

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
UNIDAD DE SALUD DE IBAGUÉ E.S.E.
Vigencia 2026

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Unidad de Salud de Ibagué E.S.E. establece los lineamientos, controles y acciones orientadas a proteger la confidencialidad, integridad y disponibilidad de la información institucional, garantizando su uso adecuado en el desarrollo de los procesos misionales, estratégicos y administrativos.

Este plan se formula en coherencia con el **Plan Estratégico de Tecnologías de la Información – PETI**, el **Modelo Integrado de Planeación y Gestión – MIPG**, la **Política de Gobierno Digital** y los lineamientos de **Seguridad Digital** definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

OBJETIVO

Establecer el marco de referencia para la gestión de la seguridad y privacidad de la información en la Unidad de Salud de Ibagué E.S.E., mediante la definición de controles, responsabilidades e indicadores que permitan mitigar los riesgos asociados al tratamiento, almacenamiento y uso de la información institucional.

ALCANCE

El presente Plan de Seguridad y Privacidad de la Información aplica a:

- Toda la información institucional, en formato físico y digital.
- Los sistemas de información, bases de datos y plataformas tecnológicas.
- La infraestructura tecnológica (Datacenter, redes, equipos y servicios).
- Los funcionarios, contratistas y terceros que tengan acceso a la información institucional.
- Los procesos misionales, estratégicos y de apoyo de la entidad.

MARCO NORMATIVO

El presente plan se formula con fundamento en la siguiente normatividad:

- Constitución Política de Colombia
- Ley 1581 de 2012 – Protección de Datos Personales
- Decreto 1074 de 2015
- Ley 1273 de 2009 – Delitos Informáticos
- Decreto 1078 de 2015 – Sector TIC
- Política de Gobierno Digital
- Modelo Integrado de Planeación y Gestión – MIPG
- Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Norma ISO/IEC 27001 e ISO/IEC 27002 (como referencia técnica)

ARTICULACIÓN CON EL PETI

El Plan de Seguridad y Privacidad de la Información se articula directamente con el **Plan Estratégico de Tecnologías de la Información – PETI**, desarrollando el componente de **Seguridad Digital** y fortaleciendo la gestión de riesgos tecnológicos asociados a la operación institucional.

Los controles y acciones definidos en este plan complementan los proyectos, indicadores y lineamientos establecidos en el PETI, garantizando la protección de la información que soporta la prestación de los servicios de salud y la gestión administrativa.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información en la Unidad de Salud de Ibagué E.S.E. se rige por los siguientes principios:

- **Confidencialidad:** Protección de la información frente a accesos no autorizados.
- **Integridad:** Garantía de exactitud y completitud de la información.
- **Disponibilidad:** Acceso oportuno a la información cuando sea requerida.
- **Legalidad:** Cumplimiento de la normatividad vigente.
- **Responsabilidad:** Uso adecuado de la información por parte de los usuarios.

ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Alta Dirección	Aprobar y respaldar el plan
Área de Tecnologías de la Información	Implementar y hacer seguimiento
Líder del Área de TI	Responsable del PSPI
Usuarios	Cumplir las políticas de seguridad
Terceros	Cumplir acuerdos de confidencialidad

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

La entidad implementa los siguientes controles de seguridad:

- Gestión de accesos a sistemas de información.
- Seguridad perimetral y lógica (firewall, segmentación de red).
- Gestión de respaldos y recuperación de información.
- Continuidad del servicio y contingencia tecnológica.
- Protección de datos personales.
- Gestión de incidentes de seguridad de la información.

- Sensibilización y buenas prácticas en seguridad digital.

INDICADORES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Indicador 1. Cumplimiento de controles de seguridad

Fórmula:

Controles implementados / Controles definidos \times 100

Frecuencia: Semestral

Meta: $\geq 90 \%$

Responsable: Área de Tecnologías de la Información

Indicador 2. Disponibilidad de la información crítica

Fórmula:

$(\text{Tiempo total del período} - \text{Tiempo de indisponibilidad}) / \text{Tiempo total del período} \times 100$

Frecuencia: Mensual

Meta: $\geq 99 \%$

Responsable: Área de Tecnologías de la Información

Indicador 3. Gestión oportuna de incidentes de seguridad

Fórmula:

Incidentes gestionados / Incidentes reportados \times 100

Frecuencia: Mensual

Meta: $\geq 95 \%$

Responsable: Área de Tecnologías de la Información

Indicador 4. Cumplimiento de respaldos y recuperación

Fórmula:

Respaldos exitosos / Respaldos programados \times 100

Frecuencia: Mensual

Meta: $\geq 98 \%$

Responsable: Área de Tecnologías de la Información

Indicador 5. Protección de datos personales

Fórmula:

Procesos con medidas de protección / Procesos con tratamiento de datos personales $\times 100$

Frecuencia: Anual

Meta: 100 %

Responsable: Área de TI / Área Jurídica

Indicador 6. Sensibilización en seguridad de la información

Fórmula:

funcionarios capacitados / Funcionarios programados $\times 100$

Frecuencia: Anual

Meta: ≥ 90 %

Responsable: Área de Tecnologías de la Información

SEGUIMIENTO Y MEJORA CONTINUA

El seguimiento al presente Plan de Seguridad y Privacidad de la Información se realizará mediante los indicadores definidos y será presentado periódicamente al **Comité de Gestión y Desempeño**, como parte del sistema de control y mejora continua institucional.

Los resultados del seguimiento permitirán identificar brechas, definir acciones de mejora y fortalecer la madurez en seguridad digital.

VIGENCIA

El presente Plan de Seguridad y Privacidad de la Información tendrá vigencia anual correspondiente a la vigencia **2026**, y será actualizado conforme a los cambios normativos, tecnológicos y de riesgos institucionales.

APROBACIÓN

El presente plan será sometido a aprobación de la Alta Dirección y adoptado como documento institucional de referencia para la gestión de la seguridad y privacidad de la información.



SAUL BETANCOURTH CARO

Profesional Universitario Sistemas