Plan Estratégico de Seguridad y Privacidad de la Información
Indeportes Antioquia

Fecha de elaboración: enero 2026

1. Introducción

La información es uno de los activos más valiosos para Indeportes Antioquia, pues soporta los procesos misionales, estratégicos y de apoyo que permiten cumplir su función institucional de fomentar, organizar, financiar y promover la actividad física, la recreación y el deporte en el departamento. La creciente transformación digital de la entidad, la ampliación de los servicios electrónicos, la adopción de nuevas tecnologías, así como el aumento de amenazas cibernéticas, obligan a fortalecer de manera integral la gestión de la seguridad y privacidad de la información.

En respuesta a este contexto, el presente Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) establece la hoja de ruta institucional para la implementación y consolidación del Modelo de Seguridad y Privacidad de la Información – MSPI, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) en la Resolución 500 de 2021. Este plan articula las necesidades, retos, requerimientos regulatorios y brechas identificadas en los diagnósticos institucionales, el FURAG, los análisis de riesgos y los instrumentos de planeación estratégica vigentes, particularmente el Plan Estratégico de Tecnología de la Información – PETI 2025–2027.

El PESPI presenta las estrategias, proyectos, responsables, recursos y mecanismos de seguimiento necesarios para fortalecer la confidencialidad, integridad y disponibilidad de la información, así como para garantizar que los servicios tecnológicos y la operación institucional se desarrollen en un ambiente seguro y resiliente. De igual forma, orienta el desarrollo de capacidades en liderazgo, cultura organizacional, gestión del riesgo, implementación de controles y atención de incidentes, permitiendo que la seguridad de la información se convierta en un habilitador de la innovación, la eficiencia administrativa y la confianza ciudadana.

Este plan se constituye en un instrumento vivo y dinámico, que deberá ser revisado y ajustado periódicamente para responder a la evolución del riesgo, las exigencias normativas, la gestión institucional y el avance del MSPI. Su implementación requiere el compromiso de la alta dirección, los líderes de proceso, el equipo TIC, los proveedores y todos los servidores de Indeportes Antioquia, bajo el principio de que la seguridad de la información es una responsabilidad compartida.

2. Objetivo General

Fortalecer la seguridad de la Información de la entidad, mediante la implementación progresiva del Modelo de Seguridad y Privacidad de la Información (MSPI) y la adopción de un programa integral de seguridad de la información que cierre las brechas identificadas en la preauditoria ISO/IEC 27001:2022 realizada en el 2025, que permitan reducir los riesgos institucionales a niveles aceptables y garantizar la continuidad de los servicios y procesos misionales y cumpla los lineamientos del MSPI actualizado por la Resolución 02277 de 2025.

3. Objetivos específicos

- Definir y establecer la estrategia institucional de seguridad digital, orientada por los lineamientos del MSPI, la Resolución 500 de 2021 y el marco normativo vigente en materia de seguridad y privacidad de la información.
- Identificar las necesidades, brechas, capacidades y recursos requeridos para la implementación, operación y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).
- Priorizar los proyectos e iniciativas estratégicas necesarios para el fortalecimiento de la seguridad digital, la gestión de riesgos, la implementación de controles y la atención de incidentes.
- Planificar, evaluar y monitorear el avance, la eficacia y la sostenibilidad de los controles, lineamientos, políticas y actividades ejecutadas en el marco del SGSPI, asegurando su alineación con los objetivos institucionales, el PETI 2025–2027 y la gestión de riesgos corporativa.
- Fortalecer la cultura organizacional en seguridad y privacidad, promoviendo la apropiación de buenas prácticas, roles, responsabilidades y comportamientos seguros por parte de todos los servidores y contratistas de la entidad.

4. Alcance del SGSI

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información Resolución 2025000825 Articulo 4 alcance.

