.
- Ejecutar actividades de respaldo, restauración y soporte técnico conforme a los lineamientos establecidos.
- Apoyar la identificación, actualización y control de los activos de información.
- Mantener registros operativos que soporten auditorías, seguimiento institucional y control interno.

14.6 Direcciones estratégicas, misionales y de apoyo

- Gestionar y custodiar los activos de información asociados a sus procesos.

- Cumplir y hacer cumplir los lineamientos del PSPI en el desarrollo de sus actividades.
- Reportar oportunamente riesgos e incidentes de seguridad de la información.
- Apoyar la identificación y tratamiento de riesgos asociados a la información bajo su responsabilidad.

14.7 Dirección Jurídica

- Asesorar en el cumplimiento de la normatividad relacionada con seguridad de la información, protección de datos personales y transparencia.
- Apoyar la definición e inclusión de cláusulas contractuales relacionadas con seguridad y privacidad de la información.

14.8 Dirección de Gestión Contractual

- Incluir y verificar el cumplimiento de obligaciones de seguridad y privacidad de la información en los contratos de bienes y servicios tecnológicos.
- Coordinar con el Proceso de Tecnologías de la Información la supervisión contractual de proveedores TIC.

14.9 Dirección de Control Interno

- Evaluar de manera independiente la efectividad del PSPI.
- Verificar el cumplimiento normativo y la adecuada gestión de los riesgos de seguridad y privacidad de la información.
- Emitir recomendaciones de mejora y realizar seguimiento a su implementación.

14.10 Funcionarios, contratistas y terceros

- Cumplir las políticas, procedimientos y controles definidos en el PSPI.
- Proteger la información a la que tengan acceso en el marco de sus funciones o actividades contractuales.
- Reportar de manera inmediata cualquier incidente, debilidad o evento que pueda afectar la seguridad de la información.

15. Gobernanza y Tres Líneas de Defensa

La gobernanza del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P se estructura bajo el enfoque de las tres líneas de defensa, conforme a los principios del Plan Integrado de Planeación y Gestión (MIPG), con el propósito de asegurar una gestión ordenada, coherente y verificable de los riesgos de seguridad y privacidad de la información.

Este esquema garantiza la adecuada separación entre las funciones de ejecución, supervisión y aseguramiento independiente, fortaleciendo la transparencia, la rendición de cuentas y la toma de decisiones informadas en materia de seguridad de la información.

15.1 Primera línea de defensa: Gestión y control operativo

La primera línea de defensa está conformada por las instancias responsables de la ejecución directa de los procesos y de la aplicación de los controles de seguridad de la información en el día a día.

En el marco del PSPI, esta línea está integrada por:

- Coordinador de Tecnologías de la Información, como responsable del Proceso de Tecnologías de la Información.
- Mesa de Ayuda (MDA), como instancia operativa del proceso.
- Direcciones estratégicas, misionales y de apoyo, en su calidad de propietarias y custodias de la información.

Son responsabilidades de la primera línea de defensa:

- Ejecutar y mantener los controles de seguridad de la información definidos en el PSPI.
- Gestionar los activos de información bajo su responsabilidad.
- Identificar, registrar y reportar riesgos e incidentes de seguridad de la información.
- Aplicar los procedimientos establecidos para la gestión de accesos, respaldos, incidentes y continuidad operativa.
- Generar y conservar evidencias operativas que soporten auditorías y procesos de control.

15.2 Segunda línea de defensa: Supervisión y orientación institucional

La segunda línea de defensa está conformada por las instancias responsables de establecer lineamientos, orientar la gestión, realizar seguimiento y supervisar el cumplimiento del PSPI, sin ejecutar directamente los controles operativos.

En Empresas Públicas de Cundinamarca S.A. E.S.P, esta línea está integrada por:

- Dirección de Planeación, como dueña institucional del Proceso de Tecnologías de la Información y del PSPI.
- Dirección Jurídica.

- Dirección de Gestión Contractual.

Son responsabilidades de la segunda línea de defensa:

- Definir criterios, lineamientos y metodologías para la gestión de la seguridad y privacidad de la información.
- Verificar la articulación del PSPI con el MIPG, el Plan Estratégico Institucional, el PETI y el PESI.
- Supervisar el cumplimiento de las obligaciones legales, normativas y contractuales relacionadas con la seguridad de la información.
- Analizar la evolución de los riesgos y proponer acciones de mejora a partir de los resultados de seguimiento y evaluación.

15.3 Tercera línea de defensa: Aseguramiento independiente

La tercera línea de defensa corresponde al aseguramiento independiente, ejercido por la Dirección de Control Interno, con el fin de evaluar de manera objetiva e independiente la efectividad del PSPI y la adecuada gestión de los riesgos de seguridad y privacidad de la información.

Son responsabilidades de la tercera línea de defensa:

- Realizar auditorías y evaluaciones independientes sobre la implementación y efectividad del PSPI.
- Verificar el cumplimiento normativo y la aplicación de los controles establecidos.
- Emitir recomendaciones de mejora y realizar seguimiento a su implementación.
- Informar a la alta dirección sobre los resultados de las evaluaciones y los riesgos críticos identificados.

15.4 Articulación de las tres líneas de defensa

La articulación efectiva entre las tres líneas de defensa permite a Empresas Públicas de Cundinamarca S.A. E.S.P:

- Garantizar la adecuada separación de funciones entre ejecución, supervisión y control.
- Fortalecer la gestión de riesgos de seguridad y privacidad de la información.
- Asegurar la trazabilidad de las decisiones y acciones implementadas.
- Integrar el PSPI al ciclo de planeación, seguimiento y mejora continúa definido en el MIPG.

