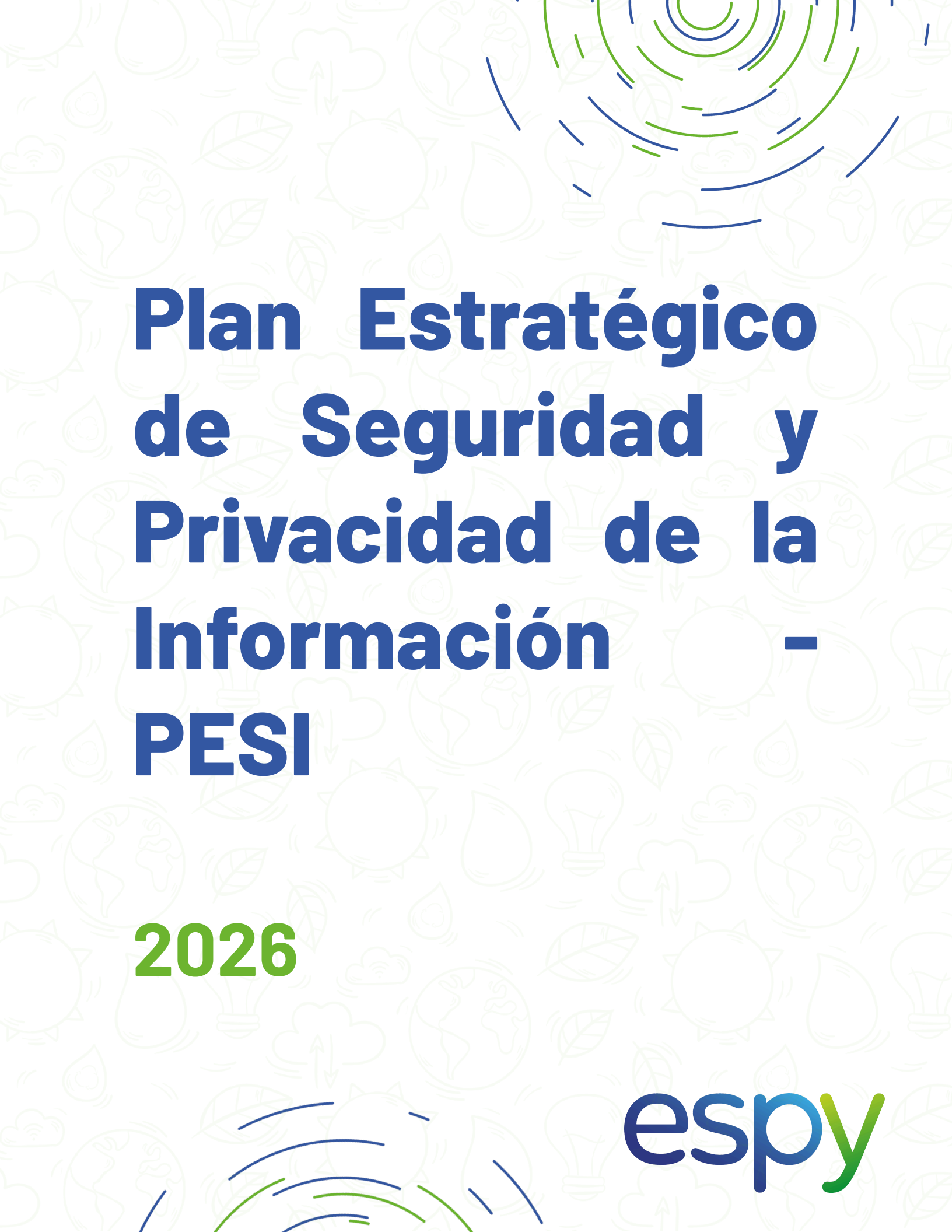




Plan Estratégico de Seguridad y Privacidad de la Información - PESI

2026

espy

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestion de Tecnologia	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