5. Marco normativo y de referencia

El Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) se fundamenta en el marco normativo, técnico y metodológico definido por el Gobierno Nacional, así como en los documentos institucionales que orientan la gestión de la seguridad, el riesgo, la planeación estratégica y la operación de Indeportes Antioquia. Los principales documentos de referencia son:

Normatividad y lineamientos nacionales:

6. **Decreto 612 de 2018** – Directrices para la integración de los planes institucionales y estratégicos al Plan de Acción, incluyendo el Plan Estratégico de Seguridad y Privacidad de la Información (PESPI).
7. **Resolución 500 de 2021 del MINTIC** – Lineamientos y estándares para la estrategia de seguridad digital y adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).
8. **Manual de Gobierno Digital – MINTIC** – Lineamientos del habilitador de Seguridad y Privacidad de la Información.
9. **Modelo de Seguridad y Privacidad de la Información – MINTIC (MSPI)** – Estructura, roles, controles y fases de implementación del SGSPI.
10. **Guía de Gestión de Riesgos de Seguridad de la Información – MINTIC** – Metodología para la valoración, tratamiento y seguimiento del riesgo.
11. **Guía de Gestión de Incidentes de Seguridad de la Información – MINTIC.**
12. **Ley 1581 de 2012 y Decreto 1377 de 2013** – Protección de Datos Personales.
13. **Ley 1273 de 2009** – Delitos informáticos y protección de la información y de los datos.
14. **Ley 1712 de 2014** – Ley de Transparencia y del Derecho de Acceso a la Información Pública.
15. **Ley 2015 de 2019** – Gestión documental en el sector público (para articulación con datos e información).
16. **ISO/IEC 27001 e ISO/IEC 27002** – Buenas prácticas en Gestión de Seguridad de la Información.

6. Estado actual de la entidad respecto al sistema de gestión de seguridad de la información.

De acuerdo con el ultimo resultado de la evaluación del FURAG, la Seguridad y Privacidad de la información ha experimentado un aumento de 6.0 puntos, lo que sugiere avances en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y en la adopción de medidas para proteger la información sensible de la entidad. Es fundamental que el Instituto continúe fortaleciendo estas áreas y aborde las oportunidades de mejora identificadas para avanzar en su transformación digital y en la generación de valor público para los ciudadanos de Antioquia.

Igualmente luego de realizar el Autodiagnostico de Seguridad del MINTC se han obtenido los siguientes resultados, que permiten identificar las debilidades y necesidades con que continua la entidad en seguridad de la información.

No.	Evaluación de Efectividad de controles

	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	64	100	**GESTIONADO**
A.6	CONTROLES DE PERSONAS	78	100	**GESTIONADO**
A.7	CONTROLES FÍSICOS	97	100	**OPTIMIZADO**
A.8	CONTROLES TECNOLÓGICOS	57	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**74**	**100**	**GESTIONADO**

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	**Planificación**	Contexto de la organización	11%	14%
		Liderazgo	13%	14%
		Planificación	13%	14%
		Soporte	11%	14%
	Implementación	Operación	13%	16%
	Evaluación de Desempeño	Evaluación del desempeño	7%	14%
	Mejora Continua	Mejora	8%	14%
TOTAL			**77%**	**100%**

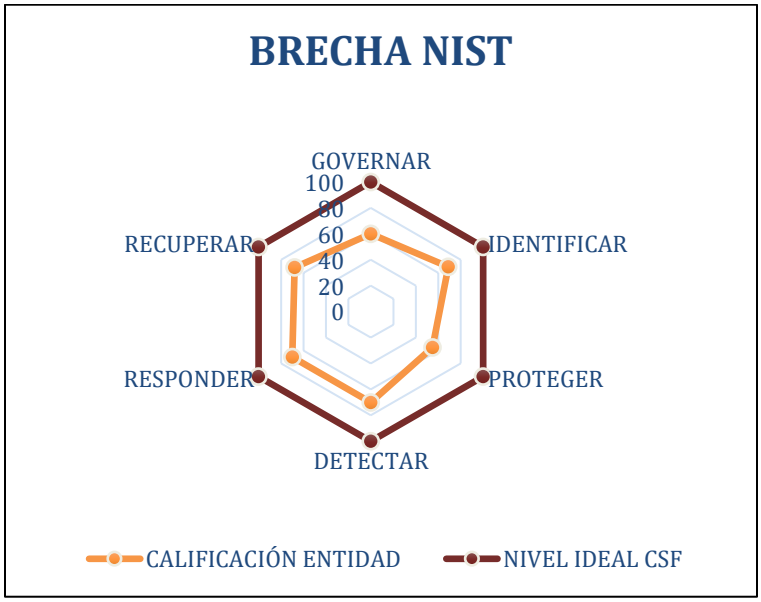
Indeportes presenta un avance global del 77%, lo cual evidencia que el SGSI está implementado de manera parcial.

