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

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Unidad de Salud de Ibagué E.S.E. establece las acciones orientadas a gestionar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Este plan se formula como complemento del **Plan de Seguridad y Privacidad de la Información**, del **Plan Estratégico de Tecnologías de la Información – PETI**, y en cumplimiento de los lineamientos del **Modelo de Seguridad y Privacidad de la Información – MSPI**, la **Política de Seguridad Digital** y el **Modelo Integrado de Planeación y Gestión – MIPG**.

OBJETIVO

Definir e implementar acciones de tratamiento que permitan reducir el impacto y la probabilidad de ocurrencia de los riesgos de seguridad y privacidad de la información, garantizando la continuidad operativa, la protección de los datos personales y la confiabilidad de la información institucional.

ALCANCE

El presente plan aplica a:

- Información institucional en formato físico y digital.
- Sistemas de información y bases de datos.
- Infraestructura tecnológica (Datacenter, redes y conectividad).
- Funcionarios, contratistas y terceros con acceso a la información.
- Procesos misionales, estratégicos y de apoyo.

MARCO NORMATIVO

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

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

METODOLOGÍA DE GESTIÓN DEL RIESGO

La gestión del riesgo de seguridad y privacidad de la información se desarrolla mediante las siguientes etapas:

1. Identificación de riesgos
2. Análisis del riesgo (probabilidad e impacto)
3. Evaluación del nivel de riesgo inherente
4. Definición del tratamiento del riesgo
5. Evaluación del riesgo residual
6. Seguimiento y control

ESCALA DE VALORACIÓN DEL RIESGO

Probabilidad

Valor	Descripción
1	Baja
2	Media
3	Alta

Impacto

Valor	Descripción
1	Bajo
2	Medio
3	Alto

Nivel de Riesgo

Nivel de Riesgo = Probabilidad × Impacto

Resultado	Nivel
1 – 2	Bajo
3 – 4	Medio
6 – 9	Alto

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

CRITERIOS DE TRATAMIENTO DEL RIESGO

Los riesgos identificados se tratan de acuerdo con las siguientes opciones:

- **Mitigar:** Reducir el riesgo mediante controles.
- **Aceptar:** Asumir el riesgo dentro del nivel tolerable.
- **Evitar:** Eliminar la causa del riesgo.
- **Transferir:** Compartir el riesgo con terceros.

MATRIZ DE TRATAMIENTO DE RIESGOS

Riesgo 1. Pérdida de información crítica

- **Activo:** Bases de datos institucionales
- **Amenaza:** Fallas técnicas / error humano
- **Vulnerabilidad:** Fallas en respaldo o recuperación
- **Probabilidad:** 2 (Media)
- **Impacto:** 3 (Alto)
- **Nivel de Riesgo Inherente:** 6 – Alto
- **Tratamiento:** Mitigar
- **Acciones de Tratamiento:**
    - Implementación de backups externos
    - Pruebas periódicas de restauración
- **Nivel de Riesgo Residual:** 3 – Medio
- **Responsable:** Área de Tecnologías de la Información

Riesgo 2. Acceso no autorizado a la información

- **Activo:** Sistemas de información
- **Amenaza:** Ataques informáticos / uso indebido de credenciales
- **Vulnerabilidad:** Controles de acceso insuficientes
- **Probabilidad:** 2 (Media)
- **Impacto:** 3 (Alto)
- **Nivel de Riesgo Inherente:** 6 – Alto
- **Tratamiento:** Mitigar
- **Acciones de Tratamiento:**
    - Firewall perimetral de nueva generación
    - Gestión de usuarios y perfiles de acceso
- **Nivel de Riesgo Residual:** 3 – Medio
- **Responsable:** Área de Tecnologías de la Información

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

Riesgo 3. Indisponibilidad de servicios tecnológicos

- **Activo:** Datacenter y red
- **Amenaza:** Fallas eléctricas o de conectividad
- **Vulnerabilidad:** Dependencia de infraestructura crítica
- **Probabilidad:** 2 (Media)
- **Impacto:** 3 (Alto)
- **Nivel de Riesgo Inherente:** 6 – Alto
- **Tratamiento:** Mitigar
- **Acciones de Tratamiento:**
  - Adecuación del Datacenter
  - Enlaces de contingencia
- **Nivel de Riesgo Residual:** 3 – Medio
- **Responsable:** Área de Tecnologías de la Información