TABLA DE CONTENIDO

INTRODUCCIÓN.....	3
OBJETIVOS.....	4
OBJETIVOS ESPECÍFICOS.....	4
DIRECCIONAMIENTO ESTRATÉGICO.....	5
MISIÓN.....	5
VISIÓN.....	5
VALORES EMPRESARIALES.....	5
LÍNEAS ESTRATÉGICAS.....	5
OBJETIVOS ESTRATÉGICOS.....	5
ORGANIGRAMA.....	6
MAPA ESTRATÉGICO.....	6
ALCANCE DEL PLAN.....	9
NORMATIVIDAD.....	10
ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PESI)..	11
CONTEXTO Y ROLES RESPONSABLES.....	11
DIAGNÓSTICO DE SEGURIDAD (SITUACIÓN ACTUAL).....	11
POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD.....	12
PLAN DE PROYECTOS (FASE "HACER").....	12
ESTRATEGIA DE CULTURA Y CONCIENTIZACIÓN.....	13
MONITOREO Y REVISIÓN (FASE "VERIFICAR").....	14
PLAN DE ACCIÓN 2026.....	15
CONTROL DE CAMBIOS.....	16
APROBACIÓN.....	17

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

INTRODUCCIÓN

En cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y en concordancia con la estrategia de Gobierno Digital, se presenta el Plan de Seguridad y Privacidad de la Información (PESI). Este documento articula las directrices estratégicas orientadas a preservar la confidencialidad, integridad y disponibilidad de los activos de información, los cuales constituyen el recurso más crítico para la operación y la toma de decisiones de la entidad.

El PESI se fundamenta en un ciclo de mejora continua (Planear, Hacer, Verificar y Actuar), estableciendo un marco de control robusto para la protección de datos y la gestión de la ciberseguridad. Su implementación responde a la necesidad imperativa de blindar a la institución frente a un entorno de amenazas dinámicas, asegurando el cumplimiento normativo en materia de protección de datos personales y garantizando la confianza de los grupos de valor en los servicios tecnológicos ofrecidos.

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestion de Tecnologia	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

OBJETIVOS

Este plan busca la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando la protección de los activos.

Objetivo General: Implementar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, estableciendo un entorno de control robusto que garantice la confidencialidad, integridad y disponibilidad de los activos de información, en cumplimiento con la normativa legal vigente y las mejores prácticas internacionales.

OBJETIVOS ESPECÍFICOS

1. **Gestionar los Activos de Información:** Identificar, clasificar y proteger los activos de información críticos de la entidad (físicos y digitales) para asegurar que cuenten con los niveles de protección adecuados según su criticidad y sensibilidad.
2. **Fortalecer la Cultura de Ciberseguridad:** Ejecutar programas de concientización y formación dirigidos a funcionarios y contratistas para mitigar los riesgos derivados del factor humano (como ingeniería social o mal manejo de datos), promoviendo hábitos seguros en el manejo de la información.
3. **Asegurar el Cumplimiento y Mejora Continua:** Realizar auditorías periódicas y revisiones de cumplimiento para verificar la eficacia de los controles implementados, ajustando las políticas de seguridad frente a nuevas amenazas y cambios en el entorno tecnológico.

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

DIRECCIONAMIENTO ESTRATÉGICO

MISIÓN

Prestar de manera efectiva los servicios públicos domiciliarios de acueducto y saneamiento básico, con responsabilidad social y ambiental, acorde con las normas legales vigentes, buscando siempre mayor cobertura, continuidad y calidad en los servicios que prestamos a nuestros clientes.

VISIÓN

En 2035, la ESPY será una empresa líder, innovadora y sostenible, reconocida por la gestión integral del agua, el saneamiento básico y el aprovechamiento responsable de los recursos asociados, impulsando energías limpias, economía circular y servicios públicos de alta calidad que fortalecen el bienestar, el desarrollo territorial y la confianza de nuestros usuarios.

VALORES EMPRESARIALES

- Honestidad
- Respeto
- Compromiso
- Diligencia
- Justicia
- Solidaridad
- Tolerancia

LÍNEAS ESTRATÉGICAS

- **LE 1.** Gestión Gerencial Sostenible.
- **LE 2.** Gestión Integral de los Servicios Administrativos, Tecnológicos y de Bienestar Laboral.