Los componentes de Planificación, Liderazgo y Operación muestran avances similares y relativamente estables.

Las brechas más significativas se encuentran en:

- Evaluación del desempeño (7%)
- Mejora continua (8%)
- Esto indica que aún se requiere consolidar procesos de monitoreo, auditoría, revisión, medición y retroalimentación del SGSI para alcanzar la madurez esperada (100%).

Calificación frente a mejores prácticas en ciberseguridad (nist):



MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
GOBVERNAR	76	100
IDENTIFICAR	69	100
PROTEGER	55	100
DETECTAR	70	100
RESPONDER	70	100
RECUPERAR	69	100

Interpretación del autodiagnóstico

La entidad presenta un nivel aceptable en las funciones Gobernar, Detectar, Responder y Recuperar, ubicándose entre 69% y 76%.

La brecha más crítica se encuentra en la función Proteger (55%), relacionada con:

- Controles de acceso
- Protección de datos
- Gestión de vulnerabilidades
- Endurecimiento de sistemas
- Implementación de tecnologías de protección
- Estas áreas requieren fortalecimiento prioritario para consolidar una postura de seguridad más robusta.

El autodiagnóstico evidencia que Indeportes Antioquia se encuentra en un nivel de madurez intermedio, con avances significativos en controles físicos y en funciones de ciberseguridad relacionadas con detección y respuesta, pero con brechas relevantes en:

- Controles tecnológicos
- Políticas y gobernanza del SGSI
- Evaluación del desempeño y mejora continua
- Función “Proteger” del NIST-CSF

Estos resultados establecen la línea base precisa desde la cual se definirá la ruta estratégica del PESI y las metas de madurez que debe alcanzar la entidad en el periodo 2025–2027.

17. Gobernanza, roles y responsabilidades

Se establece el siguiente esquema:

- **Alta Dirección:** Aprobar política, revisar el desempeño del SGSI (9.3), proveer recursos (5.1) y asumir la rendición de cuentas.

- **Comité**: El Comité de Gestión y Desempeño ejercerá la función de máximo órgano de dirección en materia de seguridad de la información, apoyado por el Subcomité de Protección de Datos Personales, el cual cuenta con un Equipo de Cumplimiento dependiente de la Oficina de Sistemas e Informática. Dicho equipo es responsable de liderar y coordinar, junto con contratistas especializados, el cumplimiento del Sistema de Gestión en Seguridad de la Información – SGSI y el Sistema de Gestión en Protección de Datos Personales – SGPDP.

- **Oficina de Sistemas e Informática:** La Oficina de Sistemas e Informática asumirá el liderazgo operativo de la seguridad de la información, la seguridad digital y la gestión de incidentes, articulando las actividades del Equipo Técnico TIC y del Equipo de Cumplimiento. En desarrollo de este rol, coordinará el cumplimiento de las políticas, lineamientos y estándares internacionales (ISO/IEC 27001:2022) en toda la entidad.

- **Oficial de Seguridad de la Información**: El Oficial de Seguridad de la Información dependerá funcionalmente de la Oficina de Sistemas e Informática. Tendrá como responsabilidad principal coordinar, implementar y supervisar el Sistema de Gestión de Seguridad de la Información – SGSI, asegurando su alineación con la normativa vigente y con el Sitema de Gestión de Protección de Datos Personales – SGPDP. Sus funciones serán, entre otras:

    - Elaborar y mantener actualizado el mapa de riesgos de seguridad de la información de la entidad.
    - Coordinar la implementación de controles técnicos, organizativos y administrativos para proteger los activos de información.
    - Gestionar, junto con el Equipo de Cumplimiento, los procesos de evaluación y auditoría del SGSI.
    - Liderar la respuesta institucional ante incidentes de seguridad de la información, garantizando su adecuada documentación y cierre.
    - Servir de enlace entre la Gerencia, el Subcomité de Protección de Datos Personales y las diferentes dependencias en materia de seguridad digital y ciberseguridad.
    - Velar por la adopción de la norma ISO/IEC 27001:2022 en todos los procesos y sistemas de información de la entidad
    - Define y aplica la política de servicios cloud (A.5.23).

