# TRATAMIENTO DE RIESGOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024-2027

## INTRODUCCIÓN AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El entorno actual de la atención médica está marcado por avances tecnológicos significativos y una creciente dependencia de sistemas de información para la gestión eficiente de los datos clínicos y administrativos. En este contexto, la seguridad y privacidad de la información se vuelven imperativas para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como el cumplimiento de las normativas y la preservación de la confianza del paciente.
Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se presenta como un marco integral diseñado para identificar, evaluar y gestionar proactivamente los riesgos asociados con la información confidencial en La Unidad de Salud de Ibagué. Este plan refleja nuestro compromiso continuo con la excelencia en la gestión de la información, la protección de la privacidad del paciente y el mantenimiento de los más altos estándares de seguridad de la información.

### OBJETIVOS DEL PLAN

1. Protección de la Información Sensible:
   - Salvaguardar la información médica y administrativa crítica, garantizando su confidencialidad y evitando accesos no autorizados.

2. Cumplimiento Normativo:
   - Asegurar el cumplimiento de las leyes y regulaciones locales e internacionales relacionadas con la privacidad de la información, incluyendo la Ley Estatutaria 1581 de 2012 sobre Protección de Datos Personales en Colombia.

3. Resiliencia ante Amenazas:
   - Desarrollar y mantener la capacidad de respuesta frente a posibles amenazas y eventos adversos que puedan afectar la seguridad y privacidad de la información.

4. Cultura de Seguridad:
   - Fomentar una cultura organizacional en la que el personal comprenda la importancia de la seguridad de la información y esté comprometido con prácticas seguras.

### ALCANCE DEL PLAN:

Este plan abarca todos los aspectos relacionados con la seguridad y privacidad de la información en la Unidad de Salud de Ibagué. Esto incluye, pero no se limita a, datos médicos de pacientes, información administrativa, registros financieros y cualquier otro tipo de información sensible que forme parte de las operaciones diarias de la entidad

## ENFOQUE METODOLÓGICO

El desarrollo y ejecución de este plan seguirán una metodología estructurada que incluye:

1. Identificación de Riesgos:
Analizar y reconocer las amenazas potenciales y vulnerabilidades que podrían comprometer la seguridad y privacidad de la información.
2. Análisis de Riesgos:
Evaluar la probabilidad y el impacto de cada riesgo identificado para priorizar las acciones de tratamiento.
3. Desarrollo de Controles:
Implementar controles y salvaguardas para mitigar los riesgos y fortalecer la seguridad de la información.
4. Políticas y Procedimientos:
Establecer políticas y procedimientos claros que guíen al personal en prácticas seguras y en la gestión adecuada de la información.
5. Monitoreo y Revisión Continua:
Implementar sistemas de monitoreo continuo y revisiones periódicas para adaptar el plan a los cambios en los riesgos y la tecnología.
Este plan es una herramienta dinámica que evolucionará en respuesta a nuevas amenazas, cambios en la tecnología y lecciones aprendidas de incidentes anteriores. El compromiso de la Unidad de Salud de Ibague con la seguridad y privacidad de la información es fundamental para mantener la confianza de nuestros pacientes y la integridad de nuestras operaciones. Este documento sirve como guía para garantizar que la información crítica sea manejada de manera segura y ética, cumpliendo con los más altos estándares profesionales y legales.

## ESCALA DE MEDICION DE LOS RIESGOS DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

La medición de riesgos en la seguridad y privacidad de la información en las entidades del sector salud implica evaluar la probabilidad e impacto de posibles eventos que podrían comprometer la confidencialidad, integridad y disponibilidad de los datos. Aquí te presento una posible escala de medición de riesgos adaptada para un entorno hospitalario:

**1. PROBABILIDAD:**
Muy Baja (1): La ocurrencia del evento es extremadamente improbable.

Baja (2): La ocurrencia del evento es poco probable, pero no se puede descartar completamente.
Moderada (3): La ocurrencia del evento tiene una probabilidad significativa.
Alta (4): La ocurrencia del evento es probable y puede ocurrir con cierta frecuencia.
Muy Alta (5): La ocurrencia del evento es casi segura o muy probable.

