
Sistema Integral de Seguridad y Privacidad de la Información

2025

espy

	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Portada

- Título del Plan.
- Vigencia.
- Responsable del Plan. **Nombre del proceso**
- Fecha de Aprobación. **Exclusivo Oficina Asesora de Planeación Proyectos.**
- Código de Identificación del Documento. **Exclusivo Oficina Planeación.**



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Tabla de Contenido

Introducción	4
Propósito del Sistema	5
Objetivos	6
Objetivo General:	6
Objetivos Específicos:	6
Criterios de Medición:	6
Alcance del Plan	7
Normatividad	8
Direccionamiento Estratégico	9
Términos y Definiciones	11
Componentes del Sistema	13
Planes:	13
Plan Estratégico de Tecnologías de la Información y Comunicación (PETIC)	13
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)	14
6.3. Plan de Seguridad y Privacidad de la Información (PSPI)	15
Políticas:	15
Política de Gobierno Digital.	15
Política de Seguridad Digital	15
Política de Transparencia	16
Metas del Plan	17
Conclusiones	19
Seguimiento, Evaluación y Control	21
Anexos	24
Matriz de Riesgos de Seguridad y Privacidad de la Información	24
Política de Gobierno Digital.	24
Política de Seguridad Digital	24
Política de Transparencia	24

	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Introducción

En la Empresa Oficial de Servicios Públicos de Yumbo ESPY S.A. E.S.P., conscientes de la importancia vital de la información para la prestación de nuestros servicios públicos de acueducto y alcantarillado, presentamos el Sistema Integral de Seguridad y Privacidad de la Información (SISPI). Este sistema integral se define como un conjunto de políticas, procedimientos, controles y recursos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información que manejamos. Como proveedores de un servicio público esencial, manejamos una gran cantidad de datos sensibles, incluyendo información personal de nuestros usuarios, datos operativos de la infraestructura y datos financieros. La protección de esta información es fundamental para asegurar la continuidad del servicio, mantener la confianza de la comunidad y cumplir con las exigencias legales y regulatorias. El SISPI surge como respuesta a la necesidad de fortalecer nuestra postura frente a las crecientes amenazas cibernéticas y los riesgos asociados a la privacidad de la información. Este sistema abarca todas las áreas de la empresa que manejan información, buscando establecer un marco integral que nos permita gestionar de manera efectiva los riesgos y garantizar la seguridad y privacidad de nuestros activos de información.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Propósito del Sistema

El SISPI busca generar un impacto positivo en la empresa al fortalecer su postura de seguridad y privacidad, minimizando riesgos operativos, legales y reputacionales. Se espera mejorar la eficiencia en la gestión de la información, optimizar la respuesta ante incidentes y asegurar la continuidad del servicio público esencial que proporciona la empresa. Este sistema es relevante porque protege un activo crítico como la información, esencial para la toma de decisiones, la operación y la interacción con los usuarios.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Objetivos

Objetivo General:

Implementar un SISPI que garantice la confidencialidad, integridad y disponibilidad de la información, cumpliendo con la normatividad vigente y protegiendo los activos de la empresa.

Objetivos Específicos:

- Establecer políticas y procedimientos de seguridad y privacidad.
- Implementar controles técnicos para proteger la infraestructura y los datos.
- Capacitar al personal en materia de seguridad y privacidad.
- Gestionar los riesgos de seguridad y privacidad de forma proactiva.
- Establecer un sistema de monitoreo y respuesta a incidentes.

Criterios de Medición:

- Número de incidentes de seguridad reportados.
- Nivel de cumplimiento de las políticas de seguridad.
- Porcentaje de personal capacitado en seguridad y privacidad.
- Tiempo de respuesta ante incidentes.
- Resultados de auditorías de seguridad.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Alcance del Plan

Áreas de Influencia: Todas las áreas de la empresa que manejan información, incluyendo (pero no limitado a) áreas operativas, administrativas, financieras, de recursos humanos y de atención al cliente.

Población Objetivo: Todos los empleados, contratistas, proveedores y usuarios que interactúan con los sistemas de información de la empresa.

