PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2024-2027

APROBÓ: SANDRA MILENA QUIROZ VILLA, GERENTE DE INDESA
REVISÓ Y VALIDÓ: DANIEL ESTEBAN MONTOYA, LÍDER OPERATIVO Y ADMINISTRATIVO

FECHA DE ELABORACIÓN: ENERO DE 2026

Contenido

1. PRESENTACIÓN 3
2. OBJETIVO GENERAL 3
3. OBJETIVOS ESPECÍFICOS 3
4. ALCANCE 3
5. MARCO NORMATIVO 3
6. DIAGNÓSTICO ACTUAL (SITUACIÓN REAL DE INDESA) 4
Fortalezas Identificadas 4
Debilidades Identificadas 4
7. ANÁLISIS DE RIESGOS INSTITUCIONALES 4
8. ESTRATEGIAS Y LÍNEAS DE ACCIÓN 5
SEGURIDAD TÉCNICA 5
SEGURIDAD HUMANA 5
SEGURIDAD ADMINISTRATIVA 5
9. RESPONSABLES 5
10. SEGUIMIENTO Y EVALUACIÓN 5
11. MATRIZ DE RIESGOS 5
12. PLAN DE ACCIÓN 6
13. INDICADORES DE SEGUIMIENTO (MIPG / GOBIERNO DIGITAL) 7
14. INCORPORACIÓN AL PETI 8
CRONOGRAMA DE TRABAJO 8

1. PRESENTACIÓN

La gestión adecuada de la información es uno de los pilares fundamentales para el funcionamiento eficiente, transparente y seguro de las entidades públicas. En este contexto, el Instituto para el Deporte y la Recreación de Sabaneta – INDESA, consciente de su responsabilidad frente al tratamiento, custodia y administración de los datos institucionales y personales, formula el presente Plan Estratégico de Seguridad y Privacidad de la Información (PESPI).

Este plan establece las directrices, estrategias y líneas de acción que permiten fortalecer la protección de la información institucional, garantizando principios fundamentales como la confidencialidad, integridad, disponibilidad y legalidad en el tratamiento de los datos.

El PESPI se articula de manera directa con el Plan Estratégico de Tecnologías de la Información (PETI), la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan de Desarrollo Municipal de Sabaneta.

2. OBJETIVO GENERAL

Establecer las estrategias institucionales para proteger la información de INDESA, garantizando su confidencialidad, integridad, disponibilidad y privacidad, conforme a la normativa legal vigente y las buenas prácticas en seguridad de la información.

3. OBJETIVOS ESPECÍFICOS

- Fortalecer la cultura de seguridad digital entre funcionarios y contratistas.
- Minimizar los riesgos asociados al manejo inadecuado de la información.
- Establecer lineamientos para el uso seguro de los sistemas de información.
- Asegurar el cumplimiento normativo en protección de datos personales.
- Implementar controles técnicos, administrativos y humanos en seguridad de la información.
- Articular el PESPI con el PETI institucional.

4. ALCANCE

El presente plan aplica a todos los funcionarios, contratistas, practicantes y proveedores tecnológicos de INDESA, así como a todos los sistemas de información, bases de datos, documentos físicos y digitales, equipos de cómputo, servidores, redes y plataformas digitales institucionales.

5. MARCO NORMATIVO

El PESPI se rige bajo el siguiente marco legal y técnico colombiano:

• **Ley 1581 de 2012:** Disposiciones generales para la protección de datos personales.

• **Decreto 1074 de 2015:** Decreto Único Reglamentario del Sector Comercio (Compila el Decreto 1377 de 2013).

• **Ley 2345 de 2023 ("Ley Chao Marcas"):** Por la cual se promueve la identidad visual de las entidades estatales y se prohíben marcas de gobierno en activos digitales.

• **Resolución 500 de 2021 (MinTIC):** Por la cual se establecen los lineamientos para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).

• **CONPES 3854 de 2016:** Política Nacional de Seguridad Digital.