16. Relación con Proveedores y Servicios en la Nube

La gestión de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P se extiende a los proveedores, contratistas y terceros que, en el marco de relaciones contractuales, acceden, procesan, almacenan o administran activos de información o servicios tecnológicos de la entidad, en este sentido, el PSPI establece lineamientos para asegurar que dichas relaciones se desarrollen bajo criterios de seguridad, control y cumplimiento normativo.

16.1 Relación con proveedores y contratistas tecnológicos: Empresas Públicas de Cundinamarca S.A. E.S.P deberá asegurar que todos los contratos que involucren bienes o servicios tecnológicos incorporen obligaciones explícitas relacionadas con la seguridad y privacidad de la información, de acuerdo con la normatividad vigente y los lineamientos del PSPI.

Estas obligaciones deberán contemplar, como mínimo:

- Compromisos de confidencialidad y reserva de la información institucional.
- Cumplimiento de la normatividad aplicable en materia de protección de datos personales y seguridad de la información.
- Responsabilidades frente a la gestión y reporte de incidentes de seguridad de la información.
- Requisitos de continuidad del servicio, cuando aplique, acordes con la capacidad real de Empresas Públicas de Cundinamarca S.A. E.S.P.
- Mecanismos de supervisión y verificación del cumplimiento de las obligaciones contractuales.

La supervisión del cumplimiento de estas obligaciones se realizará de manera articulada entre el Proceso de Tecnologías de la Información, la Dirección de Gestión Contractual y la Dirección Jurídica, dejando evidencia verificable para efectos de control y auditoría.

16.2 Acceso de terceros a la información institucional: El acceso de proveedores y terceros a los activos de información de Empresas Públicas de Cundinamarca S.A. E.S.P deberá ser autorizado de manera formal, limitada al alcance contractual y sujeta a controles de acceso, registro y trazabilidad.

Empresas Públicas de Cundinamarca S.A. E.S.P deberá garantizar que:

- Los accesos otorgados a terceros se encuentren debidamente documentados.
- Se apliquen controles de acceso acordes con el principio de mínimo privilegio.

- Los accesos sean revocados oportunamente una vez finalizada la relación contractual o cuando ya no sean requeridos.

16.3 Uso de servicios en la nube: El uso de servicios en la nube por parte de Empresas Públicas de Cundinamarca S.A. E.S.P deberá realizarse únicamente cuando se encuentren debidamente autorizados y evaluados, considerando criterios de seguridad, disponibilidad, cumplimiento normativo y capacidad institucional.

En el marco del PSPI, el uso de servicios en la nube deberá:

- Contar con evaluación previa de riesgos de seguridad y privacidad de la información.
- Garantizar la propiedad y control de la información por parte de Empresas Públicas de Cundinamarca S.A. E.S.P.
- Establecer obligaciones contractuales claras respecto a la protección de la información, la confidencialidad y la disponibilidad del servicio.
- Definir mecanismos de respaldo, recuperación y portabilidad de la información, cuando aplique.

No se incluirán plataformas o servicios no existentes ni se asumirán capacidades tecnológicas no evidenciables o no soportadas institucionalmente.

16.4 Supervisión y seguimiento a proveedores: El Proceso de Tecnologías de la Información, en articulación con las instancias competentes, deberá realizar seguimiento periódico al cumplimiento de las obligaciones de seguridad y privacidad de la información por parte de proveedores y contratistas tecnológicos.

Los resultados del seguimiento deberán documentarse y servir como insumo para:

- La gestión de riesgos de seguridad de la información.
- La evaluación del desempeño de proveedores.
- La definición de acciones correctivas o de mejora.
- Los procesos de auditoría interna y externa.

17. Gestión de Incidentes de Seguridad de la Información

La gestión de incidentes de seguridad de la información es un componente esencial del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, orientado a garantizar la detección oportuna, el registro, la atención, la mitigación y el cierre de los eventos que afecten o puedan afectar la confidencialidad, integridad, disponibilidad o privacidad de la información institucional.

La gestión de incidentes se articula con la gestión de riesgos, la continuidad del negocio, la planeación institucional y los procesos de control interno, asegurando trazabilidad, aprendizaje organizacional y mejora continua.

17.1 Definición de incidente de seguridad de la información: Se considera incidente de seguridad de la información cualquier evento, real o potencial, que comprometa o intente comprometer la seguridad y privacidad de la información de Empresas Públicas de Cundinamarca S.A. E.S.P, incluyendo, entre otros:

- Accesos no autorizados a sistemas o información.
- Pérdida, alteración o divulgación indebida de información.
- Fallas de infraestructura tecnológica que afecten la disponibilidad de servicios.
- Infecciones por software malicioso o ataques cibernéticos.
- Incidentes relacionados con el tratamiento de datos personales.

17.2 Detección y reporte de incidentes: Todos los funcionarios, contratistas, proveedores y terceros que tengan conocimiento de un incidente o una debilidad de seguridad de la información deberán reportarlo de manera inmediata a través de los canales establecidos por Empresas Públicas de Cundinamarca S.A. E.S.P, la Mesa de Ayuda (MDA) actúa como punto de contacto operativo para el registro inicial de los incidentes, bajo la coordinación del Coordinador de Tecnologías de la Información.