Restricciones: Presupuesto asignado, cronograma de implementación, disponibilidad de recursos humanos, compatibilidad con sistemas existentes.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Normatividad

Normativa	Descripción
Ley 1581 de 2012	Establece los principios y derechos relacionados con el tratamiento de datos personales.
Normas ISO 27001/27002	Estándares internacionales para la gestión de la seguridad de la información.
Normativa sectorial.	Regulaciones específicas del sector de acueducto y alcantarillado en materia de seguridad y privacidad de la información.
Ley 594 de 2000	Normas relacionadas con la gestión documental y la preservación de la información.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

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:**

- Ser en el año 2025 una empresa líder en materia de prestación de servicios públicos domiciliarios en el municipio de Yumbo, cubriendo las demandas de los servicios prestados en forma oportuna y suficiente.

- **Valores Empresariales:**

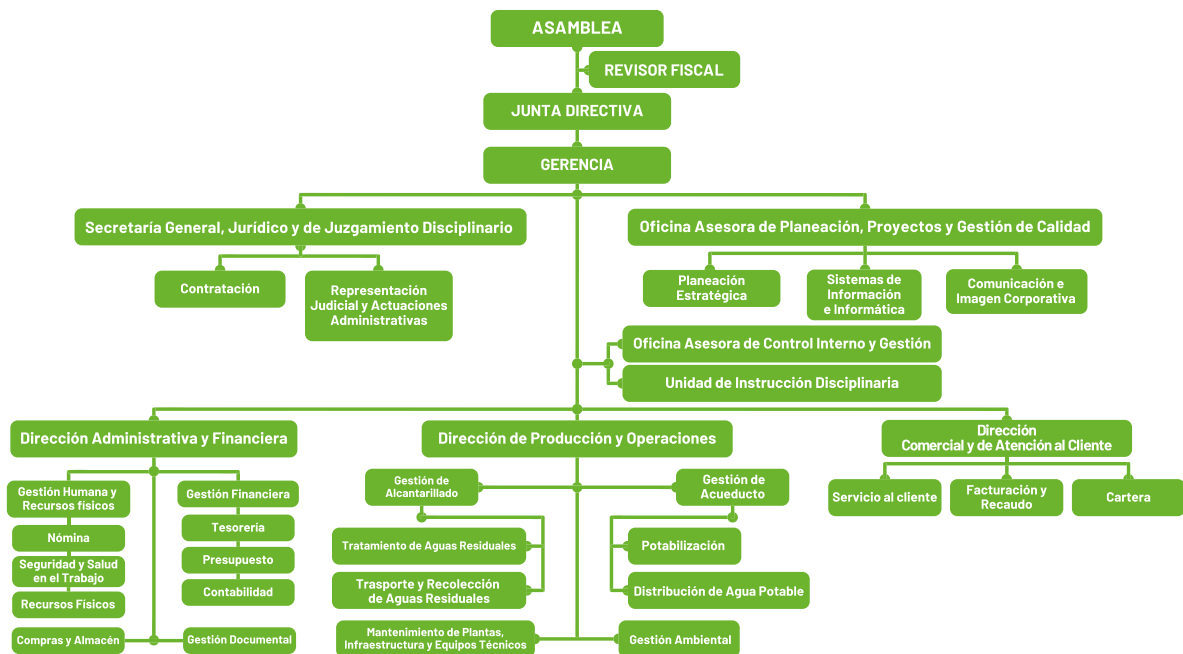
- **Ambiente:** Somos guardianes del medio ambiente. Nos esforzamos por minimizar nuestro impacto ambiental y promover prácticas responsables en cada aspecto de nuestros servicios.
- **Diligencia:** Trabajamos con diligencia para brindarte servicios públicos de calidad. Nos esforzamos en cumplir con eficiencia y rapidez, garantizando que tus necesidades sean atendidas con prontitud.
- **Honestidad:** Operamos con transparencia y sinceridad en todo lo que hacemos, construyendo relaciones de confianza y credibilidad duraderas.
- **Compromiso:** Nuestro compromiso es contigo. Trabajamos incansablemente para proporcionar servicios sostenibles que mejoren tu calidad de vida y cuiden nuestro planeta.
- **Respeto:** En nuestra empresa, el respeto es la base de todas nuestras interacciones. Valoramos a cada cliente y colega, fomentando un ambiente de cordialidad y consideración en cada paso que damos.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

- **Justicia:** Promovemos la justicia en todos nuestros procesos. Buscamos equidad en la distribución de servicios, garantizando que cada individuo reciba un trato justo y equitativo.