- **Oficial de Protección de Datos:** Las funciones del oficial de protección de datos son claves para que la entidad cumpla en sistema de protección de datos personales, por tal motivo, el comité de protección de datos delega la supervisión, asesoría y coordinación en el oficial para que desarrolle, sin limitarse a ellas, las siguientes funciones:
    - Supervisar la observancia del Régimen General de Protección de Datos Personales.
    - Analizar y comprobar la conformidad de las actividades de tratamiento con la normativa, a partir de la información recabada en la entidad.
    - Asesorar y emitir recomendaciones sobre políticas, prácticas, medidas adoptadas e interpretación normativa.
    - Revisar y promover la actualización de manuales, cláusulas contractuales, autorizaciones y lineamientos relacionados con protección de datos.
    - Las demás consignadas en la resolución No. S2025000814 del 03 de septiembre de 2025.

- **Responsables de Proceso:** Incorporan requisitos del SGSI en las caracterizaciones, operan controles y gestionan riesgos del proceso.

- **Gestión de Contratación:** Aplica requisitos de seguridad en la cadena de suministro (A.5.19–A.5.22).

- **ColCERT/CSIRT interno o proveedor:** Soporte en inteligencia de amenazas, respuesta a incidentes y gestión de vulnerabilidades.

18. Política de Seguridad de la Información

La política se deberá actualiza para incluir: cumplimiento de requisitos de partes interesadas, mejora continua, compromiso con la protección de datos personales y alineación con el MSPI. Será publicada, comunicada y revisada anualmente.

19. Plan de cierre de brechas y acciones ISO 27001

Las siguientes acciones responden a las no conformidades de la preauditoría y a los controles del Anexo A de ISO/IEC 27001:2022:

- 4.3.c — Límites tecnológicos del alcance: Definir y documentar el perímetro tecnológico del SGSI (redes, sistemas, aplicativos, integraciones, ambientes on-premise y nube), con diagrama de arquitectura y matriz de interacciones.
- 4.4 — Caracterizaciones de proceso: Actualizar las caracterizaciones para incluir objetivos, riesgos y controles de seguridad aplicables; vincular procedimientos TI y requisitos del MSPI.
- 5.2 — Política incompleta: Reformar la política incorporando requisitos de partes interesadas, mejora continua y responsabilidades.
- 6.1/8.1–8.3 — Gestión de riesgos: Completar la metodología: identificación, análisis, evaluación, decisiones (mitigar/aceptar/transferir), riesgos inherentes y residuales, planes de tratamiento, aceptación formal; mapear contra Anexo A.
- 6.1.3.d — Declaración de aplicabilidad: Codificar la DoA, justificar exclusiones (incl. 8.14 si aplica), evidenciar implementación/planificación de cada control.
- 5.1.e/6.2/9.1 — Métricas y objetivos: Definir KPIs (ver sección 9) y planes para alcanzarlos; establecer metas trimestrales.
- 7.5.3.a — Recuperación de información: Definir esquema de gestión documental y repositorios; tiempos de recuperación; responsables y capacitaciones.
- 9.2 — Auditorías internas: Plan anual de auditoría, ciclo completo y gestión de acciones correctivas.

