EMPRESA DE SERVICIOS PÚBLICOS DE SABANETA

PLAN DE SEGURIDAD Y TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN

GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES
DIRECCIÓN DE PROYECTOS

EMPRESA DE SERVICIOS PÚBLICOS DE SABANETA E.S.P – EAPSA
Vigencia: 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Seguridad y Tratamiento de Riesgos y Privacidad de la Información de la Empresa de Servicios Públicos de Sabaneta E.S.P. – EAPSA establece el marco estratégico, técnico y operativo para la adecuada gestión de la seguridad de la información, la ciberseguridad y la protección de los datos personales.

Este plan responde a los desafíos actuales asociados al uso intensivo de las tecnologías de la información, al incremento de amenazas cibernéticas, a las exigencias normativas vigentes y a la necesidad de garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional, asegurando la continuidad y calidad en la prestación de los servicios públicos.

2. OBJETIVO GENERAL

Fortalecer y consolidar el Sistema de Gestión de Seguridad de la Información (SGSI) de EAPSA mediante la identificación, análisis, tratamiento y seguimiento de los riesgos que puedan afectar la seguridad de la información y la privacidad de los datos personales, garantizando el cumplimiento normativo, la continuidad operativa

○ Objetivos Específicos

- Identificar, analizar y priorizar los riesgos de seguridad de la información y ciberseguridad.
- Proteger los activos de información críticos de la entidad.
- Fortalecer la cultura organizacional en seguridad y privacidad de la información.
- Garantizar el tratamiento adecuado de los datos personales conforme a la normativa vigente.
- Asegurar la continuidad de los servicios y la capacidad de recuperación ante incidentes.
- Mantener la alineación con el MIPG, el MSPI y los estándares internacionales aplicables.

3. ALCANCE

El presente plan aplica a todos los procesos, dependencias, funcionarios, contratistas y terceros que tengan acceso, gestionen o administren información de EAPSA, independientemente del medio en el que esta se encuentre.

4. METODOLOGÍA DE IMPLEMENTACIÓN

Para la vigencia 2026, la Empresa de Servicios Públicos de Sabaneta E.S.P. – EAPSA implementará el Plan de Seguridad y Tratamiento de Riesgos y Privacidad de la Información bajo el enfoque del ciclo PHVA (Planear, Hacer, Verificar y Actuar), garantizando su alineación con el Plan Estratégico Institucional, el Modelo Integrado de Planeación y Gestión – MIPG y el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio TIC.

Las fases de implementación son:

1. Diagnosticar.

2. Planear.
3. Hacer.
4. Verificar.
5. Actuar.

Este enfoque permite una gestión sistemática, preventiva y orientada a resultados frente a los riesgos de seguridad de la información, ciberseguridad y protección de datos personales.

5. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con las fases mencionadas, EAPSA desarrollará los siguientes dominios estratégicos de seguridad de la información:

- Política de Seguridad y Privacidad de la Información.
- Gobierno de la Seguridad de la Información.
- Gestión de Riesgos de Seguridad de la Información y Ciberseguridad.
- Gestión y Clasificación de Activos de Información.
- Seguridad ligada al Talento Humano y Cultura Organizacional.
- Gestión de Identidades y Controles de Acceso.
- Seguridad en Infraestructura Tecnológica, Telecomunicaciones y Servicios Digitales.
- Gestión de Incidentes de Seguridad de la Información.
- Continuidad del Negocio y Recuperación ante Desastres.
- Gestión de Proveedores y Terceros.
- Protección de Datos Personales y Privacidad de la Información.

6. ENTREGABLES

- **Fase I y II (Diagnóstico – Planeación)**

- Diagnóstico del estado actual del Sistema de Gestión de Seguridad de la Información – SGSI.
- Definición y actualización del alcance del SGSI.
- Actualización y aprobación del Manual de Políticas de Seguridad y Privacidad de la Información.

- Inventario y clasificación de activos de información según criticidad. Análisis de riesgos de seguridad de la información.
- Matriz de riesgos y plan de tratamiento de riesgos.
- Declaración de aplicabilidad. Matriz de cumplimiento normativo (ISO 27001:2022, MSPI, MIPG, Ley 1581 de 2012).

  - **FASE III (IMPLEMENTACIÓN)**

- Documento de planificación y control operacional del SGSI.
- Implementación de los controles definidos en el plan de tratamiento de riesgos.
- Gestión y análisis de vulnerabilidades técnicas.
- Resultados de pruebas y análisis de vulnerabilidades.
- Entrevistas y validaciones con líderes de proceso y responsables tecnológicos.
- Actualización de la matriz de riesgos.
- Indicadores de gestión, cumplimiento y madurez del SGSI.
- Evidencias de implementación de controles.

  - **FASE IV (EVALUACIÓN DEL DESEMPEÑO DE LA SEGURIDAD IMPLEMENTADA)**

- Evaluación integral del desempeño del SGSI.
- Seguimiento y evaluación del plan de tratamiento de riesgos.
- Análisis del riesgo residual.

  - **FASE V (MEJORA CONTINUA)**

- Plan de seguimiento, evaluación y análisis del SGSI.
- Auditoría interna del Sistema de Gestión de Seguridad de la Información.
- Formulación y ejecución del plan de mejoramiento.
- Comunicación de resultados.
- Plan anual de comunicación, sensibilización y capacitación en seguridad de la información.

7. ARTICULACIÓN CON EL PLAN ACCIÓN GERENCIAL

El presente plan se articula directamente con el Plan Estratégico de EAPSA E.S.P, contribuyendo al fortalecimiento del gobierno digital, la gestión del riesgo, la continuidad de los servicios públicos y la confianza de los ciudadanos.

Las acciones definidas en este plan aportan al cumplimiento de los objetivos estratégicos relacionados con:

- Modernización institucional.
- Gestión eficiente del riesgo.
- Transparencia y protección de la información.
- Continuidad y calidad en la prestación de los servicios públicos.

8. SEGUIMIENTO, INDICADORES Y CONTROL

El seguimiento al Plan de Seguridad y Tratamiento de Riesgos y Privacidad de la Información se realizará de manera trimestral, mediante indicadores alineados al Plan Estratégico Institucional, MIPG y el Sistema de Control Interno.

Acciones a realizar:

- Seguimiento a indicadores frente a riesgos identificados.
- Seguimiento a nivel de cumplimiento del plan de tratamiento de riesgos.
- Seguimiento a número de incidentes de seguridad de la información.
- Capacitación a funcionarios y contratistas en seguridad de la información.

9. CONSULTAS

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000)

Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley1712 de 2014, art 6).

Indicadores: son herramientas (cuantitativas o cualitativas) que miden el progreso hacia objetivos, evalúan el desempeño, simplifican la complejidad de los datos y guían la toma de decisiones, mostrando si las estrategias funcionan, si se cumplen metas y si los procesos operan eficientemente

Matriz de riesgos: es una herramienta visual y práctica que ayuda a una entidad a identificar, evaluar y priorizar los peligros y riesgos a los que se enfrenta, clasificándolos según su probabilidad de ocurrencia y el impacto que tendrían, usando colores (rojo, amarillo, verde) para visualizar rápidamente cuáles son críticos y necesitan atención inmediata, facilitando así la toma de decisiones y la asignación de recursos para controlarlos o mitigarlos.

JUAN PABLO ARROYAVE ROMAN
Gerente
Empresa de Servicios Públicos de Sabaneta E.S.P – EAPSA