- **Organigrama:**



- **Estrategias Clave:** Enlazar los valores y la misión con acciones concretas para orientar el cumplimiento del plan.

	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Términos y Definiciones

Para el desarrollo del presente sistema, es importante tener en cuenta las definiciones que a continuación se establecen en concordancia con lo estipulado por el Departamento Administrativo de la Función Pública -DAFP.

Factores de riesgos: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad.

Impacto: Es la medición y valoración del daño que podría producir a la empresa un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

Riesgo: Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Seguridad: Calidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Seguridad física: Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir procesamiento de información.

Seguridad lógica: Consiste en la aplicación de barreras y procedimientos para mantener la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Seguridad de las redes: Es la capacidad de las redes para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles y que son tan costosos como los ataques intencionados.

Seguridad Informática: Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Vulnerabilidad: Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Componentes del Sistema

Planes:

Plan Estratégico de Tecnologías de la Información y Comunicación (PETIC)

- **Diagnóstico:**
 - Análisis del inventario de hardware y software.
 - Evaluación de la infraestructura de red y comunicaciones.
 - Revisión de la arquitectura de sistemas y bases de datos.
 - Identificación de brechas tecnológicas y oportunidades de mejora.
- **Metodología:**
 - Análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas).
 - Definición de objetivos estratégicos de TI alineados con el negocio.
 - Elaboración de un plan de acción con cronograma y presupuesto.
- **Programas, Objetivos, Metas e Indicadores:**
 - **Objetivo:** Modernizar la infraestructura tecnológica.
 - **Meta:** Crear un plan de modernización tecnológica en 12 meses.
 - **Indicador:** Porcentaje de implementación del plan de modernización tecnológica.
- **Actividades y Responsables:**

Actividad	Responsable	Inicio	Fin
Análisis del estado actual de la infraestructura.	Área de Sistemas de Información e Informática – Contratista externo.	2025-05-01	2025-06-01
Definición del plan.	Área de Sistemas de Información e Informática	2025-06-05	2025-07-05
Crear el plan.	Área de Sistemas de Información e Informática	2025-07-10	2025-11-10



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Implementar el plan.	Área de Sistemas de Información e Informática	2025-11-15	2025-12-15
----------------------	---	------------	------------

- **Entregables:** Documento del PETIC, inventario actualizado de TI, plan de modernización tecnológica, informe de capacitación.
- **Grupo de Interés Beneficiado:** Toda la empresa, especialmente las áreas operativas y de gestión.

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)

- **Diagnóstico:**
 - Identificación de activos de información críticos.
 - Análisis de amenazas y vulnerabilidades.
 - Evaluación del impacto potencial de los riesgos.
- **Metodología:**
 - Metodologías de gestión de riesgos como ISO 31000 o Magerit.
 - Priorización de riesgos según su probabilidad e impacto.
 - Definición de controles para mitigar los riesgos.
- **Programas, Objetivos, Metas e Indicadores:**
 - **Objetivo:** Reducir el riesgo de pérdida de datos sensibles.
 - **Meta:** Implementar controles de acceso reforzados en 6 meses.
 - **Indicador:** Número de accesos no autorizados a datos sensibles.
- **Actividades y Responsables:**

Actividad	Responsable	Inicio	Fin
Evaluación de riesgos	Área de Sistemas de Información e Informática	2025-01-15	2025-02-15
Pruebas de penetración	Auditor externo de Seguridad	2025-04-25	2025-05-25

- **Entregables:** Matriz de riesgos, plan de tratamiento de riesgos, informe de pruebas de penetración.