- 9.3 — Revisión por la dirección: Agenda semestral con entradas/salidas exigidas por la norma.
- A.5.7 — Inteligencia de amenazas: Suscribir fuentes (ColCERT/CVE/ISAC), establecer proceso de ingestión y comunicaciones mensuales.
- A.5.8 — Seguridad en proyectos: Incluir seguridad por diseño: criterios, riesgos y validaciones en el ciclo de vida de proyectos.
- A.5.9 — Gestión de activos: Inventario y clasificación de activos (dueños, criticidad, ubicación), etiquetas y registros.
- A.5.13 — Etiquetado de información: Implementar esquema de clasificación y etiquetado (Pública/Interna/Confidencial/Reservada).
- A.5.14 — Transferencia de información: Definir y firmar acuerdos de intercambio seguro con cifrado y trazabilidad.
- A.5.19–A.5.22/8.30 — Proveedores y cadena de suministro: Gestionar riesgos de terceros, requisitos en contratos, control de cambios y monitoreo continuo.
- A.5.23 — Servicios de nube: Aprobar política de uso de nube (modelos, responsabilidades compartidas, residencia de datos, cifrado, evaluación de riesgos).
- A.5.29–A.5.30 — Continuidad TIC: Realizar BIA, definir RTO/RPO, estrategias de recuperación, simulacros anuales y evidencias.
- A.5.24–A.5.28/A.5.29 — Gestión de incidentes: Establecer proceso E2E: detección, clasificación, respuesta, evidencias, continuidad y lecciones aprendidas.
- A.5.32 — Propiedad intelectual: Eliminar software no autorizado, licenciamiento y control de instalaciones.
- A.5.34 — Protección de datos personales: Revisión del programa de privacidad; PIAs y registros de tratamiento.
- A.5.35 — Revisión independiente: Programar revisión externa independiente del SGSI.
- A.5.37 — Procedimientos aprobados: Aprobar e implementar procedimientos de TI y seguridad operativa.
- A.6.3/6.3 — Formación y contraseñas: Programa de formación; política de contraseñas seguras, gestores de contraseñas y prohibición de compartir por mensajería.
- 5.3/7.2/A.5.3 — Roles y segregación: Definir roles/autoridades, separación de funciones críticas y designación del Oficial de Seguridad.
- A.6.7 — Trabajo remoto: Verificación de condiciones de seguridad para teletrabajo.
- A.7.1 — Diseño de seguridad física: Definir zonas seguras y controles de acceso físicos.
- A.7.5 — Protección ante amenazas externas: Diseñar medidas contra incendio, terremoto, inundación y documentar pruebas.
- A.7.7 — Escritorio limpio: Aplicar política de escritorio/almacenamiento limpio y cumplimiento.

- A.7.9 — Protección de equipos fuera de sitio: Controles para dispositivos en campo: cifrado, inventario, custodia.
- A.7.13 — Mantenimiento: Programa de mantenimiento de servidores y equipos.
- A.7.14 — Disposición segura: Procedimientos de borrado seguro y destrucción certificada.
- A.8.1 — Protección de endpoint y medios: Controles EDR, cifrado de discos y políticas de uso de medios extraíbles.
- A.8.6 — Gestión de capacidad: Monitoreo y proyección de capacidad.
- 8.12 — Prevención de fuga de datos: Implementar DLP en correo, endpoints y repositorios.
- 8.13 — Pruebas de restauración: Calendarizar y evidenciar pruebas de backup/restore.
- 8.17 — Sincronización horaria: NTP corporativo y verificación periódica (incluye CCTV).
- 8.32 — Control de cambios: Metodología formal de cambios en TI y desarrollo.
- 8.25–8.33 — Desarrollo seguro: Definir ciclo de vida seguro, requisitos, arquitectura, ambientes y pruebas de seguridad.

20. Estrategia de seguridad digital

La Entidad establecerá una Estrategia de Seguridad Digital que articule los principios, políticas, procedimientos, lineamientos y controles necesarios para garantizar la adecuada protección de la información y el cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI. Esta estrategia incorpora los habilitadores definidos en la Política de Gobierno Digital y se estructura a partir de seis componentes esenciales, tal como se presenta en el documento institucional.

Cada uno de estos componentes constituye una línea estratégica que, en su conjunto, permiten establecer un marco integral de protección, prevención, control y respuesta frente a los riesgos de seguridad digital que enfrenta la Entidad.