OBJETIVOS ESTRATÉGICOS

- **OE 1.** Implementar una gestión gerencial sostenible que promueva el crecimiento institucional, garantice el cumplimiento de los procesos misionales y fortalezca la eficacia, eficiencia y efectividad en la prestación de los servicios de acueducto y alcantarillado en el territorio.

espy	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

- **OE 2.** Desarrollar una gestión integral que articule los procesos administrativos, tecnológicos y de bienestar laboral orientada al fortalecimiento institucional y al desarrollo eficiente, transparente y oportuno de los procesos de la entidad.

ORGANIGRAMA



MAPA ESTRATÉGICO

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

MAPA ESTRATÉGICO

MISIÓN

Prestar de manera efectiva los servicios públicos domiciliarios de acueducto y saneamiento básico, con responsabilidad social y ambiental, acorde con las normas legales vigentes, buscando siempre mayor cobertura, continuidad y calidad en los servicios que prestamos a nuestros clientes.

VALORES CORPORATIVOS

HONESTIDAD

RESPECTO

DILIGENCIA

SOLIDARIDAD

COMPROMISO

JUSTICIA

TOLERANCIA

LÍNEAS ESTRATÉGICAS

LÍNEA ESTRATÉGICA 1

Gestión Gerencial Sostenible

LÍNEA ESTRATÉGICA 2

Gestión Integral de los Servicios Administrativos, Tecnológicos y de Bienestar Laboral

OBJETIVOS ESTRATÉGICOS

OE 1

Implementar una gestión gerencial sostenible que promueva el crecimiento institucional, garantice el cumplimiento de los procesos misionales y fortalezca la eficacia, eficiencia y efectividad en la prestación de los servicios de acueducto y alcantarillado en el territorio.

OE 2

Desarrollar una gestión integral que articule los procesos administrativos, tecnológicos y de bienestar laboral orientada al fortalecimiento institucional y al desarrollo eficiente, transparente y oportuno de los procesos de la entidad.

ESTRATEGIAS

E1

Impulsar la gestión ambiental, social y económica, como herramientas para fortalecer la sostenibilidad de la entidad.

E2

Orientar a la empresa hacia la integración de los planes institucionales, con el fin de asegurar una planeación estratégica efectiva que impacte positivamente el ciclo de vida del servidor público y el fortalecimiento de los procesos misionales, garantizando así la transparencia y la satisfacción del usuario.



	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

ALCANCE DEL PLAN

El Plan de Seguridad y Privacidad de la Información (PESI) define el marco de actuación para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Su alcance comprende la protección de la confidencialidad, integridad y disponibilidad de todos los activos de información de la entidad, independientemente de su formato (físico, digital o verbal) o del medio por el cual se transmitan o almacenen.

Este alcance aplica a:

- **Personas:** Todos los funcionarios, contratistas, proveedores y terceros que tengan acceso a la información institucional.
- **Procesos:** Todos los procesos del mapa de procesos institucional, con énfasis en aquellos que manejan datos sensibles o críticos (como la operación de la PTAP y la gestión administrativa).
- **Tecnología:** Toda la infraestructura tecnológica, redes, sistemas de información, bases de datos y dispositivos móviles institucionales.
- **Normativa:** El cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales) y los lineamientos de Gobierno Digital.

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

NORMATIVIDAD

Tipo de Norma	Norma / Referencia	Descripción / Aplicación
Ley	Ley 1581 de 2012	Ley General de Protección de Datos Personales (Habeas Data). Obliga a la entidad a proteger los datos personales de usuarios y funcionarios.
Ley	Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal y se crea el bien jurídico tutelado de "la protección de la información y los datos" (Delitos Informáticos).
Ley	Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Define qué información debe ser pública y cuál es reservada/clasificada.
Decreto	Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012 en materia de protección de datos personales.
Estándar	NTC-ISO/IEC 27001:2013 / 2022	Norma técnica colombiana que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.
Circular	Circular Externa 005 de 2022 (SuperServicios)	(Sugerida) Directrices sobre ciberseguridad y protección de infraestructura crítica para empresas de servicios públicos (verificar aplicabilidad específica a ESPY).
Guía	Guía de Gestión de Riesgos de Seguridad (MinTIC)	Documento base que orienta la identificación y tratamiento de riesgos de seguridad digital.