17.3 Registro y clasificación de incidentes: Todo incidente de seguridad de la información debe ser registrado de manera formal, indicando como mínimo la fecha, la descripción del evento, los activos afectados, el nivel de impacto y las acciones iniciales adoptadas, los incidentes se clasifican de acuerdo con su nivel de impacto y criticidad, con el fin de priorizar su atención y definir los mecanismos de escalamiento correspondientes.

17.4 Atención y respuesta a incidentes: La atención de los incidentes de seguridad de la información se realiza de manera coordinada entre el Coordinador de Tecnologías de la Información, la Mesa de Ayuda y las áreas involucradas, aplicando medidas de contención, mitigación y recuperación conforme a los procedimientos establecidos, en caso de incidentes de alto impacto, se deberá informar a la Dirección de Planeación y a la Gerencia General, de acuerdo con los lineamientos institucionales.

17.5 Cierre y documentación del incidente: Una vez atendido el incidente, se debe realizar su cierre formal, documentando las causas, las acciones implementadas, los tiempos de respuesta y las lecciones aprendidas, esta información constituye

evidencia para auditorías y sirve como insumo para la actualización de controles, la gestión de riesgos y la mejora continua del PSPI.

17.6 Articulación con la mejora continua: Los resultados de la gestión de incidentes de seguridad de la información deben integrarse al ciclo Planear, Hacer, Verificar y Actuar (PHVA), permitiendo fortalecer los controles existentes, ajustar el plan de tratamiento de riesgos y reducir la probabilidad de recurrencia de incidentes similares.

18. Continuidad de Negocio y Recuperación ante Desastres

La continuidad del negocio y la recuperación tecnológica constituyen componentes esenciales del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, orientados a garantizar que los procesos críticos y los servicios institucionales puedan mantenerse o restablecerse en niveles aceptables ante la ocurrencia de incidentes, emergencias o eventos disruptivos que afecten la información y la infraestructura tecnológica.

La gestión de la continuidad se articula con la planeación institucional, la gestión del riesgo, la seguridad de la información y los procesos de control interno, conforme a la normatividad vigente y a la capacidad real de la entidad.

18.1 Enfoque de continuidad del negocio: Empresas Públicas de Cundinamarca S.A. E.S.P adopta un enfoque preventivo y gradual para la continuidad del negocio, orientado a:

- Identificar los procesos críticos y los servicios institucionales que requieren niveles mínimos de disponibilidad.
- Analizar los impactos que podrían generarse ante interrupciones de la información o de los servicios tecnológicos.
- Definir estrategias de continuidad acordes con la capacidad operativa, técnica y presupuestal de la entidad.
- La continuidad del negocio se gestiona de manera integrada con el PSPI y el sistema de gestión del riesgo institucional.

18.2 Plan de Continuidad del Negocio: Empresas Públicas de Cundinamarca S.A. E.S.P define y mantiene un Plan de Continuidad del Negocio que establece las acciones, responsabilidades y procedimientos necesarios para responder ante eventos que afecten la operación institucional.

El plan debe contemplar, como mínimo:

- Identificación de procesos y servicios críticos.

- Responsables de la activación y coordinación de las acciones de continuidad.
- Procedimientos básicos de respuesta ante interrupciones.
- Mecanismos de comunicación interna y externa durante situaciones de contingencia.

18.3 Recuperación tecnológica: La recuperación tecnológica se orienta a restablecer la disponibilidad de los sistemas, la información y la infraestructura tecnológica afectados por incidentes de seguridad, fallas técnicas o eventos disruptivos.

En el marco del PSPI, la recuperación tecnológica incluye:

- Procedimientos de respaldo y restauración de la información.
- Priorización de sistemas y servicios tecnológicos críticos.
- Roles y responsabilidades para la ejecución de acciones de recuperación.
- Coordinación entre el Coordinador de Tecnologías de la Información y la Mesa de Ayuda (MDA).

18.4 Pruebas y revisión de la continuidad: Empresas Públicas de Cundinamarca S.A. E.S.P deberá realizar ejercicios de revisión y verificación de los planes de continuidad y recuperación tecnológica, en la medida de su capacidad institucional, con el fin de identificar oportunidades de mejora y fortalecer la preparación ante eventos reales.

Los resultados de estas revisiones deberán documentarse y servir como insumo para la mejora continua del PSPI y la gestión del riesgo.

18.5 Articulación con la mejora continua: La gestión de la continuidad del negocio y la recuperación tecnológica se integra al ciclo Planear, Hacer, Verificar y Actuar (PHVA), permitiendo ajustar planes, procedimientos y controles a partir de los resultados de incidentes, auditorías y evaluaciones institucionales.

19. Sostenibilidad Digital y Gestión Ambiental de TIC

La sostenibilidad digital y la gestión ambiental de las Tecnologías de la Información y las Comunicaciones (TIC) hacen parte del enfoque integral del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, orientado a promover el uso responsable, eficiente y racional de los recursos tecnológicos, minimizando impactos ambientales y fortaleciendo la gestión institucional sostenible.

La gestión ambiental de TIC se articula con la planeación institucional, el Sistema Integrado de Gestión, la gestión documental y las políticas de responsabilidad ambiental adoptadas por Empresas Públicas de Cundinamarca S.A. E.S.P.

19.1 Uso eficiente de recursos tecnológicos: Empresas Públicas de Cundinamarca S.A. E.S.P promueve el uso eficiente de la infraestructura tecnológica y de los recursos digitales, priorizando prácticas que contribuyan a la optimización del consumo energético, la reducción de reprocesos y el aprovechamiento adecuado de los activos tecnológicos existentes.

