PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

1. INTRODUCCIÓN

En el contexto actual de transformación digital del sector salud, la seguridad y la privacidad de la información se constituyen como elementos estratégicos para garantizar la continuidad operativa, la calidad en la prestación de los servicios y el cumplimiento del marco normativo vigente. En particular, las instituciones prestadoras de servicios de salud mental enfrentan riesgos elevados asociados al tratamiento de información altamente sensible, cuya exposición, alteración o indisponibilidad puede generar impactos legales, operativos, reputacionales y sociales significativos.

El Hospital Mental de Antioquia, en cumplimiento de su misión institucional y de su responsabilidad como entidad pública del sector salud, reconoce la necesidad de gestionar de manera sistemática y preventiva los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de pacientes, colaboradores, proveedores y demás partes interesadas.

El presente Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se formula como resultado del proceso de identificación, análisis y evaluación de riesgos de seguridad de la información de la entidad, y constituye el instrumento mediante el cual se definen las acciones, controles y medidas orientadas a tratar los riesgos residuales identificados, manteniéndolos dentro de los niveles de riesgo aceptables para la organización.

Este plan se encuentra alineado con el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones, el Modelo Integrado de Planeación y Gestión – MIPG, la Política Nacional de Seguridad Digital y las mejores prácticas internacionales en gestión de la seguridad de la información. Asimismo, integra enfoques técnicos, administrativos y humanos, reconociendo que la gestión efectiva del riesgo requiere no solo de soluciones tecnológicas, sino también de procesos claros y una cultura organizacional orientada a la protección de la información.

A través de la implementación de este plan, el Hospital Mental de Antioquia busca fortalecer su Sistema de Gestión de Seguridad de la Información, asegurar la protección de los activos de información durante todo su ciclo de vida y garantizar un entorno digital confiable que respalde la prestación segura, oportuna y continua de los servicios de salud mental.

2. JUSTIFICACIÓN

La implementación de un Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en el Hospital Mental de Antioquia se justifica en la

naturaleza crítica y sensible de la información que gestiona la entidad, así como en los riesgos inherentes a los procesos asistenciales, administrativos y tecnológicos propios del sector salud mental.

La información relacionada con la salud mental de los pacientes es considerada dato sensible conforme a la Ley 1581 de 2012, dado que su uso indebido, divulgación no autorizada o pérdida puede generar afectaciones graves a la intimidad, dignidad, bienestar psicosocial y derechos fundamentales de los titulares de la información. En este contexto, la gestión inadecuada de los riesgos de seguridad y privacidad no solo expone a la institución a sanciones legales y disciplinarias, sino que también compromete la confianza de los pacientes, sus familias y los entes de control.

Adicionalmente, el marco normativo colombiano establece obligaciones específicas para las entidades del sector salud en relación con la protección, custodia, confidencialidad, disponibilidad e integridad de la información clínica, particularmente en lo referente a la historia clínica y a su progresiva digitalización. Normas como la Ley 2015 de 2020, la Resolución 1995 de 1999 y la Resolución 839 de 2017 exigen la implementación de controles que garanticen el manejo seguro de la información en entornos físicos y digitales.

El crecimiento de las amenazas cibernéticas dirigidas al sector salud, tales como ataques de ransomware, accesos no autorizados, pérdida de información y fallas en la disponibilidad de los sistemas, incrementa de manera significativa el nivel de exposición al riesgo. Estas amenazas se ven potenciadas por los procesos de transformación digital, la adopción de servicios en la nube, la interoperabilidad de sistemas y el uso de herramientas de telemedicina, los cuales amplían la superficie de ataque y requieren controles de seguridad acordes con estos nuevos escenarios.

Desde una perspectiva operativa, la indisponibilidad o alteración de la información clínica puede afectar directamente la continuidad de la atención en salud mental, poniendo en riesgo la seguridad del paciente y la toma de decisiones clínicas oportunas. Por ello, la gestión de los riesgos de seguridad de la información se convierte en un componente esencial para garantizar la continuidad del servicio y la estabilidad institucional.

Finalmente, este plan permite al Hospital Mental de Antioquia adoptar un enfoque preventivo y estructurado para el tratamiento de los riesgos de seguridad y privacidad de la información, optimizando el uso de los recursos tecnológicos, humanos y financieros, fortaleciendo la cultura de seguridad organizacional y asegurando el cumplimiento de los lineamientos del MSPI, el MIPG y las políticas nacionales de seguridad digital.