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PESI)

CONTEXTO Y ROLES RESPONSABLES

Este plan establece el marco de gobierno para proteger la información de ESPY S.A. E.S.P. frente a amenazas internas y externas, garantizando la continuidad de la prestación de los servicios públicos.

Roles y Responsabilidades:

- **Comité Institucional de Gestión y Desempeño:** Instancia máxima de aprobación de las políticas de seguridad.
- **Oficial de Seguridad de la Información (CISO):** Responsable de coordinar la implementación del MSPI, reportar incidentes y monitorear riesgos. *(Nota: Si este cargo no existe, debe asignarse a un rol de liderazgo en TI o Control Interno).*
- **Líderes de Procesos:** Responsables de identificar los activos de información de sus áreas (ej. PTAP, Comercial) y aplicar los controles definidos.

DIAGNÓSTICO DE SEGURIDAD (SITUACIÓN ACTUAL)

Basado en el análisis de la infraestructura y los incidentes recientes, se presenta el siguiente diagnóstico:

Dominio	Hallazgo / Debilidad Identificada	Fuente
Gobierno de Seguridad	Inexistencia de políticas claras. No hay lineamientos formalizados sobre seguridad de la información.	Informe de la situación actual – Auditoría Externa
Gestión de Activos	Inventario desactualizado.	Informe de la situación actual – Auditoría Externa

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

Seguridad en Operaciones	Fuga de información y uso de canales no oficiales. Se evidencian incidentes relacionados con el uso de WhatsApp personal para transmitir información operativa confidencial (ej. caso PTAP Nuevo Horizonte).	Informe de la situación actual – Auditoría Externa
Recursos Humanos	Falta de cultura de seguridad. El personal operativo y administrativo carece de formación en riesgos digitales, lo que aumenta la vulnerabilidad ante ingeniería social.	Informe de la situación actual – Auditoría Externa

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD

Declaración de Política:

"La Alta Dirección de ESPY S.A. E.S.P. se compromete a proteger la confidencialidad, integridad y disponibilidad de los activos de información, mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la gestión de riesgos y la mejora continua. Se garantiza el cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales) y se prohíbe el uso de recursos tecnológicos institucionales para fines ajenos a la misión de la entidad."

PLAN DE PROYECTOS (FASE "HACER")

Este es el núcleo del PESI. Aquí se definen las acciones concretas para cerrar las brechas identificadas en el diagnóstico.

Eje 1: Fortalecimiento del Gobierno y Cumplimiento

- **Objetivo:** Establecer las reglas de juego.
- **Acción 1.1:** Elaboración y socialización del **Manual de Políticas de Seguridad de la Información** (Control de acceso, uso aceptable de activos, escritorio limpio).

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

- **Acción 1.2:** Implementación del procedimiento de **Protección de Datos Personales** (Avisos de privacidad, gestión de bases de datos registradas ante la SIC).

Eje 2: Gestión de Riesgos y Activos

- **Objetivo:** Identificar qué protegemos y de qué lo protegemos.
- **Acción 2.1:** Levantamiento del **Inventario de Activos de Información** clasificado por criticidad (Confidencial, Restringido, Público), incluyendo la información física de la PTAP.
- **Acción 2.2:** Elaboración del **Mapa de Riesgos de Seguridad Digital** siguiendo la metodología de la Guía de Gestión de Riesgos (Identificar, Analizar, Valorar y Tratar).