Estas prácticas incluyen, entre otras:

- Uso racional de equipos de cómputo y dispositivos tecnológicos.
- Optimización del almacenamiento digital y reducción de información redundante.
- Promoción de trámites y procesos digitales que reduzcan el uso de papel.

19.2 Gestión de residuos de aparatos eléctricos y electrónicos (RAEE): Empresas Públicas de Cundinamarca S.A. E.S.P implementa prácticas orientadas a la adecuada gestión de los residuos de aparatos eléctricos y electrónicos, garantizando que la disposición, reutilización o baja de equipos tecnológicos se realice conforme a la normatividad ambiental vigente y a los lineamientos institucionales, la gestión de RAEE debe quedar debidamente documentada como evidencia de cumplimiento ambiental y de control de activos tecnológicos.

19.3 Compras y contratación sostenible en TIC: En los procesos de adquisición de bienes y servicios tecnológicos, Empresas Públicas de Cundinamarca S.A. E.S.P promueve criterios de sostenibilidad, eficiencia y vida útil de los equipos, en la medida de su capacidad institucional y de los lineamientos de contratación pública, estos criterios se integran de manera articulada con la Dirección de Gestión Contractual y la Dirección de Planeación, sin comprometer la seguridad, la continuidad ni la operatividad de los servicios institucionales.

19.4 Cultura de sostenibilidad digital: Empresas Públicas de Cundinamarca S.A. E.S.P fomenta una cultura institucional orientada a la sostenibilidad digital, mediante acciones de sensibilización y buenas prácticas dirigidas a funcionarios, contratistas y terceros, relacionadas con el uso responsable de las tecnologías de la información, estas acciones se integran a los programas de capacitación y cultura organizacional asociados al PSPI.

19.5 Articulación con el PSPI y la mejora continua: La sostenibilidad digital y la gestión ambiental de TIC se integran al ciclo de mejora continua del PSPI, permitiendo evaluar y ajustar prácticas institucionales a partir de indicadores,

auditorías y revisiones periódicas, fortaleciendo una gestión tecnológica responsable y alineada con los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A. E.S.P.

20. Protección de Datos Personales y Privacidad

La protección de los datos personales y la garantía del derecho a la privacidad constituyen un componente fundamental del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, orientado a asegurar que el tratamiento de la información personal se realice de manera legal, transparente, segura y conforme a los principios establecidos en la normatividad vigente.

La gestión de la protección de datos personales se articula con la planeación institucional, la gestión del riesgo, la seguridad de la información y los procesos de control interno, garantizando la responsabilidad institucional en el manejo de la información de los titulares.

20.1 Principios para el tratamiento de datos personales: El tratamiento de datos personales en Empresas Públicas de Cundinamarca S.A. E.S.P se rige por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, los cuales orientan todas las actividades relacionadas con la recolección, almacenamiento, uso, circulación y supresión de información personal.

Estos principios deben ser observados por todos los funcionarios, contratistas, proveedores y terceros que, en el marco de sus funciones o actividades contractuales, realicen tratamiento de datos personales por cuenta de Empresas Públicas de Cundinamarca S.A. E.S.P.

20.2 Responsabilidad institucional en la protección de datos personales: Empresas Públicas de Cundinamarca S.A. E.S.P es responsable de garantizar la adopción de medidas técnicas, administrativas y organizacionales que permitan proteger los datos personales contra pérdida, acceso no autorizado, uso indebido, alteración o divulgación no autorizada.

La protección de datos personales se integra al PSPI como un componente transversal, asegurando que los controles de seguridad de la información consideren de manera explícita los riesgos asociados al tratamiento de información personal.

20.3 Medidas de seguridad para la protección de datos personales: En el marco del PSPI, Empresas Públicas de Cundinamarca S.A. E.S.P implementa medidas de seguridad proporcionales al nivel de riesgo del tratamiento de datos personales, que incluyen, entre otras:

- Controles de acceso a la información personal.
- Restricción de accesos bajo el principio de mínimo privilegio.
- Procedimientos para el respaldo y la protección de la información personal.
- Gestión de incidentes de seguridad relacionados con datos personales.

Estas medidas deben ser documentadas y mantenerse como evidencia para efectos de control y auditoría.

20.4 Derechos de los titulares de la información: Empresas Públicas de Cundinamarca S.A. E.S.P garantiza a los titulares de los datos personales el ejercicio de sus derechos, incluyendo el acceso, actualización, rectificación y supresión de la información, así como la revocatoria de la autorización cuando sea procedente, conforme a los procedimientos institucionales establecidos, la atención de solicitudes de los titulares debe realizarse de manera oportuna, trazable y documentada, en coordinación con las instancias institucionales competentes.

20.5 Gestión de incidentes relacionados con datos personales: Los incidentes que involucren datos personales deben ser gestionados conforme a los procedimientos de gestión de incidentes de seguridad de la información definidos en el PSPI, asegurando su registro, análisis, atención y documentación, cuando sea necesario, se deberán adoptar las acciones correctivas correspondientes y fortalecer los controles para prevenir la recurrencia de incidentes similares.

20.6 Articulación con la mejora continua: La protección de datos personales y la privacidad se integran al ciclo Planear, Hacer, Verificar y Actuar (PHVA), permitiendo ajustar controles, procedimientos y medidas de seguridad a partir de los resultados de auditorías, incidentes y evaluaciones institucionales, fortaleciendo la gestión responsable de la información personal en Empresas Públicas de Cundinamarca S.A. E.S.P.