3. OBJETIVO

Implementar y mantener un Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en el Hospital Mental de Antioquia, orientado a la identificación, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando que los riesgos residuales se mantengan dentro de los niveles de riesgo aceptables definidos por la entidad, en cumplimiento del marco normativo vigente, el Modelo de Seguridad y Privacidad de la Información – MSPI y las mejores prácticas en seguridad de la información aplicables al sector salud.

Objetivos Específicos:

- **Sobre Riesgos y Nube:** Identificar, evaluar y tratar los riesgos de seguridad asociados tanto a la infraestructura local como a los nuevos servicios en la nube (**Microsoft Azure y Office 365**), asegurando que la migración tecnológica no comprometa la privacidad del paciente.
- **Sobre Ciberseguridad Activa:** Fortalecer la seguridad perimetral y de punto final mediante la implementación de controles avanzados (**FortiGate y EDR**), enfocados en la detección temprana y bloqueo de amenazas tipo *Ransomware*.
- **Sobre Cultura:** Desarrollar un programa de cultura de seguridad digital que concientice al personal sobre las técnicas de ingeniería social (*Phishing*), reduciendo el riesgo de incidentes causados por factor humano.
- **Sobre Continuidad:** Establecer y probar planes de respuesta a incidentes y recuperación de desastres que garanticen la disponibilidad de la Historia Clínica Electrónica ante fallos críticos o ciberataques.

4. MARCO NORMATIVO

El presente Plan de Tratamiento de Riesgos se fundamenta en el siguiente marco normativo:

NORMA	CONTENIDO
Ley 1581 de 2012	Ley Estatutaria de Protección de Datos Personales, que establece los principios y disposiciones generales para el tratamiento de datos personales.
Decreto 1377 de 2013	Reglamenta la Ley 1581 de 2012, especificando los requisitos para el tratamiento de datos personales y las

	obligaciones de los responsables y encargados.
Ley 527 de 1999	Define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales.
Ley 2015 de 2020	Regula la Historia Clínica Electrónica Interoperable (HCEI) y establece los requisitos para su implementación.
Resolución 1995 de 1999	Establece normas para el manejo de la Historia Clínica.
Resolución 839 de 2017	Define el manejo, custodia, tiempo de retención y conservación de las historias clínicas.
Ley 1438 de 2011	Reforma el Sistema General de Seguridad Social en Salud, incluyendo disposiciones sobre el manejo de información en salud.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 2106 de 2019	Normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios en la administración pública.
MSPI	Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC
Ley 1616 de 2013	Ley de Salud Mental, que incluye disposiciones sobre la confidencialidad y manejo de información de pacientes con trastornos mentales.
Resolución 2417 de 2022	Por la cual se actualizan los lineamientos de la Política de Salud Mental.

5. DEFINICIONES

- **Activo de Información**: Todo elemento que contiene, procesa, almacena o transmite información de valor para el Hospital Mental de Antioquia. Incluye bases de datos, archivos, sistemas, historias clínicas y documentación institucional.

- **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño a los sistemas de información o a la institución. Pueden ser internas o externas, naturales o provocadas.

- **Confidencialidad:** Propiedad que garantiza que la información sea accesible únicamente por personal autorizado. En el contexto de salud mental, es especialmente crítica debido a la naturaleza sensible de los datos clínicos.

- **Control:** Medida que modifica o gestiona un riesgo específico. Incluye políticas, procedimientos, directrices, prácticas o estructuras organizativas diseñadas para mantener la seguridad de la información.

- **Datos Sensibles:** Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación. En el contexto hospitalario, incluye diagnósticos, tratamientos y toda información relacionada con la salud mental.

- **Disponibilidad:** Propiedad que garantiza que la información sea accesible y utilizable cuando se requiera por personal autorizado. Es crucial para la continuidad en la prestación de servicios de salud.

- **Historia Clínica Electrónica:** Registro sistemático de las condiciones de salud del paciente, en formato digital, que incluye datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica.

- **Incidente de Seguridad:** Evento único o serie de eventos inesperados que comprometen la seguridad de la información y tienen una probabilidad significativa de comprometer las operaciones del hospital.

- **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información y los métodos de procesamiento. Garantiza que los datos no han sido alterados de manera no autorizada.

- **Privacidad:** Derecho que tienen los individuos de determinar cuándo, cómo y qué información sobre ellos puede ser compartida con otros.

- **Riesgo:** Posibilidad de que una amenaza específica explote una vulnerabilidad de un activo o grupo de activos de información, causando daño a la organización.

- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información, manteniendo la confidencialidad, disponibilidad e integridad de la misma.