6. DIAGNÓSTICO ACTUAL (SITUACIÓN REAL DE INDESA)

Con base en la información suministrada:

Fortalezas Identificadas

- Existe una Coordinación de Comunicaciones y TIC que toma decisiones sobre tecnología y seguridad digital.
- INDESA cuenta con servidor institucional.
- Existen correos corporativos institucionales pagos.
- Se cuenta con protocolos de copias de seguridad; sin embargo, se identifica la necesidad prioritaria de aumentar la frecuencia y automatización de los backups (tránsito hacia esquema diario en nube/servidor) para garantizar la continuidad del negocio y minimizar la pérdida de datos (RPO) ante posibles incidentes.
- INDESA cuenta con política de protección de datos personales desde 2018.
- Existe conciencia administrativa sobre la importancia de la información.

Debilidades Identificadas

- Uso simultáneo de correos Gmail no corporativos para información institucional.
- Uso de Google Drive sin control técnico institucional formal.
- Antivirus instalado pero sin licencia ni actualización oficial.
- Brecha entre la existencia de correos corporativos y su uso real.
- No existe una política formal de control de accesos.
- Falta de protocolos de gestión de incidentes digitales.
- Ausencia de clasificación de la información por niveles de confidencialidad.

7. ANÁLISIS DE RIESGOS INSTITUCIONALES

Riesgo	Impacto
Acceso indebido a información	Alto
Pérdida de archivos institucionales	Alto
Uso de cuentas personales	Alto
Virus y malware	Alto
Fuga de datos personales	Alto
Fallas en backups	Medio
Manipulación indebida de información	Medio

8. ESTRATEGIAS Y LÍNEAS DE ACCIÓN

SEGURIDAD TÉCNICA

- Adquisición de antivirus institucional.
- Respaldos periódicos automatizados.
- Control de accesos a carpetas y sistemas.
- Protección del servidor institucional.
- Uso obligatorio de correos corporativos.

SEGURIDAD HUMANA

- Capacitaciones en ciberseguridad.
- Firmas de acuerdos de confidencialidad.
- Socialización de la política de datos personales.
- Sensibilización sobre phishing o correos falsos.

SEGURIDAD ADMINISTRATIVA

- Protocolos escritos de acceso.
- Política de contraseñas.
- Manual interno de seguridad digital.
- Procedimiento de manejo de incidentes.

9. RESPONSABLES

- Gerencia de INDESA.
- Coordinación de Comunicaciones y TIC.
- Talento Humano.
- Área Jurídica.
- Supervisores de contrato.

10. SEGUIMIENTO Y EVALUACIÓN

Indicadores propuestos:

- % funcionarios capacitados.
- Número de incidentes reportados.
- Cumplimiento de backups.
- Uso de correos institucionales.
- Actualización de antivirus.

11. MATRIZ DE RIESGOS

Nº	Riesgo	Causa	Impacto	Probabilidad	Nivel	Medida de Control
1	Pérdida de información	No respaldo automático	Alto	Media	ALTO	Backups periódicos y controlados
2	Fuga de datos personales	Uso de correos personales	Alto	Alta	CRÍTICO	Uso obligatorio de correo corporativo
3	Infección por virus	Antivirus desactualizado	Alto	Alta	CRÍTICO	Licencia antivirus corporativo

4	Acceso indebido	Falta de control de usuarios	Alto	Media	ALTO	Roles de acceso por carpeta
5	Mal uso de dispositivos	Falta de políticas claras	Media	Media	MEDIO	Manual de uso de equipos
6	Pérdida de archivos Drive	Cuentas personales	Alto	Alta	CRÍTICO	Migración a almacenamiento institucional
7	Ataques de phishing	Falta de cultura digital	Alto	Media	ALTO	Capacitaciones
8	Manipulación de datos	Sin perfiles de permisos	Medio	Media	MEDIO	Control de edición
9	Copias de seguridad incompletas	Proceso manual	Medio	Media	MEDIO	Automatización
10	Uso indebido de contraseñas	Sin política definida	Medio	Alta	ALTO	Política de contraseñas