21. Servicios Ciudadanos Digitales y Transparencia

La provisión de servicios ciudadanos digitales y la gestión de la transparencia se desarrollan en Empresas Públicas de Cundinamarca S.A. E.S.P bajo un enfoque de seguridad, confiabilidad y protección de la información, en coherencia con la Política de Gobierno Digital y los principios de acceso a la información pública.

El PSPI establece los lineamientos necesarios para garantizar que los servicios digitales y los mecanismos de transparencia se implementen y operen con controles adecuados de seguridad y privacidad de la información, fortaleciendo la confianza institucional y ciudadana.

21.1 Servicios ciudadanos digitales: Empresas Públicas de Cundinamarca S.A. E.S.P promueve la prestación de servicios ciudadanos digitales que faciliten el acceso a la información, los trámites y los servicios institucionales, asegurando que estos se desarrollen bajo condiciones de confidencialidad, integridad, disponibilidad y privacidad.

- En el marco del PSPI, los servicios ciudadanos digitales deben:
- Contar con controles de seguridad de la información acordes con su nivel de riesgo.
- Garantizar la protección de la información personal y sensible de los ciudadanos.
- Mantener la disponibilidad y continuidad de los servicios, conforme a la capacidad institucional.
- Asegurar la trazabilidad de las transacciones y actuaciones realizadas a través de medios digitales.

21.2 Seguridad de la información en servicios digitales: Los sistemas y plataformas que soportan los servicios ciudadanos digitales deben gestionarse conforme a los lineamientos del PSPI, integrando controles de acceso, registro de eventos, respaldo de la información y gestión de incidentes de seguridad de la información.

El Proceso de Tecnologías de la Información es responsable de coordinar la aplicación de estos controles, con el apoyo de las áreas propietarias de los servicios y la información.

21.3 Transparencia y acceso a la información pública: En cumplimiento de la normatividad vigente sobre transparencia y acceso a la información pública, Empresas Públicas de Cundinamarca S.A. E.S.P garantiza la publicación oportuna, completa y actualizada de la información de carácter público a través de sus canales institucionales.

La gestión de la transparencia se desarrolla bajo criterios de seguridad de la información, asegurando que la información publicada:

- Sea íntegra, confiable y verificable.

- Se encuentre protegida frente a alteraciones no autorizadas.
- Mantenga disponibilidad para la consulta ciudadana.

21.4 Protección de la información publicada: Empresas Públicas de Cundinamarca S.A. E.S.P implementa controles orientados a proteger la información publicada en medios digitales, incluyendo el sitio web institucional, con el fin de prevenir accesos no autorizados, alteraciones indebidas o pérdida de información, estos controles se articulan con los procedimientos del PSPI y deben contar con evidencia documentada para efectos de seguimiento y auditoría.

21.5 Articulación con la mejora continua: La gestión de los servicios ciudadanos digitales y la transparencia se integran al ciclo Planear, Hacer, Verificar y Actuar (PHVA), permitiendo ajustar controles, procesos y prácticas a partir de los resultados de auditorías, indicadores y ejercicios de evaluación institucional.

22. Capacitación y Cultura Organizacional en Seguridad Digital

La capacitación y la cultura organizacional en seguridad digital constituyen un componente transversal del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P, orientado a fortalecer el conocimiento, la conciencia y la responsabilidad de los funcionarios, contratistas y terceros frente a la protección de la información y la gestión adecuada de los riesgos de seguridad y privacidad.

El fortalecimiento de la cultura en seguridad digital contribuye a reducir incidentes asociados a errores humanos, mejorar el cumplimiento normativo y asegurar la aplicación efectiva de los controles definidos en el PSPI.

22.1 Enfoque de capacitación en seguridad digital: Empresas Públicas de Cundinamarca S.A. E.S.P adopta un enfoque de capacitación progresivo y acorde con su capacidad institucional, orientado a asegurar que los actores que gestionan o acceden a la información comprendan sus responsabilidades y apliquen buenas prácticas de seguridad de la información, la capacitación en seguridad digital se integra a los procesos de inducción, reinducción y formación institucional, y se articula con la planeación y el Sistema Integrado de Gestión.

22.2 Contenidos mínimos de capacitación: Los programas de capacitación en seguridad digital deben contemplar, como mínimo, los siguientes contenidos:

- Principios de seguridad y privacidad de la información.
- Buenas prácticas en el uso de herramientas tecnológicas y manejo de la información.

- Gestión de contraseñas y control de accesos.
- Identificación y reporte de incidentes de seguridad de la información.
- Responsabilidades frente al tratamiento de datos personales y la confidencialidad de la información.

Los contenidos deben ajustarse al rol y nivel de responsabilidad de los participantes.

22.3 Responsables de la capacitación: El Proceso de Tecnologías de la Información, bajo la coordinación del Coordinador de Tecnologías de la Información, es responsable de definir los lineamientos técnicos de la capacitación en seguridad digital, la ejecución de las actividades de capacitación se articula con la Dirección de Gestión Humana, garantizando su integración a los planes institucionales de formación y dejando evidencia verificable de su realización.

22.4 Cultura organizacional en seguridad digital: Empresas Públicas de Cundinamarca S.A. E.S.P promueve una cultura organizacional en seguridad digital basada en la responsabilidad compartida, la prevención y el cumplimiento de los lineamientos del PSPI.