- **Tratamiento de Riesgos:** Proceso de selección e implementación de medidas para modificar el nivel de riesgo, incluyendo evitar, reducir, transferir o aceptar el riesgo.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. Puede ser de naturaleza técnica, procedural o humana.

- **Plan de Continuidad:** Conjunto de procedimientos documentados que guían a la organización para responder, recuperar, reanudar y restaurar sus operaciones a un nivel predefinido después de una interrupción.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Marco de políticas y procedimientos que incluyen todos los controles técnicos y legales necesarios para gestionar y proteger los activos de información de una organización.

- **Telemedicina:** Provisión de servicios de salud a distancia utilizando tecnologías de la información y comunicación. Requiere medidas específicas de seguridad para proteger la confidencialidad de las consultas virtuales.

- **Usuario:** Persona o entidad que utiliza los sistemas de información del hospital, incluyendo personal médico, administrativo, pacientes y proveedores externos.

6. METODOLOGIA Y RECURSOS FISICOS, HUMANOS Y ECONOMICOS

METODOLOGÍA DE IMPLEMENTACIÓN

La implementación del Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital Mental de Antioquia se desarrolla bajo un enfoque de gestión integral del riesgo, alineado con el Modelo de Seguridad y Privacidad de la Información – MSPI, el Modelo Integrado de Planeación y Gestión – MIPG, y las buenas prácticas establecidas en la norma ISO/IEC 27005.

La metodología adoptada se fundamenta en el ciclo PHVA (Planear – Hacer – Verificar – Actuar), lo cual permite garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) y la efectividad de los controles implementados.

Fase 1: Enfoque de Gestión del Riesgo

La gestión de los riesgos de seguridad y privacidad de la información se realiza mediante un proceso sistemático que comprende las siguientes etapas:

- Identificación de activos de información
- Identificación de amenazas y vulnerabilidades
- Análisis y evaluación del riesgo
- Definición del tratamiento del riesgo
- Implementación de controles
- Seguimiento y mejora continua

Este enfoque permite asegurar que los riesgos asociados a los activos de información se mantengan dentro de los niveles de riesgo aceptables definidos por la entidad.

Fase 2: Criterios de Análisis y Evaluación del Riesgo

Se identifican y clasifican los activos de información del hospital, considerando su criticidad y su relación con los procesos misionales, estratégicos y de apoyo, incluyendo, entre otros:

- Historias clínicas físicas y electrónicas
- Sistemas de información asistenciales y administrativos
- Infraestructura tecnológica (servidores, red, equipos de seguridad)
- Información almacenada en servicios en la nube
- Recurso humano y conocimiento institucional

Fase 3: Identificación de Amenazas y Vulnerabilidades

Para cada activo de información se identifican:

- **Amenazas internas y externas** (ciberataques, errores humanos, fallas tecnológicas, eventos naturales, accesos no autorizados, entre otros).
- **Vulnerabilidades técnicas, procedimentales y humanas** que puedan ser explotadas por dichas amenazas.

Fase 4: Análisis del Riesgo

El análisis del riesgo se realiza evaluando:

- **Impacto**: Consecuencia que tendría la materialización del riesgo sobre la confidencialidad, integridad y disponibilidad de la información, así como sobre la atención al paciente, la continuidad del servicio y el cumplimiento normativo.
- **Probabilidad**: Posibilidad de ocurrencia del evento de riesgo, considerando el historial de incidentes, la exposición del activo y la efectividad de los controles existentes.

Cada riesgo se valora utilizando una escala cualitativa:

Nivel	Impacto / Probabilidad
Alto	Afectación grave a la operación, pacientes o cumplimiento normativo
Medio	Afectación moderada y controlable
Bajo	Afectación menor o limitada

Fase 5: Evaluación y Aceptación del Riesgo

Con base en el análisis de impacto y probabilidad, se determina el nivel de riesgo inherente y el riesgo residual, una vez considerados los controles existentes.
La entidad define criterios de aceptación del riesgo, los cuales permiten:

- Priorizar los riesgos críticos
- Definir los riesgos que requieren tratamiento inmediato
- Identificar los riesgos que pueden ser aceptados de manera justificada

Fase 6: Tratamiento del Riesgo

Para cada riesgo identificado se define una estrategia de tratamiento, de acuerdo con los siguientes enfoques:

- Reducir: Implementar o fortalecer controles para disminuir el impacto o la probabilidad del riesgo.
- Evitar: Eliminar la actividad que origina el riesgo.
- Transferir: Compartir el riesgo con terceros (seguros, contratos, proveedores).
- Aceptar: Asumir el riesgo cuando se encuentra dentro de los niveles aceptables definidos por la entidad.