12. PLAN DE ACCIÓN

Línea Estratégica	Actividad	Responsable	Fecha	Indicador
Seguridad Técnica	Compra e implementación de antivirus corporativo	Líder Operativo / Apoyo TIC	2024-2027	100% equipos protegidos
Continuidad y recuperación	Diseño, socialización y prueba del Plan de Recuperación antes Desastres (DRP).	Líder Operativo / Apoyo TIC	Segundo semestre 2026	Plan activo
Seguridad Técnica	Backup automatizado	Líder Operativo / Apoyo TIC	2024-2027	Plan activo
Seguridad Técnica	Asegurar servidor institucional	Líder Operativo / Apoyo TIC	2024-2027	Servidor protegido

Seguridad Técnica	Migración a nube institucional	Líder Operativo / Apoyo TIC	2024-2027	Drive institucional activo
Seguridad Técnica	Control de accesos	Líder Operativo / Apoyo TIC	2024-2027	Carpetas con permisos
Seguridad Humana	Inducciones	Talento Humano	Semestral	% personas capacitadas
Seguridad Humana	Firmar compromisos	Jurídica	2024-2027	% contratos con cláusula
Seguridad Humana	Guía de buenas prácticas	Líder Operativo / Apoyo TIC	2024-2027	Manual entregado
Seguridad Administrativa	Política de contraseñas	Líder Operativo / Apoyo TIC	2024-2027	Política publicada
Seguridad Administrativa	Protocolo de incidentes	Líder Operativo / Apoyo TIC	2024-2027	Documento aprobado
Seguridad Administrativa	Socializar política de datos	Jurídica	Anual	Evidencia
Seguimiento	Auditoría interna	Dirección	Anual	Informe emitido
Seguimiento	Informe trimestral	Líder Operativo / Apoyo TIC	Trimestral	Actas

13. INDICADORES DE SEGUIMIENTO (MIPG / GOBIERNO DIGITAL)

Indicador	Fórmula
Funcionarios capacitados	Capacitaciones realizadas / total personal
Incidentes reportados	Conteo trimestral
Uso de correos corporativos	Cuentas activas / total personal
Backups realizados	Actividades ejecutadas
Antivirus actualizados	Equipos actualizados

Cumplimiento normativo	Ítems cumplidos / total

14. INCORPORACIÓN AL PETI

Este PESPI se articula con:

- Infraestructura Tecnológica.
- Gobierno Digital.
- Continuidad Tecnológica.
- Riesgos TIC.
- Protección de Datos.

CRONOGRAMA DE TRABAJO

Fase	Actividad	Periodo	Responsable	Producto / Resultado
Planeación	Socialización del PESPI	ene-26	TIC	Acta de socialización
Planeación	Actualización de matriz de riesgos de información	Enero – Febrero 2026	TIC / Control Interno	Matriz actualizada
Seguridad Técnica	Implementación de antivirus corporativo	Febrero – Marzo 2026	TIC	Equipos protegidos
Seguridad Técnica	Implementación de backups automatizados	Marzo – Abril 2026	TIC	Backups operativos
Seguridad Técnica	Control de accesos a información crítica	Abril – Mayo 2026	TIC	Roles definidos
Seguridad Administrativa	Implementación de política de contraseñas	may-26	TIC	Política vigente
Seguridad Administrativa	Protocolo de gestión de incidentes	Mayo – Junio 2026	TIC	Protocolo aprobado
Seguridad Humana	Capacitaciones en seguridad digital	Junio y Octubre 2026	TIC / Talento Humano	Funcionarios capacitados
Seguridad Humana	Firmas de compromisos de confidencialidad	Permanente	Jurídica / Talento Humano	Compromisos firmados
Seguimiento	Monitoreo de cumplimiento de controles	Trimestral	TIC	Informes trimestrales
Evaluación	Auditoría interna de seguridad de la información	oct-26	Control Interno	Informe de auditoría
Mejora	Ajustes al PESPI	Noviembre – Diciembre 2026	TIC	Plan actualizado