**2. IMPACTO:**
Bajo (1): El impacto del evento es mínimo y tiene poco efecto en la seguridad y privacidad de la información.
Moderado (2): El impacto tiene consecuencias moderadas y podría afectar la operación normal.
Significativo (3): El impacto es significativo y podría causar interrupciones importantes.
Alto (4): El impacto es alto y podría resultar en pérdida considerable de datos o servicios.
Muy Alto (5): El impacto es crítico y podría tener consecuencias graves para la seguridad y privacidad.

**3. RIESGO TOTAL (PROBABILIDAD X IMPACTO):**
Bajo (15): Riesgo mínimo; se requieren acciones mínimas.
Moderado (610): Riesgo aceptable; se deben implementar medidas preventivas y de mitigación.
Alto (1115): Riesgo significativo; se necesitan acciones inmediatas y medidas intensivas.
Muy Alto (1625): Riesgo crítico; se requieren acciones urgentes y medidas de mitigación inmediatas.
4. PRIORIZACIÓN DE RIESGOS:
Bajo (15): Riesgos pueden ser aceptados con seguimiento periódico.
Moderado (610): Requiere acciones preventivas y monitoreo continuo.
Alto (1115): Acciones inmediatas y seguimiento riguroso son esenciales.
Muy Alto (1625): Acciones urgentes y medidas intensivas son críticas.
Esta escala permite evaluar la probabilidad, impacto y riesgo total de eventos que podrían afectar la seguridad y privacidad de la información la Unidad de Salud de Ibagué. Cuantificar estos factores ayuda a priorizar acciones y asignar recursos de manera eficiente para gestionar los riesgos de manera efectiva. Es fundamental revisar y actualizar regularmente esta evaluación a medida que cambian las circunstancias y la infraestructura tecnológica de la Unidad de Salud de Ibague.

**MEDICION DE RIESGOS**

A continuación, proporcionamos un ejemplo de clasificación de riesgos de la seguridad y privacidad de la información que se pueden dar en la unidad de salud de Ibagué utilizando una escala de 1 a 5 para probabilidad e impacto.

**Riesgo 1:** Acceso No Autorizado a Datos Médicos
Probabilidad: 3 (Moderada)
Impacto: 4 (Alto)
Riesgo = 3 x 4 = 12
Clasificación: Riesgo Alto

**Riesgo 2: Ataque de Ransomware**
- Probabilidad: 2 (Baja)
- Impacto: 5 (Muy Alto)
Riesgo = 2 x 5 = 10
Clasificación: Riesgo Moderado

**Riesgo 3: Fallo en la Infraestructura de Red**
- Probabilidad: 3 (Moderada)
- Impacto: 3 (Significativo)
Riesgo = 3 x 3 = 9
Clasificación: Riesgo Moderado

**Riesgo 4: Errores Humanos En La Administración De Datos**
- Probabilidad: 4 (Alta)
- Impacto: 2 (Moderado)
Riesgo = 4 x 2 = 8
Clasificación: Riesgo Moderado

**Riesgo 5: Incumplimiento Normativo en la Gestión de Datos**
- Probabilidad: 2 (Baja)
- Impacto: 4 (Alto)
Riesgo = 2 x 4 = 8
Clasificación: Riesgo Moderado

**Riesgo 6: Falta de Actualizaciones de Seguridad**
- Probabilidad: 3 (Moderada)
- Impacto: 3 (Significativo)
Riesgo = 3 x3 = 9
Clasificación: Riesgo Moderado

Riesgo 7: Falta de Concientización del Personal en Seguridad
Probabilidad: 4 (Alta)
Impacto: 2 (Moderado)
Riesgo = 4 x 2 = 8
Clasificación: Riesgo Moderado

## INTERPRETACIÓN:

- Riesgo Alto (12-25): Requiere acciones inmediatas y medidas intensivas.
- Riesgo Moderado (6-11): Requiere acciones preventivas y monitoreo continuo.
- Riesgo Bajo (1-5): Puede ser aceptado con seguimiento periódico.

### CONCLUSION

El tratamiento de riesgos en seguridad y privacidad de la información es un proceso crítico para salvaguardar la integridad, confidencialidad y disponibilidad de los datos en cualquier organización, especialmente en entornos sensibles como los hospitales.

En conclusión, el tratamiento de riesgos en seguridad y privacidad de la información no es solo un proceso técnico, sino una estrategia holística que involucra a toda la organización. Un enfoque proactivo y una cultura de seguridad sólida son fundamentales para proteger la información crítica en un entorno hospitalario.