A continuación, se describen las seis estrategias específicas, conforme al esquema definido en el documento:

a. **Cumplimiento de los Lineamientos de Seguridad de la Información:** Asegurar que la Entidad adopte, actualice e implemente los lineamientos, políticas, estándares y controles definidos para la seguridad de la información, en concordancia con los requisitos del MSPI y la normativa vigente. Esta estrategia garantiza la alineación institucional con los marcos regulatorios, incluyendo la Resolución 500 de 2021 y sus anexos.

b. **Gestión de Activos de Información:** Fortalecer el proceso de identificación, clasificación, inventario, valoración y protección de los activos de información. Esta estrategia permite mantener un control claro sobre la información crítica, su ciclo de vida y su nivel de exposición al riesgo, asegurando que los activos cuenten con responsables, características documentadas y medidas de protección adecuadas.

c. **Gestión de Riesgos de Seguridad de la Información:** Implementar de manera continua y sistemática la identificación, análisis, evaluación y tratamiento de riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información. Esta estrategia se articula con el Modelo de Gestión del Riesgo de la Entidad y con la guía de riesgos de seguridad de la información del MSPI, permitiendo tomar decisiones basadas en riesgo y priorizar controles.

d. **Cultura en Seguridad de la Información:** Desarrollar acciones de formación, sensibilización y apropiación dirigidas a servidores públicos, contratistas y actores que interactúan con la información institucional. Esta estrategia busca fortalecer el comportamiento seguro, minimizar errores humanos, promover el cumplimiento de políticas y fomentar una cultura preventiva frente a las amenazas digitales.

e. **Análisis de Vulnerabilidades:** Realizar ejercicios periódicos de identificación, testeo y revalidación de vulnerabilidades técnicas presentes en los sistemas, infraestructura tecnológica, aplicaciones, servicios y plataformas de la Entidad. Esta estrategia permite anticipar riesgos, corregir debilidades y verificar la efectividad de los controles tecnológicos implementados.

f. **Gestión de Incidentes:** Definir, implementar y operar el procedimiento para la atención, análisis, tratamiento y cierre de incidentes de seguridad de la información. Esta estrategia garantiza una respuesta oportuna ante eventos que comprometan la operación o los activos de información, incluyendo protocolos de reporte, escalamiento, mitigación de impacto y registro estructurado de incidentes.

Conclusión

Estas seis estrategias conforman la Estrategia General de Seguridad Digital de la Entidad, y proporcionan la ruta estructural para fortalecer la protección de la información, cumplir con el MSPI y asegurar la gestión integral de los riesgos, incidentes y vulnerabilidades que puedan afectar los procesos institucionales.

21. Descripción de las Estrategias Específicas (Ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
1. Cumplimiento de los Lineamientos de Seguridad de la Información	Asegurar la adopción, actualización e implementación de la política general, lineamientos, directrices y estándares de seguridad y privacidad de la información establecidos para la Entidad, conforme al MSPI y la Resolución 500 de 2021. Busca garantizar el liderazgo institucional, el compromiso de la alta dirección y la definición clara de roles y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de la información.

2. Gestión de Activos de Información	Identificar, clasificar, registrar, custodiar y proteger los activos de información a lo largo de su ciclo de vida, garantizando que cuenten con responsables asignados y controles adecuados de acuerdo con su criticidad. Permite mantener un inventario actualizado y aplicar medidas coherentes con el nivel de riesgo asociado a cada activo.
3. Gestión de Riesgos de Seguridad de la Información	Identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional. Esta estrategia orienta la toma de decisiones basada en riesgo, previene impactos no deseados y promueve la implementación de controles de seguridad acordes con las amenazas identificadas.
4. Cultura en Seguridad de la Información	Fortalecer la cultura institucional mediante procesos de sensibilización, formación y apropiación de buenas prácticas en seguridad y privacidad de la información. Busca que el personal incorpore la seguridad como hábito, conozca sus responsabilidades y aplique las políticas y procedimientos establecidos.
5. Análisis de Vulnerabilidades	Realizar evaluaciones periódicas (test y re-test) de vulnerabilidades técnicas en sistemas, infraestructura, plataformas y servicios tecnológicos de la Entidad. Permite identificar debilidades, priorizar acciones de mitigación, corregir fallas y mejorar continuamente la postura de ciberseguridad.
6. Gestión de Incidentes de Seguridad de la Información	Asegurar la detección, reporte, análisis, contención, tratamiento y cierre de incidentes de seguridad de la información mediante un procedimiento formal. Esta estrategia minimiza el impacto negativo de incidentes, garantiza la comunicación adecuada y retroalimenta el SGSI con lecciones aprendidas.

