ESE Hospital
San Juan de Dios
Santa Fe de Antioquia

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SANTIAGO VARELA MACIAS

GERENTE

JUAN DAVID ECHEVERRY

INGENIERO DE SISTEMAS

2026

CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital San Juan de Dios tiene como propósito establecer las acciones necesarias para mitigar, reducir y controlar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional. Este plan se desarrolla como parte fundamental del Sistema de Gestión de Seguridad de la Información y constituye un apoyo directo a la continuidad operativa, la protección de los datos de los pacientes y el cumplimiento normativo vigente en el sector salud.

El Hospital reconoce que, debido a limitaciones actuales en recursos humanos, tecnológicos y presupuestales, no es posible implementar de manera inmediata todos los controles ideales recomendados por los estándares internacionales. Sin embargo, se adoptan medidas alineadas con la realidad institucional, priorizando los riesgos que pueden tener mayor impacto operativo, asistencial o legal. Este plan, por tanto, se construye bajo un enfoque progresivo, basado en la capacidad instalada y en el fortalecimiento gradual de los procesos de seguridad.

Asimismo, el Plan de Tratamiento de Riesgos busca establecer controles compensatorios que permitan disminuir vulnerabilidades mientras el Hospital avanza en la consolidación de una infraestructura más robusta y, cuando sea necesario, en la vinculación de proveedores especializados que apoyen la gestión de seguridad, copias de respaldo, continuidad y protección de datos.

2. OBJETIVO GENERAL

Establecer y ejecutar un plan de tratamiento de riesgos de seguridad y privacidad de la información que permita identificar, analizar, evaluar y mitigar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, garantizando el cumplimiento de la normatividad vigente, la protección de los datos personales y sensibles, y la continuidad de los procesos misionales y administrativos de la organización.

3. OBJETIVOS ESPECÍFICOS

1. Identificar y priorizar los riesgos de seguridad y privacidad que afectan la información institucional, enfocándose en aquellos que representan mayor impacto para los procesos asistenciales, administrativos y misionales del Hospital.
2. Establecer controles y acciones de mitigación acordes con la capacidad operativa actual, reconociendo las limitaciones de personal especializado, infraestructura tecnológica y recursos económicos.

3. Definir medidas progresivas y viables, que permitan fortalecer la seguridad de la información de manera gradual, sin afectar la operación diaria y adaptándose a las condiciones reales del Hospital.
4. Implementar controles compensatorios que permitan reducir vulnerabilidades mientras se avanza hacia soluciones más robustas, como la adquisición de herramientas especializadas o la contratación de proveedores externos.
5. Garantizar la continuidad de los servicios críticos, protegiendo la disponibilidad de la información clínica, operativa y administrativa mediante mecanismos de respaldo básicos pero esenciales.
6. Cumplir con los requisitos legales y regulatorios relacionados con la protección de datos personales, la seguridad de la información en salud y la gestión del riesgo institucional.

4. ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a los procesos, sistemas, activos y datos institucionales del Hospital San Juan de Dios que son necesarios para la prestación de los servicios asistenciales, administrativos y de apoyo. Su alcance abarca las siguientes áreas:

1. Sistemas de información institucionales
2. Infraestructura tecnológica
3. Información crítica y sensible
4. Procesos internos que soportan la gestión de seguridad y privacidad
5. Actividades y controles implementados directamente por el área de Sistemas
6. Controles compensatorios aplicables a áreas administrativas y asistenciales
7. Proveedores y terceros relacionados con servicios tecnológicos

5. DEFINICIONES

* Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos
* Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
*

* Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
* Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
* Impacto: son las consecuencias que genera un riesgo una vez se materialice.
* Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

6. MARCO REFERENCIAL

6.1. Política de Administración de Riesgos

El Hospital San Juan de Dios de Santa Fe de Antioquia se compromete a fortalecer y mantener una cultura institucional orientada a la gestión integral del riesgo, que permita prevenir, detectar, mitigar y monitorear oportunamente cualquier acontecimiento que pueda afectar la seguridad y privacidad de la información, la seguridad digital, la continuidad operativa, la transparencia institucional y el cumplimiento normativo.

La gestión del riesgo en el Hospital se fundamenta en prácticas sistemáticas y en la implementación de controles técnicos, administrativos y operativos, en concordancia con los lineamientos del sector TIC, las normas de protección de datos personales, las directrices del Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y las necesidades reales de operación de nuestros servicios asistenciales y de apoyo.

La Entidad promueve mecanismos de prevención y detección temprana que garanticen:

* La protección, integridad, confidencialidad y disponibilidad de la información institucional, clínica, administrativa y financiera.
* La continuidad de los servicios críticos, incluyendo plataformas tecnológicas, sistemas de información y servicios asistenciales soportados en TIC.
* La adecuada administración de riesgos asociados a proveedores, tercerizados y servicios en la nube utilizados por el Hospital.

* El uso eficiente de los recursos destinados a la gestión del riesgo y la atención oportuna a los grupos de interés.