Eje 3: Seguridad Operativa y Tecnológica

- **Objetivo:** Implementar controles técnicos para evitar incidentes como el reportado en abril de 2023.
- **Acción 3.1:** Implementación de controles de **Acceso Lógico** (Políticas de contraseñas robustas y bloqueo de sesiones inactivas).
- **Acción 3.2:** Restricción de uso de medios extraíbles (USB) y software no autorizado en equipos críticos.
- **Acción 3.3:** Establecimiento de canales oficiales de comunicación (Correo institucional, herramientas colaborativas corporativas) para eliminar la dependencia de WhatsApp personal en procesos críticos.

ESTRATEGIA DE CULTURA Y CONCIENTIZACIÓN

Dado el incidente de fuga de información mencionado en los documentos, este componente es prioritario.

Cronograma de Sensibilización:

Temática	Público Objetivo	Frecuencia
Ingeniería Social y Phishing	Administrativos	Semestral

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestión de Tecnología	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

Uso Seguro de Dispositivos Móviles y Redes Sociales	Todos (Énfasis Operativos PTAP)	Trimestral
Ley de Protección de Datos (Habeas Data)	Atención al Cliente	Anual
Manejo de Contraseñas y Bloqueo de Equipos	Todos los funcionarios	Permanente (Boletines)

MONITOREO Y REVISIÓN (FASE "VERIFICAR")

Para asegurar que el PESI funciona, se medirán los siguientes indicadores:

1. **Porcentaje de implementación de controles:** (Controles implementados / Controles definidos en el plan de tratamiento) * 100.
2. **Número de incidentes de seguridad reportados:** Medición de incidentes de fuga de información o accesos no autorizados por semestre.
3. **Nivel de capacitación:** Porcentaje de funcionarios que aprobaron los cursos/talleres de seguridad.

Revisión por la Dirección:

El PESI será revisado anualmente o cuando ocurran cambios significativos en la infraestructura (como el cambio de proveedor de alquiler de equipos mencionado) para asegurar su vigencia.

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestion de Tecnologia	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

PLAN DE ACCIÓN 2026

Tema	Línea Base	Objetivo	Actividades	Medio de verificación	Fecha
Políticas de Seguridad (ISO 27001)	Existen controles técnicos pero falta formalidad (actos administrativos y políticas escritas).	Formalización Documental SGSI: Contar con el marco normativo interno aprobado.	Crear un documento de roles de seguridad y formalizar control de acceso.	Documento creado	JUNIO 30, 2026
Gestión de Activos	Inventario disperso y falta de política de reposición de equipos.	Control Total de Activos: Inventario centralizado y plan de reposición.	Crear un inventario de Hardware y Software en repositorio único.	Inventario creado	JUNIO 30, 2026
Copias de Seguridad	Backups dependen de proveedores o sincronización simple en Drive.	Backup Robusto: Estrategia de respaldo formalizada y probada.	Documentar un manual de restauración y copias de seguridad.	Manual creado	MAYO 30, 2026

	Planeación y Desarrollo Institucional	CÓDIGO: GPDI-GT-PL02
	Gestion de Tecnologia	VERSIÓN: 6
	Plan Estratégico de seguridad y Privacidad de la Información PESI	FECHA: Enero 23 de 2026

CONTROL DE CAMBIOS

Versión	Breve Descripción del Cambio	Fecha de Emisión
6	Modificación del documento para vigencia 2026 adoptado según resolución No. 1.33-022-1	23 enero 2026

APROBACIÓN

Elaboró	Revisó	Aprobó
<p>JAIME VELEZ ESCANDON</p> <p>PROFESIONAL ESPECIALIZADO GESTION DE TECNOLOGIA</p> <p>Original firmado en Oficina de Planeación y Desarrollo Institucional</p>	<p>ANA MARIA GONZALEZ JIMENEZ</p> <p>JEFE DE PLANEACIÓN Y DESARROLLO INSTITUCIONAL</p> <p>Original firmado en Oficina Asesora de Planeación y Proyectos</p>	<p>MARIA LYDA SERNA FAJARDO</p> <p>PRESIDENTE</p> <p>COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO</p> <p>Original firmado en Oficina Asesora de Planeación Proyectos y y Desarrollo Institucional</p>
Fecha: 23 enero 2026	Fecha: 23 enero 2026	Fecha: 23 enero 2026