Riesgo 4. Incumplimiento en protección de datos personales

- **Activo:** Información personal de usuarios
- **Amenaza:** Manejo inadecuado de datos
- **Vulnerabilidad:** Falta de controles y sensibilización
- **Probabilidad:** 1 (Baja)
- **Impacto:** 3 (Alto)
- **Nivel de Riesgo Inherente:** 3 – Medio
- **Tratamiento:** Mitigar
- **Acciones de Tratamiento:**
  - Implementación de políticas de tratamiento de datos
  - Capacitación al personal
- **Nivel de Riesgo Residual:** 2 – Bajo
- **Responsable:** Área de TI

Riesgo 5. Falta de conocimiento en seguridad de la información

- **Activo:** Talento humano
- **Amenaza:** Errores por desconocimiento
- **Vulnerabilidad:** Falta de capacitación
- **Probabilidad:** 2 (Media)
- **Impacto:** 2 (Medio)
- **Nivel de Riesgo Inherente:** 4 – Medio
- **Tratamiento:** Mitigar
- **Acciones de Tratamiento:**
  - Programas de sensibilización

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

- Capacitaciones periódicas
- **Nivel de Riesgo Residual:** 2 – Bajo
- **Responsable:** Área de Tecnologías de la Información

INDICADORES DEL PLAN DE TRATAMIENTO DE RIESGOS

Indicador 1. Riesgos de Seguridad de la Información Tratados

Descripción:
Mide el porcentaje de riesgos de seguridad y privacidad de la información que cuentan con acciones de tratamiento implementadas.

Fórmula:
Riesgos tratados / Riesgos identificados × 100

Frecuencia: Trimestral
Meta: ≥ 90 %
Responsable: Área de Tecnologías de la Información

Indicador 2. Cumplimiento de Acciones de Tratamiento de Riesgos

Descripción:
Mide el grado de ejecución de las acciones definidas en el plan de tratamiento de riesgos.

Fórmula:
Acciones de tratamiento ejecutadas / Acciones de tratamiento definidas × 100

Frecuencia: Mensual
Meta: ≥ 90 %
Responsable: Área de Tecnologías de la Información

Indicador 3. Reducción del Nivel de Riesgo Residual

Descripción:
Mide la efectividad de los controles implementados, comparando el nivel de riesgo inherente frente al riesgo residual.

Fórmula:
Riesgos con nivel residual menor al inherente / Riesgos tratados × 100

Frecuencia: Semestral
Meta: ≥ 80 %
Responsable: Área de Tecnologías de la Información

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

Indicador 4. Riesgos Críticos Mitigados

Descripción:
Mide el porcentaje de riesgos clasificados como altos o críticos que han sido mitigados mediante controles implementados.

Fórmula:
Riesgos críticos mitigados / Total de riesgos críticos × 100

Frecuencia: Semestral
Meta: ≥ 85 %
Responsable: Área de Tecnologías de la Información

Indicador 5. Incidentes Asociados a Riesgos Identificados

Descripción:
Mide la proporción de incidentes de seguridad relacionados con riesgos previamente identificados.

Fórmula:
Incidentes asociados a riesgos identificados / Total de incidentes reportados × 100

Frecuencia: Mensual
Meta: ≤ 10 %
Responsable: Área de Tecnologías de la Información

Indicador 6. Actualización del Mapa de Riesgos de Seguridad de la Información

Descripción:
Mide el cumplimiento en la actualización periódica del mapa de riesgos de seguridad y privacidad de la información.

Fórmula:
Actualizaciones realizadas / Actualizaciones programadas × 100

Frecuencia: Anual
Meta: 100 %
Responsable: Área de Tecnologías de la Información

SEGUIMIENTO Y CONTROL

El seguimiento al presente plan se realizará mediante los indicadores definidos y será presentado periódicamente al **Comité de Gestión y Desempeño**, permitiendo evaluar la efectividad de los controles implementados y la reducción del riesgo residual.

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

VIGENCIA

El presente Plan de Tratamiento de Riesgos tendrá vigencia anual correspondiente a la vigencia **2026**, y será actualizado cuando se presenten cambios significativos en los riesgos, la tecnología o la normatividad aplicable.

APROBACIÓN

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

SAUL BETANCOURTH CARO

Profesional Universitario Sistemas

"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co