	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

- **Grupo de Interés Beneficiado:** Toda la empresa, especialmente la alta dirección y el área legal.

6.3. Plan de Seguridad y Privacidad de la Información (PSPI)

- **Diagnóstico:**
 - Revisión de políticas y procedimientos de seguridad existentes.
 - Análisis de incidentes de seguridad previos.
 - Evaluación del cumplimiento normativo en materia de privacidad.
- **Metodología:**
 - Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001.
 - Definición de políticas, procedimientos y controles de seguridad.
 - Establecimiento de un programa de capacitación y concientización.
- **Programas, Objetivos, Metas e Indicadores:**
 - **Objetivo:** Fortalecer la cultura de seguridad en la empresa.
 - **Meta:** Capacitar al 100% del personal en seguridad y privacidad en 3 meses.
 - **Indicador:** Porcentaje de personal capacitado.
- **Actividades y Responsables:**

Actividad	Responsable	Inicio	Fin
Elaboración de políticas de privacidad	Oficial de Privacidad	2024-06-01	2024-07-01
Diseño del programa de capacitación	Recursos Humanos	2024-07-05	2024-08-05
Ejecución de las capacitaciones	Contratista externo - Área de Sistemas de Información e Informática	2024-08-10	2024-09-10

Políticas:

Política de Gobierno Digital.

Ver Anexo No. 2, 8. ESTRATEGIA GOBIERNO DIGITAL.docx

Política de Seguridad Digital.

Ver Anexo No. 3, 9. ESTRATEGIA SEGURIDAD DIGITAL.docx



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Política de Transparencia.

Ver Anexo No. 4, 8. ESTRATEGIA POLITICA TRANSPARENCIA.docx



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Metas del Plan

A continuación, encontrará la matriz de seguimiento a las metas y actividades del sistema.

META	TIPO DE META	INDICADOR	DESCRIPCIÓN DEL INDICADOR	LINEA BASE	CANTIDAD PROGRAMADA A 2025	ACTIVIDADES PROGRAMADAS	RESPONSABLES
ADOPTAR EL SISTEMA INTEGRAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	MI	Plan Adoptado	N/A	0	100%	Crear el Sistema Integral de Seguridad y Privacidad de la Información. Adoptar el Sistema Integral de Seguridad y Privacidad de la Información	Sistemas de Información e Informática / Planeación
IMPLEMENTAR EL 100% DE LAS ACTIVIDADES DEL PETIC	MI	AVANCES DE IMPLEMENTACIÓN DEL PLAN SEGÚN AVANCE DE ACTIVIDADES	(ACTIVIDADES EJECUTADAS/ ACTIVIDADES PROGRAMADAS) * 100	0%	100%	Realizar un (1) diagnóstico de la situación actual de la infraestructura tecnológica de la empresa. Elaborar un (1) Plan de Modernización tecnológica el cual constara de 3 fases. Implementar fase 1 del Plan de Modernización tecnológica.	Sistemas de Información e Informática / Planeación
IMPLEMENTAR EL 100% DE LAS ACTIVIDADES DEL PTRSPI	MI	AVANCES DE IMPLEMENTACIÓN DEL PLAN SEGÚN AVANCE DE ACTIVIDADES	(ACTIVIDADES EJECUTADAS/ ACTIVIDADES PROGRAMADAS) * 100	0%	100%	Elaborar una (1) matriz de evaluación de Riesgos. Elaborar un (1) informe de vulnerabilidades de riesgos de seguridad y privacidad de los sistemas de negocio de la empresa.	Sistemas de Información e Informática / Planeación

	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

IMPLEMENTAR EL 100% DE LAS ACTIVIDADES DEL PSPI	MI	AVANCES DE IMPLEMENTACIÓN DEL PLAN SEGÚN AVANCE DE ACTIVIDADES	(ACTIVIDADES EJECUTADAS/ ACTIVIDADES PROGRAMADAS) * 100	0%	100%	Elaborar una (1) política en materia de privacidad de la información.	Sistemas de Información e Informática / Planeación
						Realizar un (1) diagnostico seguridad y privacidad de la información.	