Como parte del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Hospital adopta las siguientes categorías de respuesta al riesgo:

1. Aceptar el riesgo

El Hospital podrá aceptar riesgos clasificados como bajos o aquellos para los cuales no sea viable técnica o económicamente implementar controles adicionales. La aceptación del riesgo deberá estar formalmente documentada y tendrá un seguimiento permanente. *Ningún riesgo asociado a corrupción será aceptado.*

2. Reducir o mitigar el riesgo

Consiste en implementar controles técnicos, administrativos, físicos y de seguridad digital que disminuyan la probabilidad de ocurrencia o el impacto del riesgo. Esto implica, entre otros: medidas de ciberseguridad, controles de acceso, gestión de identidades, copias de seguridad, segmentación de redes, capacitación continua, segregación de funciones y monitoreo permanente.

3. Evitar el riesgo

Implica suspender, no iniciar o no continuar con actividades que generen un riesgo inaceptable para la seguridad de la información, la operación o el cumplimiento normativo. Aplica especialmente cuando el riesgo excede la capacidad institucional de control.

4. Compartir o transferir el riesgo

Consiste en reducir la probabilidad o impacto del riesgo mediante la transferencia parcial a terceros responsables, sin dejar de lado la responsabilidad interna del Hospital. Ejemplos: pólizas de seguros, contratos de tercerización con cláusulas de seguridad, servicios especializados en la nube bajo acuerdos de nivel de servicio (SLA). Los riesgos relacionados con corrupción pueden compartirse, pero su responsabilidad no es transferible.

7. METODOLOGIAS

La metodología utilizada por el Hospital para el tratamiento de riesgos de seguridad y privacidad de la información se fundamenta en un proceso sistemático, continuo y basado en criterios objetivos que permiten garantizar la protección de los activos de información y la continuidad de los servicios asistenciales y administrativos.

El proceso se desarrolla bajo las siguientes fases:

FASE 1: Planeación de la gestión del riesgo

Objetivo: Definir el alcance y los responsables sin generar carga al área TI.

Actividades:

1. Definir alcance reducido: sistemas, procesos y datos críticos del Hospital.
2. Nombrar responsables mínimos (TI + líder del proceso afectado).
3. Revisar incidentes ocurridos en el último año.
4. Acordar herramientas simples:
    - Matriz en Excel
    - Evidencias en capturas o correos
5. Establecer frecuencia de revisión: **trimestral** (máximo 30 minutos).

FASE 2: Identificación y valoración de activos (rápida y práctica)

Objetivo: Identificar solo los activos críticos para no sobrecargar al equipo.

Activos considerados:

* Sistemas de información (HIS, facturación, laboratorio, RIPS, etc.)
* Base de datos y repositorios con información clínica o personal
* Infraestructura esencial (red, servidores, nube, Backups)
* Usuarios con rol crítico (secretarias, facturadores, médicos, TI)
* Servicios tercerizados o en la nube

Valoración rápida del activo:

* ¿Qué tan crítico es? (Bajo – Medio – Alto)
* ¿Qué datos maneja?
* ¿Qué pasa si falla?

Se registra solo lo esencial.

FASE 3: Identificación y análisis del riesgo

Objetivo: Detectar los riesgos de forma simple y priorizar lo importante.

Identificación:
Se consideran amenazas como: fallas técnicas, errores humanos, accesos indebidos, pérdida de información, ataques digitales, fallas de proveedor, indisponibilidad de red o HIS.

Análisis simplificado:
Probabilidad (1–3) + Impacto (1–3)

* 2–3 = Bajo
* 4 = Medio
* 5–6 = Alto

Solo los riesgos **altos** requieren intervención prioritaria.

FASE 4: Evaluación y priorización del riesgo

Objetivo: Definir qué riesgos deben tratarse primero.

Criterios:

* Riesgos que afecten atención del paciente.
* Riesgos sobre datos personales o clínicos.
* Riesgos recurrentes o sin control actual.

* Riesgos asociados a proveedores o sistemas externos.

Se seleccionan máximo **5 riesgos críticos**.

FASE 5: Tratamiento del Riesgo

Objetivo: Elegir el tratamiento realista para cada riesgo.

Se usan solo tres opciones:

1. Reducir

La más usada. Controles rápidos como:

* Cambios de contraseñas
* Restricción de accesos
* Revisión de perfiles en sistemas
* Backups semanales
* Sensibilización corta al personal
* Verificación de actualizaciones

2. Aceptar

Cuando el riesgo es bajo o no hay capacidad de control.
Se revisa trimestralmente.

3. Compartir

Para proveedores o sistemas externos.
Se piden evidencias mínimas: SLA, contrato, certificación, respaldo.

FASE 6: Implementación de controles (solo lo esencial)

Objetivo: Documentar controles de forma rápida y sin burocracia.

Cada control debe incluir:

* Responsable

* Acción puntual (una frase)
* Evidencia simple (captura o correo)

Ejemplo:
“Se habilitó el doble factor en Workspace – evidencia adjunta.”

No se requieren procedimientos extensos.

