



Alcaldía de Rionegro
Departamento de Antioquia

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PSPI

**INSTITUTO MUNICIPAL DE EDUCACIÓN FÍSICA, DEPORTE Y RECREACIÓN DE
RIONEGRO – IMER**

2026



CONTENIDO

INTRODUCCION.....	3
OBJETIVOS.....	4
Objetivo General	4
Objetivos Específicos	4
Marco normativo	6
Principios de Seguridad y Privacidad de la Información.....	8
Principios para la Políticas de Seguridad de la Información	9
Controles de Seguridad Implementados	9
Plan de Implementación	10
Responsables.....	10
Seguimiento y Control.....	10

INTRODUCCIÓN

El Instituto Municipal de Educación Física, Deporte y recreación de Rionegro - IMER, en cumplimiento de los lineamientos del Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establece el presente Plan de Seguridad y Privacidad de la Información, con el propósito de proteger los activos de información institucional, garantizar su adecuado manejo y prevenir riesgos asociados al uso de las tecnologías de la información.

OBJETIVOS

Objetivo General

Establecer lineamientos y acciones orientadas a proteger la información institucional del IMER, garantizando su confidencialidad, integridad y disponibilidad, mediante la implementación de controles de seguridad y buenas prácticas en el uso de los sistemas de información y tecnologías institucionales.

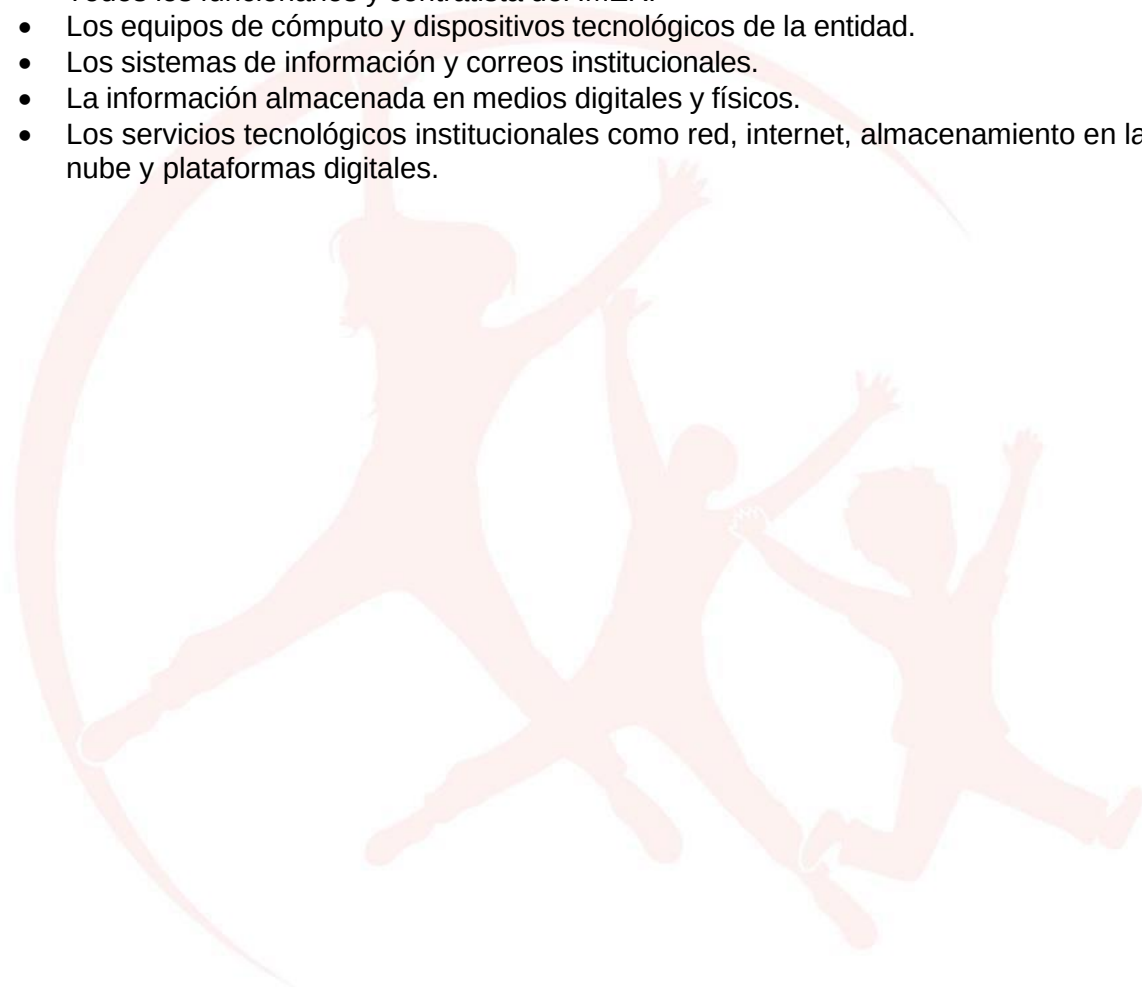
Objetivos Específicos

- Definir y establecer la estrategia de seguridad digital del Instituto.
- Definir y establecer las necesidades del Instituto, para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

ALCANCE

El presente plan aplica a:

- Todos los funcionarios y contratista del IMER.
- Los equipos de cómputo y dispositivos tecnológicos de la entidad.
- Los sistemas de información y correos institucionales.
- La información almacenada en medios digitales y físicos.
- Los servicios tecnológicos institucionales como red, internet, almacenamiento en la nube y plataformas digitales.



MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información del Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro (IMER) se fundamenta en las disposiciones legales y lineamientos establecidos por el Gobierno Nacional en materia de gestión de la información, seguridad digital, protección de datos personales y transparencia.

A continuación, se relaciona el marco normativo aplicable:

Normatividad	Entidad	Descripción
Resolución 02277 de 2025	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
Circular Externa No. 002 del 21 de agosto de 2024	Superintendencia de Industria y Comercio	Lineamientos sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial.
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 2893 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano, y se dictan otras disposiciones.

Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones – TIC
CONPES 3995 de 2020	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
CONPES 3854 de 2016	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Se expide el Decreto Único Reglamentario del sector Tecnologías de la Información y las Comunicaciones
Ley 1712 de 2014	Presidencia de la Republica	Ley de transparencia y el derecho a la información pública nacional
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales
CONPES 3701 de 2011	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Principios de Seguridad y Privacidad de la Información

- **Confidencialidad:** El Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro (IMER) garantizará que la información confidencial se mantenga protegida y solo sea accesible para las personas autorizadas. Se establecerán mecanismos adecuados para clasificar y controlar el acceso a la información confidencial.
- **Integridad:** Se implementarán controles y medidas técnicas para proteger la información contra modificaciones no autorizadas.
- **Disponibilidad:** Se implementarán medidas para garantizar la disponibilidad de la información cuando sea requerida, evitando interrupciones no planificadas y asegurando la continuidad de los servicios.
- **Autenticidad:** Permite verificar la identidad de los usuarios o sistemas, asegurando que quien accede a la información Asegurar que la información esté disponible cuando sea requerida por los usuarios autorizados.es realmente quien dice ser.
- **Cumplimiento Legal:** El Instituto Municipal de Educación Física, Deporte y Recreación de Rionegro (IMER), cumplirá con todas las leyes y regulaciones aplicables en materia de seguridad y privacidad de la información. Se establecerán mecanismos para identificar, evaluar y mitigar los riesgos de incumplimiento.
- **Responsabilidad:** Todos los usuarios y miembros del personal serán responsables de la seguridad y privacidad de la información a la que tengan acceso. Se promoverá la conciencia y formación en seguridad de la información para asegurar el cumplimiento de esta política.

Medidas de Seguridad y Privacidad de la Información

- **Identificación y Clasificación de la Información:** Se establecerán procedimientos para identificar y clasificar la información de acuerdo con su nivel de confidencialidad, definiendo los controles de seguridad apropiados para cada categoría de información.
- **Acceso y Control de la Información:** Se establecerán controles de acceso basados en los principios de “necesidad de conocer” y “menor privilegio”. Se implementarán mecanismos de autenticación y autorización para garantizar que solo las personas autorizadas tengan acceso a la información.

- **Protección de los Activos de Información:** Se implementarán medidas técnicas y físicas para proteger los activos de información contra amenazas internas y externas. Esto incluirá la utilización de firewalls, antivirus, encriptación de datos, control de acceso físico, entre otros.
- **Gestión de Incidentes de Seguridad:** Se establecerá un proceso de gestión de incidentes de seguridad para detectar, notificar, investigar y responder a los incidentes de seguridad de la información de manera oportuna y efectiva.
- **Protección de la Privacidad:** Se adoptarán medidas para proteger la privacidad de los individuos cuya información personal sea recolectada, utilizada y almacenada por el Instituto Municipal del Deporte y la Recreación de Palmira. Se cumplirá con las leyes y regulaciones aplicables en materia de privacidad de datos personales.
- **Continuidad del Negocio:** Se desarrollará un plan de continuidad del negocio que asegure la disponibilidad de la información y los servicios en caso de eventos que puedan interrumpir las operaciones normales.

Principios para la Política de Seguridad de la Información

El Instituto Municipal de Educación Física, Deporte y recreación de Rionegro – IMER, establece los siguientes principios:

- Uso adecuado de los equipos de cómputo institucionales.
- Protección y manejo seguro de contraseñas.
- Realización periódica de copias de seguridad (backup).
- Control de acceso a la información institucional.
- Uso adecuado del correo institucional.
- Protección de datos personales.
- Uso responsable de internet y redes institucionales.

Controles de Seguridad Implementados

Entre las medidas implementadas se encuentran:

- Copias de seguridad periódicas mediante OneDrive.
- Actualización de sistemas operativos y software.
- Uso de antivirus y herramientas de protección.
- Restricción de instalación de software no autorizado.
- Monitoreo del uso de los recursos tecnológicos.

Plan de Implementación

Las acciones para implementar el plan incluyen:

- Capacitación a funcionarios en seguridad de la información.
- Implementación de políticas de manejo de contraseñas.
- Respaldo periódico de la información institucional.
- Revisión y actualización de los equipos tecnológicos.
- Implementación de controles de acceso a sistemas.

Responsables

- **Comité Institucional Gestión y Desempeño**– Aprobación del plan.
- **Área de Sistemas** – Implementación y seguimiento.
- **Funcionarios y contratistas** – Cumplimiento de las políticas establecidas.

Seguimiento y Control

El seguimiento al cumplimiento del presente plan se realizará mediante:

- Revisión periódica de las copias de seguridad.
- Evaluación del uso adecuado de los recursos tecnológicos.
- Verificación del cumplimiento de las políticas de seguridad.
- Actualización del plan cuando sea necesario.