	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Conclusiones

La implementación del SISPI representa una inversión estratégica esencial para ESPY S.A. E.S.P. Este sistema no solo responde a las exigencias normativas y a la creciente complejidad de las amenazas cibernéticas, sino que también fortalece la resiliencia de la organización frente a posibles incidentes de seguridad y privacidad. Al establecer un marco integral de políticas, procedimientos y controles, el SISPI busca garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando riesgos operativos, legales, financieros y reputacionales. En última instancia, el SISPI contribuye a la sostenibilidad de la empresa y a la prestación continua de un servicio público esencial para la comunidad.

Puntos Clave que Refuerzan la Conclusión:

- **Protección de la información sensible:** El SISPI protege la información personal de los usuarios, los datos operativos de la infraestructura, la información financiera y otros datos críticos para la empresa, previniendo accesos no autorizados, pérdidas o alteraciones.
- **Cumplimiento normativo:** El sistema asegura el cumplimiento de las leyes y regulaciones vigentes en materia de protección de datos personales y seguridad de la información, evitando sanciones legales y protegiendo la reputación de la empresa.
- **Continuidad del negocio:** Al mitigar los riesgos de seguridad y privacidad, el SISPI contribuye a la continuidad de las operaciones de la empresa, asegurando la prestación ininterrumpida del servicio público.
- **Fortalecimiento de la confianza:** La implementación del SISPI demuestra el compromiso de la empresa con la seguridad y privacidad de la información, fortaleciendo la confianza de los usuarios, los empleados y otras partes interesadas.
- **Mejora de la eficiencia:** La gestión eficiente de la información, facilitada por el SISPI, puede contribuir a la optimización de los procesos internos y a la toma de decisiones informadas.
- **Cultura de seguridad:** El programa de capacitación y concientización incluido en el SISPI fomenta una cultura de seguridad en la empresa, donde todos los empleados comprenden su rol en la protección de la información.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

- **Enfoque preventivo y proactivo:** El SISPI no solo se centra en la respuesta a incidentes, sino también en la prevención y la gestión proactiva de riesgos, anticipándose a posibles amenazas.

Recomendación Final:

Se enfatiza la importancia de la implementación, el seguimiento continuo y la evaluación periódica del SISPI. La adaptación a los cambios en el entorno tecnológico y regulatorio, así como la actualización constante de las políticas y los controles, son cruciales para mantener la eficacia del sistema a largo plazo. El compromiso continuo de la alta dirección y la participación de todos los empleados son fundamentales para el éxito del SISPI y para la protección efectiva de la información en ESPY S.A. E.S.P.

En resumen, el SISPI representa una inversión estratégica que protege el activo más valioso de la empresa: la información. Su implementación efectiva no solo mitiga riesgos, sino que también genera valor al fortalecer la confianza, mejorar la eficiencia y asegurar la continuidad del negocio.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Seguimiento, Evaluación y Control

Seguimiento:

El seguimiento es un proceso continuo y sistemático de recolección de información sobre el progreso del SISPI, comparándolo con los objetivos y metas establecidos. Se enfoca en monitorear la implementación de los planes (PETIC, PTRSPI, PSPI) y la efectividad de los controles de seguridad y privacidad.

- **Indicadores Clave de Desempeño (KPIs):** Se definirán KPIs específicos para cada plan y para el SISPI en general.
 - Número de incidentes de seguridad reportados (por tipo y severidad).
 - Tiempo medio de resolución de incidentes.
 - Porcentaje de cumplimiento de las políticas de seguridad (medido a través de auditorías o autoevaluaciones).
 - Número de evaluaciones de vulnerabilidad realizadas.
 - Porcentaje de personal capacitado en seguridad y privacidad.
 - Nivel de satisfacción de los usuarios con los servicios de TI (relacionado con la seguridad).
- **Recolección de Datos:** Se utilizarán diversas fuentes para recopilar datos, incluyendo:
 - Sistemas de gestión de incidentes de seguridad.
 - Registros de auditorías y pruebas de penetración.
 - Informes de monitoreo de seguridad (SIEM, firewalls, etc.).
 - Encuestas de satisfacción a usuarios.
 - Revisiones periódicas de políticas y procedimientos.
- **Frecuencia del Seguimiento:** El seguimiento se realizará de forma continua, con revisiones periódicas (mensuales, trimestrales) para analizar las tendencias y tomar acciones correctivas.