FASE 7: Monitoreo y revisión periódica (30 minutos cada trimestre)

Objetivo: Revisar si los controles funcionaron.

Actividades:

* Actualizar nivel del riesgo
* Registrar incidentes ocurridos
* Identificar nuevos riesgos si aparecieron
* Ajustar controles si es necesario

Se documenta en un registro trimestral.

FASE 8: Mejora continua

Objetivo: Mantener actualizado el plan, ajustando los riesgos y controles según incidentes y cambios en la operación del Hospital.

Actividades:

* Revisar los riesgos y controles de forma
* incorporar lecciones aprendidas
* actualizar la matriz cuando sea necesario y comunicar los cambios clave a los responsables.

Fase	Actividades	Responsable de la tarea	Fecha Inicio	Fecha Final
Fase 1 Planeación de la gestión del riesgo	Definir el alcance del proceso, los responsables, el cronograma y las herramientas que se utilizarán para gestionar los riesgos, tomando como base la información e inventarios ya existentes en el Hospital.	Equipo TI	Marzo	Marzo
Fase 2 Identificación y valoración de activos (rápida y práctica)	Realizar un inventario práctico de los activos de información (equipos, sistemas, bases de datos y procesos), clasificarlos según su importancia para la operación del Hospital y asignar un nivel de criticidad basado en su impacto ante una falla o incidente.	Equipo TI	Abril	Mayo
Fase 3 Identificación y análisis del riesgo	Identificar las amenazas y vulnerabilidades asociadas a cada activo y analizar cómo podrían afectar la operación del Hospital, determinando el nivel de riesgo según probabilidad e impacto.	Equipo TI	Junio	Junio
Fase 4 Evaluación y priorización del riesgo	Seleccionar la acción más adecuada para cada riesgo (aceptar, reducir, evitar o compartir) y definir los controles básicos que el Hospital puede implementar sin requerir grandes recursos.	Equipo TI	Julio	Julio
Fase 5 Tratamiento del riesgo	Seleccionar y aplicar los controles necesarios para disminuir el nivel de riesgo, priorizando acciones concretas y realizables como ajustes técnicos, mejoras de	Equipo TI	Agosto	Agosto

	acceso, fortalecimiento de respaldos y capacitaciones básicas al personal.			
Fase 6 Implementación de controles (solo lo esencial)	Ejecutar los controles definidos para cada riesgo, enfocándose únicamente en las acciones prioritarias y de mayor impacto, como ajustes de configuración, protección de accesos, buenas prácticas operativas y verificación básica de respaldos.	Equipo TI	Septiembre	Septiembre
Fase 7 Monitoreo y revisión periódica (30 minutos cada trimestre)	Realizar un seguimiento periódico del estado de los riesgos y verificar si los controles aplicados siguen funcionando, utilizando revisiones rápidas y registros simples para no cargar al personal.	Equipo TI	Octubre	Octubre
Fase 8 Mejora continua	Actualizar los riesgos, controles y acciones según incidentes, cambios tecnológicos o necesidades del Hospital, garantizando que el plan se mantenga vigente y ajustado a la realidad operativa.	Equipo TI	Noviembre	Noviembre

8. DESARROLLO METODOLOGICO

9. OPORTUNIDAD DE MEJORA

* Simplificar el plan y los formatos para facilitar su ejecución por parte de TI.
* Mantener actualizados los riesgos críticos y los activos del Hospital.
* Priorizar controles esenciales que generen alto impacto con poco esfuerzo.
* Mejorar la comunicación de riesgos y controles con los líderes de proceso.
* Implementar un seguimiento práctico mediante checklists breves.
* Incorporar incidentes y lecciones aprendidas para ajustar el plan.
* Alinear el plan con hallazgos de auditoría y requisitos normativos.

10. RECURSOS

El Hospital San Juan de Dios de Santa Fe de Antioquia, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través del proceso de seguridad y privacidad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

11. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios identificados en la entidad, corresponderá al dueño del riesgo quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento, como la gestión de sus recursos dentro de la planificación de estos.

12. ELABORACIÓN, REVISIÓN Y APROBACIÓN

12.1 CONTROL DEL CAMBIOS					
VERSIÓN	FECHA	DESCRIPCIÓN	ELABORÓ	REVISÓ	APROBÓ
01	Enero 2023	Elaboración del plan 2023	Juan David Echeverry	Nallybe Durán –	Claudia María Calderón –

			– Líder de sistemas	Subgerente de Calidad	Gerente
02	Enero 2024	Se actualiza Documento	Juan David Echeverry – Líder de sistemas	David Ramírez – Profesional de Calidad	Claudia María Calderón – Gerente
03	Enero 2025	Se ajusta de manera parcial el documento para la vigencia 2025.	Juan David Echeverry – Líder de TI	Jomara Usuga – Coordinadora de calidad	Santiago Varela Macias – Gerente
04	Enero 2026	Se ajusta de manera parcial el documento para la vigencia 2026.	Juan David Echeverry – Líder de TI	Jomara Usuga – Coordinadora de calidad	Santiago Varela Macias – Gerente