Las acciones de cultura organizacional incluyen, entre otras:

- Sensibilización periódica sobre riesgos de seguridad de la información.
- Divulgación de buenas prácticas y alertas de seguridad.
- Promoción del reporte oportuno de incidentes y debilidades de seguridad.

22.5 Seguimiento y mejora continua: Las actividades de capacitación y cultura organizacional en seguridad digital deben ser objeto de seguimiento y evaluación, con el fin de identificar oportunidades de mejora y fortalecer su impacto en la gestión de la seguridad de la información, los resultados de este seguimiento se integran al ciclo de mejora continua del PSPI y sirven como insumo para auditorías y procesos de control interno.

23. Indicadores de Seguimiento y Evaluación

El seguimiento y la evaluación del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P se realizan a través de un conjunto de indicadores que permiten medir el nivel de implementación, efectividad y mejora continua de la gestión de la seguridad y privacidad de la información, en coherencia con el MIPG y el Decreto 612 de 2018.

Los indicadores constituyen un insumo clave para la toma de decisiones, el control institucional, la rendición de cuentas y los procesos de auditoría interna y externa.

23.1 Objetivo de los indicadores: El objetivo de los indicadores del PSPI es evaluar de manera objetiva y verificable:

- El grado de implementación de los lineamientos y controles definidos.
- La evolución del nivel de madurez en seguridad digital.
- La efectividad de la gestión de riesgos y de incidentes.
- El impacto de las acciones de capacitación y cultura organizacional.

23.2 Indicadores estratégicos: Empresas Públicas de Cundinamarca S.A. E.S.P define indicadores estratégicos orientados a medir el desempeño global del PSPI, entre los cuales se incluyen, como mínimo:

- Porcentaje de implementación de las acciones del PSPI frente al plan anual definido.
- Nivel de madurez alcanzado en el autodiagnóstico del PSPI.
- Grado de articulación del PSPI con el Plan Estratégico Institucional, el PETI y el PESI.

23.3 Indicadores de gestión operativa: Los indicadores de gestión operativa permiten evaluar la ejecución de los controles y actividades asociadas a la seguridad y privacidad de la información, incluyendo, entre otros:

- Porcentaje de activos de información identificados y clasificados.
- Porcentaje de incidentes de seguridad de la información atendidos dentro de los tiempos definidos.
- Tiempo promedio de atención de incidentes de seguridad de la información.
- Porcentaje de proveedores tecnológicos con obligaciones de seguridad verificadas.

23.4 Indicadores de capacitación y cultura organizacional: Estos indicadores permiten medir el nivel de apropiación del PSPI por parte de los actores institucionales, incluyendo:

- Porcentaje de funcionarios y contratistas capacitados en seguridad digital.
- Número de actividades de sensibilización realizadas en el periodo evaluado.
- Nivel de participación de las áreas institucionales en las actividades de cultura organizacional.

23.5 Fuentes de información y responsables: Los indicadores del PSPI se alimentan de fuentes de información tales como registros de la Mesa de Ayuda, informes del Proceso de Tecnologías de la Información, resultados del autodiagnóstico del PSPI, reportes de auditoría y evidencias documentales.

El Proceso de Tecnologías de la Información, bajo la coordinación del Coordinador de Tecnologías de la Información, es responsable de consolidar y reportar los indicadores, con el acompañamiento de la Dirección de Planeación.

23.6 Uso de los resultados: Los resultados de los indicadores del PSPI se utilizan como insumo para:

- La revisión por la dirección.
- La definición de acciones de mejora.
- El reporte institucional y los procesos de auditoría.
- El fortalecimiento de la gestión de la seguridad y privacidad de la información.

24. Seguimiento, Articulación con Auditorías Internas y Externas, e Indicadores de Evaluación

El seguimiento al PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P es un proceso permanente orientado a verificar su adecuada implementación, efectividad y alineación con la planeación institucional, la gestión del riesgo y los principios del Plan Integrado de Planeación y Gestión (MIPG), conforme a lo establecido en el Decreto 612 de 2018.

Este seguimiento se articula con los ejercicios de auditoría interna y externa, garantizando trazabilidad, transparencia y mejora continua en la gestión de la seguridad y privacidad de la información.

24.1 Mecanismos de seguimiento al PSPI: Empresas Públicas de Cundinamarca S.A. E.S.P realiza el seguimiento al PSPI a través de mecanismos formales y documentados, que incluyen, entre otros:

- Revisión periódica del avance en la implementación de los lineamientos y controles del PSPI.
- Análisis de los resultados de los indicadores de seguimiento y evaluación.
- Seguimiento a la gestión de riesgos de seguridad y privacidad de la información.
- Revisión de los resultados de la gestión de incidentes de seguridad de la información.

Estos mecanismos permiten identificar desviaciones, brechas y oportunidades de mejora en la gestión del PSPI.

24.2 Articulación con auditorías internas: La Dirección de Control Interno incorpora el PSPI dentro de su plan de auditoría, evaluando de manera independiente la efectividad de los controles, el cumplimiento normativo y la adecuada gestión de los riesgos de seguridad y privacidad de la información, los resultados de las auditorías internas se documentan mediante informes y planes de mejoramiento, los cuales deben ser atendidos por las instancias responsables, dejando evidencia verificable de las acciones correctivas implementadas.