Evaluación:

La evaluación se centra en analizar el impacto del SISPI en el logro de sus objetivos y en la identificación de áreas de mejora. Se realiza de forma periódica (anual o bianual) y puede incluir evaluaciones internas y externas.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

- **Tipos de Evaluación:**
 - **Autoevaluación:** Realizada por el equipo interno responsable del SISPI.
 - **Auditorías Internas:** Realizadas por la unidad de auditoría interna de la empresa.
 - **Auditorías Externas:** Realizadas por una empresa independiente especializada en seguridad de la información.
- **Criterios de Evaluación: Se evaluará el SISPI en función de:**
 - El cumplimiento de los objetivos estratégicos.
 - La eficacia de los controles de seguridad y privacidad.
 - El cumplimiento de la normatividad vigente.
 - La gestión de riesgos.
 - La eficiencia en la gestión de incidentes.
 - La satisfacción de los usuarios.
- **Metodologías de Evaluación: Se pueden utilizar diferentes metodologías, como:**
 - Análisis de brechas.
 - Análisis costo-beneficio.
 - Análisis de riesgos residuales.
 - Comparación con mejores prácticas (benchmarking).

Control:

El control se refiere a las acciones que se toman para corregir desviaciones, mejorar el desempeño del SISPI y asegurar el cumplimiento de sus objetivos.

- **Acciones Correctivas:** Se implementarán acciones correctivas basadas en los resultados del seguimiento y la evaluación. Estas acciones pueden incluir:
 - Modificación de políticas y procedimientos.
 - Implementación de nuevos controles de seguridad.
 - Capacitación adicional al personal.
 - Ajustes en la infraestructura tecnológica.
- **Gestión del Cambio:** Se implementará un proceso de gestión del cambio para asegurar la correcta implementación de las acciones correctivas y la adaptación del SISPI a los cambios en el entorno.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

- **Responsabilidades:** Se definirán claramente las responsabilidades para el seguimiento, la evaluación y el control del SISPI. Se recomienda la creación de un Comité de Seguridad y Privacidad que supervise estas actividades.

Documentación:

Se mantendrá una documentación completa del SISPI, incluyendo:

- Políticas y procedimientos.
- Planes (PETIC, PTRSPI, PSPI).
- Informes de seguimiento y evaluación.
- Registros de auditorías.
- Registros de incidentes de seguridad.
- Planes de acción correctiva.

Mejora Continua:

El seguimiento, la evaluación y el control son la base para la mejora continua del SISPI. Se utilizarán los resultados de estas actividades para identificar áreas de mejora, implementar cambios y asegurar que el sistema se mantenga actualizado y eficaz frente a las nuevas amenazas y los cambios en el entorno.



	Oficina Asesora de Planeación, Proyectos y Gestión de Calidad	CÓDIGO: Espacio exclusivo oficina Planeación.
	Sistemas de Información e Informática	VERSIÓN: 1.0
	Sistema Integral de Seguridad y Privacidad de la Información	FECHA: 31 de enero de 2024

Anexos

Matriz de Riesgos de Seguridad y Privacidad de la Información

Ver Anexo No. 1, MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – 2025.xlsx

Política de Gobierno Digital.

Ver Anexo No. 2, 8. ESTRATEGIA GOBIERNO DIGITAL.docx

Política de Seguridad Digital.

Ver Anexo No. 3, 9. ESTRATEGIA SEGURIDAD DIGITAL.docx

Política de Transparencia.

Ver Anexo No. 4, 8. ESTRATEGIA POLITICA TRANSPARENCIA.docx

