PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – VIGENCIA 2026

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. INTRODUCCIÓN

La estrategia de Gobierno Digital en Colombia se enmarca en la construcción de un Estado más eficiente, transparente y participativo, que, con el apoyo de las tecnologías de la información y las comunicaciones, refleja un desarrollo sobre la base de los siguientes cuatro ejes temáticos: TIC para el estado, TIC para la sociedad y habilitadores transversales. Atendiendo lo expuesto, el Ministerio de las Tecnologías de la Información y las Comunicaciones, ha definido el Modelo de Seguridad y Privacidad de la Información, denominado MSPI, como un componente transversal basado en la adopción de mejores prácticas y metodologías como: la norma ISO/IEC 27001:2013, entre otras.

Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TI.

2. MARCO NORMATIVO Y ARTICULACIÓN ESTRATÉGICA

El presente Plan se articula con el Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) y el Plan Estratégico de TI (PETI) de INDESA. Su formulación obedece a lo establecido en:

- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC.
- **Ley 1581 de 2012:** Protección de Datos Personales.
- **Resolución 500 de 2021 (MinTIC):** Lineamientos para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Política de Administración del Riesgo de INDESA.**

3. OBJETIVOS

El objetivo principal de estas políticas es asegurar la confidencialidad, integridad y disponibilidad de la información del Instituto para el Deporte y la Recreación de Sabaneta INDESA, protegiendo sus activos digitales, recursos y operaciones, cumpliendo con las normativas vigentes y garantizando la continuidad de los servicios. Los objetivos específicos incluyen:

- Proteger la información sensible y confidencial del Instituto contra accesos no autorizados.
- Garantizar la integridad y exactitud de la información y los sistemas de información.
- Asegurar que los sistemas de información estén disponibles para el personal autorizado y los ciudadanos cuando sea necesario.
- Cumplir con todas las normativas y leyes aplicables relacionadas con la protección de la información.
- Fomentar una cultura de seguridad de la información entre el personal y los colaboradores.
- Establecer medidas de prevención, detección y respuesta a incidentes de seguridad

4. ALCANCE

Estas políticas se aplican a todos los empleados, contratistas, proveedores y cualquier persona o entidad que maneje información del Instituto para el Deporte y la Recreación de Sabaneta INDESA. Abarca el uso de sistemas, equipos de TI, información almacenada en cualquier medio y sistemas de comunicación que procesan información relacionada con el Instituto.

5. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información manejada por el Instituto se clasifica de la siguiente manera:

Pública: Información accesible a cualquier ciudadano sin restricciones.

Confidencial: Información cuyo acceso está limitado al personal autorizado debido a su sensibilidad.

Secreta: Información de alta sensibilidad que podría afectar las operaciones o reputación del Instituto si se divulga sin autorización.

Cada tipo de información debe manejarse con los niveles de seguridad adecuados para su clasificación.

6. CONTROL DE ACCESO

- El acceso a la información estará restringido según el rol y las responsabilidades de cada colaborador.

- El personal solo tendrá acceso a la información que necesite para realizar sus funciones.
- El acceso a los sistemas de información estará protegido por contraseñas fuertes.

7. USO ACEPTABLE DE LOS SISTEMAS DE INFORMACIÓN

- Los sistemas de información del Instituto deben utilizarse únicamente para fines laborales.
- Queda prohibido el uso de los recursos de TI para actividades ilegales o no autorizadas.

- Los usuarios no deben instalar software no autorizado ni modificar la configuración de seguridad de los sistemas.

Gestión de Contraseñas

- Las contraseñas deben cumplir con requisitos mínimos de complejidad: al menos 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Las contraseñas deben cambiarse cada 90 días.
- Queda prohibido compartir contraseñas entre empleados o con terceros no autorizados.