24.3 Articulación con auditorías externas y entes de control: Empresas Públicas de Cundinamarca S.A. E.S.P atiende los requerimientos de auditorías externas y entes de control relacionados con la seguridad y privacidad de la información, suministrando la información y evidencia requerida de manera oportuna y trazable, los hallazgos y recomendaciones derivados de auditorías externas se integran al proceso de seguimiento del PSPI y se gestionan a través de planes de mejoramiento, en articulación con la Dirección de Planeación y la Dirección de Control Interno.

24.4 Indicadores de evaluación del PSPI: Los indicadores de evaluación permiten medir el desempeño del PSPI en términos de cumplimiento, efectividad y mejora continua. Estos indicadores se integran a los sistemas de seguimiento institucional y constituyen insumo para la toma de decisiones y la rendición de cuentas, los indicadores de evaluación se alinean con los definidos en el capítulo de indicadores de seguimiento y evaluación, garantizando coherencia y trazabilidad en la medición de resultados.

24.5 Uso de resultados y mejora continua: Los resultados del seguimiento, las auditorías y los indicadores de evaluación se utilizan para:

- Ajustar y fortalecer los controles del PSPI.
- Priorizar acciones de mejora y gestión del riesgo.
- Apoyar la revisión por la dirección y la toma de decisiones estratégicas.
- Fortalecer la transparencia y la rendición de cuentas institucional.

En este sentido, el seguimiento y la articulación con auditorías constituyen un pilar fundamental para la sostenibilidad y evolución del PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P.

25. Verificación, Revisión y Actualización

El PSPI en Empresas Públicas de Cundinamarca S.A. E.S.P es un instrumento dinámico que debe ser verificado, revisado y actualizado de manera periódica y extraordinaria, con el fin de asegurar su vigencia, pertinencia y efectividad frente a

los cambios normativos, organizacionales, tecnológicos y operativos que puedan impactar la seguridad y privacidad de la información.

25.1 Verificación del PSPI: La verificación del PSPI tiene como propósito comprobar el grado de cumplimiento de los lineamientos, controles y responsabilidades definidos, así como la efectividad de las medidas implementadas.

La verificación se realiza a través de:

- Seguimiento a los indicadores de desempeño del PSPI.
- Revisión de la gestión de riesgos y de incidentes de seguridad de la información.
- Resultados de auditorías internas y externas.
- Evaluaciones realizadas por la Dirección de Control Interno.

Los resultados de la verificación deben quedar debidamente documentados como evidencia de control y seguimiento institucional.

25.2 Revisión periódica del PSPI: El PSPI debe ser revisado de manera ordinaria con una periodicidad anual, en coherencia con el ciclo de planeación institucional y los resultados del autodiagnóstico del PSPI.

La revisión periódica incluye:

- Análisis del contexto institucional y del entorno normativo.
- Evaluación del nivel de madurez en seguridad digital.
- Revisión de la efectividad de los controles implementados.
- Identificación de brechas y oportunidades de mejora.

La revisión del PSPI es liderada por el Proceso de Tecnologías de la Información, bajo la coordinación del Coordinador de Tecnologías de la Información, con el acompañamiento de la Dirección de Planeación.

25.3 Revisión extraordinaria del PSPI: El PSPI podrá ser objeto de revisión extraordinaria cuando se presenten, entre otros, los siguientes eventos:

- Cambios relevantes en la normatividad aplicable.
- Modificaciones en la estructura organizacional de Empresas Públicas de Cundinamarca S.A. E.S.P.
- Implementación de nuevos sistemas, servicios tecnológicos o cambios significativos en la infraestructura.
- Incidentes de seguridad de la información de alto impacto.

- Recomendaciones derivadas de auditorías internas, externas o de entes de control.

25.4 Actualización del PSPI: Las actualizaciones del PSPI deberán formalizarse mediante control de cambios, indicando la versión, la fecha, la descripción del ajuste y los responsables, garantizando trazabilidad y control documental, toda actualización del PSPI debe ser aprobada por las instancias institucionales competentes y comunicada a las áreas involucradas, asegurando su adecuada aplicación y cumplimiento.

25.5 Articulación con la mejora continua: La verificación, revisión y actualización del PSPI se integran al ciclo Planear, Hacer, Verificar y Actuar (PHVA), permitiendo que los resultados del seguimiento, las auditorías y las evaluaciones se traduzcan en acciones concretas de mejora, fortaleciendo de manera progresiva la gestión de la seguridad y privacidad de la información en Empresas Públicas de Cundinamarca S.A. E.S.P.

26. Disposiciones Finales

El PSPI es de cumplimiento obligatorio para todos los funcionarios, contratistas, proveedores y terceros que gestionen, accedan o administren activos de información y recursos tecnológicos de Empresas Públicas de Cundinamarca S.A. E.S.P, en el marco de sus funciones o actividades contractuales.

La aplicación del PSPI tiene como finalidad fortalecer la protección de la información institucional, garantizar la continuidad de los procesos y servicios, asegurar el cumplimiento normativo y consolidar una gestión pública segura, transparente y orientada a resultados.

26.1 Obligatoriedad y alcance institucional: Las disposiciones contenidas en el PSPI son de obligatorio cumplimiento en todos los procesos, dependencias y niveles de la entidad, sin excEmpresas Públicas de Cundinamarca S.A. E.S.Pión. Su aplicación se extiende a todo el ciclo de vida de la información y a los servicios tecnológicos que soportan la gestión institucional.