22. Programa de implementación (12 meses)

Se espera realizar la implementación de los siguientes puntos durante el 2026 de la siguiente forma:

- **Trimestre 1:** Gobernanza, política, alcance y límites tecnológicos; inventario y clasificación de activos; metodología de riesgos; definición de roles; política de nube; NTP.

- **Trimestre 2:** DoA codificada; planes de tratamiento; procedimientos de incidentes; escritorio limpio; cadena de suministro y contratos; DLP; backups y pruebas de restauración.
- **Trimestre 3**: Continuidad TIC (BIA, RTO/RPO, simulacros); seguridad en proyectos; mantenimiento; disposición segura; desarrollo seguro; auditoría interna.
- **Trimestre 4**: Revisión por la dirección; revisión independiente; mejora continua; reporte de indicadores y lecciones aprendidas.

23. Gestión de riesgos

Para la Gestión de riesgos se aplicará una metodología basada en ISO/IEC 27005, con matriz de riesgos que incluya riesgo inherente, residual, criterios de aceptación, tratamiento (controles del Anexo A) y registro de decisiones, que dé cumplimiento a los establecido en el modelo de gestión de riesgos de seguridad digital (MGRSD).

24. Indicadores clave (KPIs) y seguimiento

- Porcentaje de controles del Anexo A implementados vs. planificados.
- Cobertura de inventario y clasificación de activos (% activos con dueño y nivel de clasificación).
- Tiempo medio de detección (MTTD) y de respuesta (MTTR) a incidentes.
- Cumplimiento de pruebas de backup/restore (número y tasa de éxito trimestral).
- Cumplimiento de simulacros de continuidad (anuales) y alcanzar RTO/RPO definidos.
- Porcentaje de proveedores con cláusulas de seguridad y evaluación de riesgos.
- Porcentaje de usuarios formados y cumplimiento de política de contraseñas.
- Porcentaje de proyectos con evaluación de seguridad (checklist de seguridad por diseño).

Los indicadores se miden semestralmente y se reportan al Comité de Gestión y Desempeño en la revisión semestral (9.3).

25. Recursos y presupuesto estimado

- **Recursos humanos:** Oficial de Seguridad, Oficial de Protección de Datos, analista de riesgos, administrador de seguridad, soporte de proveedores (DLP/EDR/backup).

- **Recursos tecnológicos**: herramientas EDR, DLP, SIEM/registro de eventos, cifrado, gestión documental, plataforma de respaldos. Presupuesto detallado a definir con Planeación.

AÑO 2026

Necesidad	Inversión
Oficial de Seguridad	$91.905.043
Implementación de solución WAF y renovación de EDL	$85.000.000
Análisis de Vulnerabilidades y Servicio Ethical Hacking	$140.000.000
TOTAL PRESUPUESTO AÑO 2026	**$316. 905.043**

26. Comunicación y formación

Se deberá realizar un programa trimestral de sensibilización en seguridad, privacidad y trabajo remoto seguro; campañas de phishing simulado; guía de contraseñas y uso de gestores; manuales operativos.

27. Cumplimiento del MSPI (Resolución 02277 de 2025)

- Alineación explícita con ISO/IEC 27001:2022 para sujetos obligados de la Política de Gobierno Digital.
- Actualización de política, roles y esquemas de gobernanza de seguridad y privacidad.
- Gestión de riesgos integral y adopción de controles del Anexo A.
- Gestión de incidentes, continuidad del negocio y protección de datos personales.
- Seguridad en la cadena de suministro y servicios de nube conforme a responsabilidades compartidas.

28. Aprobación y vigencia

Una vez aprobado por la Alta Dirección, este plan entra en vigencia inmediata y su cumplimiento será auditado internamente cada año. Las actualizaciones se efectuarán conforme a cambios normativos del MSPI y la política de gobierno digital.