Protección contra Amenazas

- Todos los sistemas de TI deben estar equipados con software antivirus y soluciones de detección y prevención de intrusiones.
- Se realizarán actualizaciones de seguridad y parches de software de forma periódica para proteger contra vulnerabilidades conocidas.
- Se implementarán cortafuegos para proteger la red interna de accesos no autorizados.

Gestión de Incidentes

- Se establecerá un protocolo de respuesta ante incidentes de seguridad para identificar, gestionar y resolver cualquier brecha de seguridad.
- Cualquier incidente o sospecha de incidente debe ser reportado inmediatamente al equipo de seguridad de la información.
- Se mantendrán registros detallados de todos los incidentes para su análisis y mejora continua.

8. BACKUP Y RECUPERACIÓN DE DESASTRES

- Se implementará una política de copias de seguridad periódicas para asegurar la disponibilidad de la información crítica.
- Las copias de seguridad se almacenarán en ubicaciones seguras, tanto locales como externas (almacenamiento en la nube, centros de datos).
- Se realizarán pruebas periódicas de recuperación de datos para garantizar que las copias de seguridad sean funcionales.

9. CAPACITACIÓN Y CONCIENTIZACIÓN

- Todo el personal debe recibir capacitación anual sobre seguridad de la información, riesgos cibernéticos y las políticas vigentes.
- Se fomentará una cultura de responsabilidad y concienciación en cuanto a la seguridad de la información a través de talleres, seminarios y campañas internas.

10. CUMPLIMIENTO LEGAL

- Las políticas de seguridad cumplirán con las normativas nacionales e internacionales aplicables, como la Ley de Protección de Datos Personales y las regulaciones locales sobre seguridad de la información.
- Se garantizará que el tratamiento de la información de los ciudadanos y empleados cumpla con los principios de licitud, consentimiento informado y protección adecuada.

11. MONITOREO Y AUDITORÍA

- Se realizará un monitoreo continuo de los sistemas de información para detectar comportamientos sospechosos o no autorizados.

- Se llevarán a cabo auditorías periódicas para asegurar el cumplimiento de estas políticas y evaluar posibles áreas de mejora.

Revisión y Actualización

Estas políticas serán revisadas y actualizadas anualmente o cuando sea necesario debido a cambios en las leyes, normativas o tecnología utilizada por el Instituto.

12. CRONOGRAMA DE TRABAJO

Fase	Actividad	Periodo	Responsable	Producto / Resultado
Planeación	Socialización del Plan de Tratamiento del Riesgo Informático	**Permanente (Ene – Dic)**	Apoyo TIC	Acta de socialización
Planeación	Identificación y priorización de riesgos informáticos	**Permanente (Ene – Dic)**	Apoyo TIC / Control Interno	Matriz de riesgos validada
Alistamiento	Definición de controles técnicos y administrativos	**Permanente (Ene – Dic)**	Apoyo TIC	Controles definidos
Implementación	Implementación de política de contraseñas	**Permanente (Ene – Dic)**	Apoyo TIC	Política aplicada
Implementación	Control de accesos por roles	**Permanente (Ene – Dic)**	Apoyo TIC	Usuarios y permisos definidos
Operación	Fortalecimiento de antivirus y parches de seguridad	**Permanente (Ene – Dic)**	Apoyo TIC / Proveedor	Equipos protegidos y actualizados
Operación	Implementación de backups periódicos	**Permanente (Ene – Dic)**	Apoyo TIC	Copias de seguridad operativas
Capacitación	Capacitación en seguridad de la información	**Permanente (Ene – Dic)**	Apoyo TIC / Talento Humano	Funcionarios capacitados
Seguimiento	Monitoreo de incidentes de seguridad	**Permanente (Ene – Dic)**	Apoyo TIC	Registro de incidentes
Control	Auditoría interna de riesgos informáticos	**Permanente (Ene – Dic)**	Control Interno	Informe de auditoría
Evaluación	Ajustes y actualización del plan	**Permanente (Ene – Dic)**	Apoyo TIC	Plan actualizado