26.2 Responsabilidad por el cumplimiento: La responsabilidad de coordinar la implementación, seguimiento y mejora continua del PSPI recae en el Coordinador de Tecnologías de la Información, en articulación con la Dirección de Planeación como dueña del proceso y con el apoyo operativo de la Mesa de Ayuda (MDA), las direcciones estratégicas, misionales y de apoyo son corresponsables del

cumplimiento del PSPI respecto de los activos de información bajo su custodia o gestión.

26.3 Publicación y divulgación: El PSPI y sus actualizaciones deberán ser divulgados a las áreas involucradas y puestos a disposición en los canales institucionales definidos, garantizando su conocimiento, aplicación y consulta para efectos de control y auditoría, en coherencia con la normatividad de transparencia y acceso a la información pública.

26.4 Incumplimiento: El incumplimiento de las disposiciones establecidas en el PSPI podrá dar lugar a las acciones administrativas, contractuales, disciplinarias o legales a que haya lugar, de conformidad con la normatividad vigente y los procedimientos institucionales aplicables.

26.5 Vigencia: El PSPI entra en vigencia a partir de su aprobación institucional y se mantendrá vigente hasta tanto sea modificado o actualizado conforme a los procedimientos de verificación, revisión y control de cambios definidos por Empresas Públicas de Cundinamarca S.A. E.S.P.

27. Control de Cambios

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**	**CARGO**
0	28/01/2026	Versión inicial	Diego Ernesto Guevara	Director de Planeación

PROYECTÓ	**REVISÓ**	**APROBÓ**
Nombre: Héctor Gil	Nombre: Carlos Garavito	Nombre: Diego Guevara
Cargo: Coordinador TI – Planeación	Cargo: Contratista- Planeación	Cargo: Director de Planeación
Dirección: Planeación	Subgerencia y/o Dirección: Planeación	Dirección: Planeación
Fecha: 28/01/2026	Fecha: 28/01/2026	Fecha: 28/01/2026

PLAN DE TRABAJO
Plan de Seguridad y Privacidad de la Información (PSPI)

OBJETIVO	Validar, formalizar y cerrar institucionalmente el PSPI, asegurando su correcta articulación con la planeación institucional, mediante la incorporación de observaciones institucionales, la definición de evidencias, el seguimiento a su implementación
JUSTIFICACIÓN	El Plan de Mejoramiento del PSPI se formula con el fin de garantizar que el modelo aprobado para la vigencia 2026 cuente con validación institucional, trazabilidad documental y evidencias de aplicación, conforme a los lineamientos del Decreto 612 de 2018 y el Modelo Integrado de Planeación y Gestión (MIPG), este plan permite
LIDER	Coordinador TIC
EQUIPO	Dirección de Planeación

28/1/2026

Item	Acción	Responsable	Producto	Fecha inicio	Fecha Fin	DIAS PARA EL CUMPLIMIENTO
1	Realizar el Autodiagnóstico de Gobierno Digital y Seguridad como insumo base para la actualización del PSPI.	Coordinador TIC Mesa de Ayuda (MDA)	Autodiagnóstico	1/02/2026	15/03/2026	46
2	Elaborar, actualizar y consolidar el Inventario de Activos de Información institucional.	Coordinador TIC Mesa de Ayuda (MDA)	Inventario de Activos de Información actualizado	1/02/2026	30/04/2026	92
3	Desarrollar y actualizar el contexto estratégico, alcance y partes interesadas del PSPI.	Coordinador TIC	Capítulo de contexto estratégico del PSPI	15/02/2026	15/04/2026	77
4	Realizar el diagnóstico de madurez en seguridad y privacidad de la información con base en el PSPI.	Coordinador TIC	Diagnóstico de madurez documentado	1/03/2026	30/04/2026	92
5	Identificar y actualizar los riesgos de seguridad y privacidad de la información.	Coordinador TIC	Matriz de riesgos de seguridad y privacidad	1/04/2026	31/05/2026	123
6	Formular y actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Coordinador TIC	Plan de Tratamiento de Riesgos actualizado	1/05/2026	30/06/2026	153
7	Actualizar los documentos institucionales relacionados con la seguridad y privacidad de la información, asegurando coherencia con el PSPI.	Coordinador TIC	Documentos relacionados actualizados y alineados	15/05/2026	31/08/2026	215
8	Actualizar los capítulos estructurales del PSPI	Coordinador TIC	Capítulos estructurales actualizados del PSPI	15/05/2026	31/08/2026	215
9	Definir, documentar y mantener el registro de incidentes de seguridad de la información conforme a los lineamientos del PSPI.	Coordinador TIC Mesa de Ayuda (MDA)	Registro de incidentes de seguridad de la información	1/06/2026	30/11/2026	306
10	Realizar el monitoreo y seguimiento periódico a la implementación del PSPI y a los controles definidos.	Coordinador TIC	Informes de seguimiento del PSPI	1/06/2026	30/11/2026	306
11	Socializar el PSPI con las dependencias con injerencia institucional para revisión y observaciones.	Coordinador TIC	Socialización del PSPI	1/07/2026	15/08/2026	199
12	Incorporar sugerencias y/o modificaciones recibidas por las dependencias; en caso de no recibir observaciones dentro del plazo establecido, se entenderá la aceptación del documento.	Coordinador TIC	PSPI ajustado	16/08/2026	15/09/2026	230
13	Consolidar la versión final del PSPI 2026, incorporando ajustes, control de cambios y trazabilidad documental.	Coordinador TIC	PSPI 2026 consolidado	16/09/2026	30/11/2026	306