29. Plan de trabajo con fechas y responsables

Actividades, plazos, dependencias y entregables por trimestre (enero–diciembre 2026).

Actividad/Hito	Descripción	Inicio	Fin	Dependencias	Entregable
Definir alcance y límites tecnológicos del SGSI	Perímetro, diagramas de arquitectura e interacciones (on-prem/nube).	2026-02-26	2026-02-05	Oficina de sistemas	Documento de alcance y diagrama de arquitectura
Inventario y clasificación de activos	Identificación, dueños, criticidad y etiquetado.	2026-01-26	2026-02-27	Oficina de sistemas	Inventario y matriz de clasificación
Actualización de la Política de Seguridad	Incluir requisitos de partes interesadas y mejora continua.	2026-01-26	2026-02-16	Oficina de sistemas	Política aprobada y publicada
Metodología y matriz de riesgos	Identificación/análisis/evaluación; riesgo inherente/residual.	2026-02-01	2026-03-13	Oficina de sistemas Oficina Asesora de Planeación	Metodología y matriz de riesgos
Declaración de aplicabilidad (DoA) codificada	Codificación y justificación de exclusiones; mapeo de controles.	2026-03-01	2026-03-25	Oficina de sistemas	DoA aprobada Matriz de riesgos
Gestión de incidentes de seguridad	Detección, clasificación, respuesta, evidencias y lecciones.	2026-04-01	2026-04-20	Oficina de sistemas	Procedimiento publicado DoA codificada
Escritorio/almacenamiento limpio	Controles de orden y protección; campaña de sensibilización.	2026-04-05	2026-04-15	Oficina de sistemas y Oficina Asesora de comunicaciones	Política seguridad socializada publicada y campaña
Cadena de suministro y contratos	Cláusulas de seguridad, evaluaciones y control de cambios.	2026-04-10	2026-05-10	Oficina de sistemas y Oficina Asesora jurídica	Anexos contractuales y matriz de evaluación DoA codificada
Implementación de DLP	Prevención de fuga de datos (correo, endpoints, repositorios).	2026-05-01	2026-06-15	Oficina de sistemas	DLP configurado y reporte de cobertura Políticas y procedimientos

Backups y pruebas de restauración	Calendarización y evidencias de restauración.	2026-05-15	2026-06-30	Oficina de sistemas	Inventario de sistemas Actas de pruebas exitosas
BIA y definición RTO/RPO	Análisis de impacto y requisitos de continuidad.	2026-07-01	2026-07-31	Oficina de sistemas	Informe BIA y matriz RTO/RPO Inventario procesos críticos
Estrategias y simulacro de continuidad TIC	Planes de recuperación y ejercicio de simulacro.	2026-08-01	2026-09-15	Oficina de sistemas	Plan de continuidad y acta de simulacro BIA y RTO/RPO
Mantenimiento y disposición segura	Calendario de mantenimiento y procedimientos de borrado.	2026-07-15	2026-08-20	Oficina de sistemas	Plan mantenimiento y procedimiento disposición Políticas aprobadas
Desarrollo seguro (ciclo de vida y pruebas)	Requisitos, arquitectura, ambientes y pruebas SAST/DAST.	2026-08-10	2026-09-30	Oficina de sistemas	Guía y reportes de pruebas DoA y políticas de desarrollo
Auditoría interna del SGSI	Ejecución, informe y plan de acciones correctivas.	2026-09-10	2026-10-05	Oficina de Control Interno	Informe y plan de acciones Controles implementados
Revisión por la Dirección (1)	Entradas/salidas 9.3; decisiones y recursos.	2026-10-15	2026-10-15	Oficina de Control Interno Oficina de Asesora de Planeación Gerencia	Acta de revisión por la dirección Auditoría interna

Revisión independiente del SGSI	Evaluación externa independiente.	2026-10-20	2026-11-15	Oficina de Control Interno Oficina de Asesora de Planeación Gerencia	Informe de revisión independiente Revisión por la dirección
Mejora continua y cierre de brechas	Lecciones aprendidas y actualización del plan.	2026-11-20	2026-12-15	Todos los anteriores	Plan de mejora actualizado

30. Aprobación

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.