Las acciones de tratamiento se documentan en el Plan de Tratamiento de Riesgos, especificando el riesgo asociado, los controles a implementar, los responsables, los recursos requeridos y los plazos de ejecución.

Fase 7: Implementación de Controles

Los controles definidos se implementan de manera progresiva y priorizada, considerando:

- Controles técnicos (firewalls, antivirus, respaldos, controles de acceso, cifrado, monitoreo)
- Controles administrativos (políticas, procedimientos, contratos, acuerdos de confidencialidad)
- Controles humanos (capacitación, sensibilización, responsabilidades)

La implementación se articula con los proyectos tecnológicos institucionales, tales como la adopción de servicios en la nube, la migración de correo electrónico y el fortalecimiento de la infraestructura de seguridad perimetral.

Fase 8: Seguimiento, Monitoreo y Mejora Continua

El seguimiento del plan se realiza mediante:

- Indicadores de ejecución y efectividad de los controles
- Monitoreo de incidentes de seguridad de la información
- Auditorías internas y revisiones periódicas
- Reportes al Comité de Gestión y Desempeño

Con base en los resultados del seguimiento, se realizan los ajustes necesarios para mejorar la efectividad de los controles y actualizar el perfil de riesgo institucional.

Fase 9: Roles y Responsabilidades

La implementación del plan involucra a las diferentes áreas de la entidad, bajo el liderazgo del área de gestión de las tic's, con el acompañamiento de Planeación, Control Interno y los líderes de proceso, garantizando una gestión transversal y articulada de la seguridad y privacidad de la información.

RECURSOS FÍSICOS Y TECNOLÓGICOS

- Equipo de seguridad perimetral (FortiGate), destinado al control del tráfico de red, prevención de intrusiones, segmentación de red y mitigación de amenazas externas.
- Plataforma de correo y colaboración en la nube Office 365.
- Plataforma de protección de endpoints (WithSecure Premium Endpoint) para la detección y respuesta ante malware, ransomware y amenazas avanzadas.
- Sistemas de control de acceso lógico a los sistemas de información, orientados a la gestión de usuarios, perfiles y privilegios.
- Sistemas de copia de seguridad en la nube (Azure).
- Herramientas de monitoreo y registro de eventos (logs) para la detección temprana de incidentes de seguridad.
- Control de acceso al medio.

Infraestructura de Tecnologías de la Información

- Servidor principal de dominio, encargado de la autenticación, autorización y gestión centralizada de usuarios.
- Infraestructura de red institucional, incluyendo equipos de comunicación y ampliación del alcance del servicio DHCP para garantizar disponibilidad y control de acceso.
- Centro de datos institucional, con capacidades de operación y respaldo de la información crítica.

Infraestructura en la Nube (Cloud Computing)

- Servicios de Microsoft Azure, utilizados para almacenamiento seguro, copias de respaldo y recuperación de información.
- Plataforma Microsoft Office 365, destinada a servicios de correo electrónico, colaboración y productividad, con controles de seguridad integrados.

- Esquema de respaldo híbrido (local y nube) que garantiza la disponibilidad y recuperación de la información ante incidentes.

RECURSOS HUMANOS

La gestión efectiva de la seguridad y privacidad de la información requiere la participación articulada de diferentes roles institucionales, bajo un enfoque de responsabilidad compartida.

Roles Clave

- Profesional universitario encargado de la gestión de las Tic's, responsable de coordinar la implementación técnica y operativa del plan.
- Área de Planeación, encargada del seguimiento, monitoreo y evaluación del cumplimiento del plan.
- Oficina de Control Interno, responsable de la verificación independiente y la evaluación de la efectividad de los controles.
- Líderes de proceso, responsables de la identificación de riesgos y del cumplimiento de los controles en sus respectivas áreas.
- Servidores públicos y contratistas, responsables del uso adecuado de la información y del cumplimiento de las políticas de seguridad.
- Proveedores y terceros, sujetos a acuerdos de confidencialidad y cláusulas de seguridad de la información.

Capacitación y Sensibilización

- Programas periódicos de capacitación en seguridad y privacidad de la información.
- Jornadas de sensibilización sobre el manejo de datos sensibles y la responsabilidad disciplinaria.
- Socialización de políticas, procedimientos y buenas prácticas en seguridad digital.

RECURSOS ECONÓMICOS

El hospital asigna recursos financieros para la ejecución del plan, priorizando las inversiones que contribuyen a la reducción de los riesgos críticos de seguridad y privacidad de la información.

Inversiones Prioritarias

- Renta y mantenimiento del equipo de seguridad perimetral (FortiGate).
- Renovación de licencias de protección de endpoints.

- Renovación y fortalecimiento del parque computacional (renovación tecnológica).
- Mantenimiento de servicios de almacenamiento y respaldo en la nube.
- Operación continua de la plataforma de correo institucional en Office 365.
- Adquisición de herramientas y servicios asociados a la gestión de la seguridad de la información.

Optimización de Recursos

La asignación de los recursos económicos se realiza bajo criterios de:

- Prioridad del riesgo a tratar
- Costo–beneficio de los controles implementados
- Sostenibilidad financiera
- Optimización del gasto público

7. ACTIVIDADES (CRONOGRAMA)

ACTIVIDAD N°	ACTIVIDADES/ ACCIONES A DESARROLLAR	PRODUCTO O EVIDENCIA	AREA RESPONSABLE	FECHA DE ENTREGA											
				Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.	Acceso no autorizado a la red institucional y a los sistemas de información	Configuración de control de acceso en servidor DHCP	Gestión de las tic's	x											
2.	Implementación de esquema de respaldos híbridos	Reportes de respaldo y pruebas de restauración	Gestión de las tic's			X						x			
3.	Servidor de dominio actualizado	Evidencia del Windows update	Gestión de las tic's	x	x	x	x	x	x	x	x	x	x	x	x
4.	Pérdida de control sobre el correo institucional	Tenant azure activo	Gestión de las tic's				X					x			
5.	Pérdida de información por fallas locales	Tenant Azure configurado	Gestión de las tic's	x	x	x	x	x	x	x	x	x	x	x	x
6.	Desconocimiento del personal sobre manejo seguro de información	Capacitación en ciberseguridad	Gestión de las tic's			x							x		

7.	Incumplimiento normativo en protección de datos	Políticas institucionales actualizadas	Gestión de las tic's	x						x					
8.	Falta de seguimiento al estado de los riesgos	Indicadores y reportes de seguimiento	Gestión de las tic's						x						x

8. DIFUSIÓN

Mecanismo de elaboración	La metodología utilizada para la realización fue basada con la normatividad vigente, adaptándola a la E.S.E. Hospital Mental de Antioquia María Upegui – HOMO.
Mecanismo de difusión	El Plan será dado a conocer a los líderes involucrados, estos a su a vez lo darán a conocer a sus colaboradores; posteriormente se montará en la página web institucional para la consulta del público en general.
Mecanismos de capacitación	Se socializara de forma verbal por parte del líder o responsable de ejecución del plan con su equipo de trabajo y las partes interesadas.
Mecanismos de evaluación	Será evaluado y monitoreado por medio de un seguimiento según el cronograma de ejecución de cada actividad, y será la oficina de Planeación quien lo realice.
Mecanismos de retroalimentación	Se hará un acompañamiento constante a las áreas que intervengan en cada plan, para que las mismas entreguen oportunamente y con claridad el desarrollo de las actividades programadas.

9. SEGUIMIENTO

Desde el área de planeación se realiza seguimiento de forma mensual y se lleva indicador de resultado de forma trimestral en el comité de gestión y desempeño.

Indicador de seguimiento: Proporción de ejecución del Plan de tratamiento de riesgos de seguridad y privacidad de la información

Número de actividades ejecutadas en el período / Número de actividades programadas en el plan durante el periodo

RANGO		
0 – 60%	Rojo	Baja
61 – 89%	Amarillo	Media
90 – 100%	Verde	Alta

10. NOMBRES DE RESPONSABLE DE DILIGENCIAMIENTO Y EJECUCIÓN DEL PLAN

Nombre	Cargo
Mauricio Pulgarín	Profesional universitario encargado de gestión de las tic's

11. CONTROL DE CAMBIOS

ELABORÓ	Mauricio Pulgarin – Ingeniero de telecomunicaciones
ACTUALIZÓ	Mauricio Pulgarin – Ingeniero de telecomunicaciones
APROBÓ	Comité de Gestión y Desempeño
VERSIÓN	03
MOTIVO DE ACTUALIZACIÓN	Se actualiza el plan para fortalecer el enfoque de gestión del riesgo de seguridad y privacidad de la información, alinearlo con el MSPI y el MIPG, y ajustar el cronograma de actividades para el período de ejecución.
FECHA DE ACTUALIZACIÓN	15/01/2026