PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

1. INTRODUCCIÓN

En el contexto actual, la seguridad y privacidad de la información en el sector salud se han convertido en factores críticos para garantizar la continuidad de la prestación de servicios, el cumplimiento normativo y la confianza de los pacientes. El Hospital Mental de Antioquia, como institución comprometida con la protección de los datos de sus pacientes, colaboradores y demás actores involucrados, reconoce la importancia de gestionar de manera efectiva los riesgos asociados a la seguridad de la información.

Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información surge como respuesta a la necesidad de fortalecer las medidas de protección de los activos de información de la institución. Para su desarrollo, se han considerado tanto factores internos, como la infraestructura tecnológica, los procesos operativos y la cultura organizacional, como factores externos, incluyendo el marco normativo vigente, las amenazas cibernéticas en constante evolución y los estándares internacionales en seguridad de la información.

El objetivo de este plan es establecer estrategias y controles específicos para mitigar los riesgos identificados en la evaluación de seguridad y privacidad de la información, asegurando la integridad, confidencialidad y disponibilidad de los datos. A través de este documento, se presentan las acciones a implementar, los responsables de su ejecución y los indicadores que permitirán evaluar la efectividad de las medidas adoptadas.

Con este esfuerzo, el Hospital Mental de Antioquia reafirma su compromiso con la seguridad de la información, el cumplimiento de la normativa colombiana y las mejores prácticas internacionales, garantizando así un entorno digital seguro y confiable para todos sus usuarios.

2. JUSTIFICACIÓN

El sector salud enfrenta desafíos únicos en materia de seguridad y privacidad de la información, particularmente cuando se trata de instituciones especializadas en salud mental. El Hospital Mental de Antioquia, como entidad prestadora de servicios de salud mental, maneja información altamente sensible que requiere niveles excepcionales de protección, considerando tanto la naturaleza confidencial de los diagnósticos y tratamientos psiquiátricos, como la especial vulnerabilidad de su población atendida.

La implementación de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se justifica por múltiples factores críticos:

Protección de Datos Sensibles La información de salud mental es considerada como datos sensibles según la Ley 1581 de 2012 de Protección de Datos Personales. El manejo inadecuado de esta información no solo puede resultar en sanciones legales, sino que también puede causar daños significativos a los pacientes, afectando su dignidad, privacidad y bienestar psicosocial.

Cumplimiento Normativo El marco regulatorio colombiano, incluyendo la Ley 2015 de 2020 sobre Historia Clínica Electrónica y la Resolución 1995 de 1999 sobre manejo de historias clínicas, establece requisitos específicos para la gestión segura de la información en salud. Este plan permite alinear las operaciones del hospital con estas exigencias normativas.
Amenazas Cibernéticas Emergentes El incremento de ciberataques dirigidos específicamente al sector salud, incluyendo ransomware y robo de datos médicos, hace imperativo contar con estrategias robustas de protección. Los hospitales se han convertido en objetivos prioritarios para los ciberdelincuentes debido al valor de la información que manejan.
Transformación Digital La creciente digitalización de los servicios de salud, acelerada por la pandemia de COVID-19, ha ampliado la superficie de exposición a riesgos informáticos. La adopción de telemedicina y sistemas electrónicos de gestión clínica requiere medidas de seguridad acordes con estos nuevos escenarios tecnológicos.
Continuidad Operativa La disponibilidad ininterrumpida de la información clínica es crucial para la prestación de servicios de salud mental. Un incidente de seguridad que comprometa el acceso a historias clínicas o información de tratamientos podría poner en riesgo la vida de los pacientes.
Reputación Institucional Como institución líder en salud mental, el Hospital Mental de Antioquia debe mantener la confianza de pacientes, familias y entidades reguladoras. Un compromiso demostrable con la seguridad de la información fortalece esta confianza y posiciona al hospital como referente en buenas prácticas de gestión.
Gestión Eficiente de Recursos La implementación planificada de controles de seguridad permite optimizar la inversión en tecnología y recursos humanos, previniendo gastos mayores asociados a incidentes de seguridad o sanciones por incumplimiento normativo.

3. OBJETIVO

Implementar un sistema integral de gestión de riesgos de seguridad y privacidad de la información en el Hospital Mental de Antioquia, que garantice la protección efectiva de los datos sensibles de pacientes y la información institucional, asegurando su confidencialidad, integridad y disponibilidad, en cumplimiento con el marco normativo vigente y las mejores prácticas internacionales en ciberseguridad del sector salud.

Objetivos Específicos:

1. Establecer controles técnicos y administrativos que permitan identificar, evaluar y mitigar los riesgos de seguridad y privacidad de la información en

todos los procesos críticos del hospital, con especial énfasis en la protección de historias clínicas y datos sensibles de salud mental.
2. Desarrollar e implementar protocolos de respuesta a incidentes de seguridad que permitan una actuación oportuna y eficaz ante amenazas potenciales, minimizando el impacto sobre la operación del hospital y la atención a pacientes.
3. Fortalecer la cultura de seguridad de la información en el personal del hospital mediante programas de capacitación y sensibilización, promoviendo prácticas seguras en el manejo de información sensible.
4. Garantizar el cumplimiento de los requisitos normativos en materia de protección de datos personales y seguridad de la información en salud, mediante la implementación de controles alineados con la legislación colombiana vigente.
5. Optimizar la gestión de activos de información mediante la implementación de herramientas y procedimientos que aseguren su adecuada clasificación, almacenamiento y protección durante todo su ciclo de vida.
6. Establecer métricas e indicadores de desempeño que permitan evaluar la efectividad de los controles implementados y el nivel de madurez del sistema de gestión de riesgos de seguridad de la información.
7. Integrar los controles de seguridad y privacidad de la información con los procesos de transformación digital del hospital, asegurando que las nuevas tecnologías y servicios implementados cumplan con los estándares de seguridad requeridos.

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.
NTC 5254	Gestión del Riesgo

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 de Tratamiento de Riesgos seguirá un enfoque sistemático basado en el ciclo PHVA (Planear, Hacer, Verificar, Actuar) y se desarrollará en las siguientes fases:

Fase 1: Diagnóstico y Planificación

- Evaluación inicial de la infraestructura existente
- Identificación de activos críticos de información

- Análisis de brechas de seguridad
- Definición de cronograma de implementación

Fase 2: Implementación de Controles

- Despliegue de soluciones tecnológicas
- Configuración de sistemas de seguridad
- Desarrollo de políticas y procedimientos
- Capacitación del personal

Fase 3: Monitoreo y Evaluación

- Seguimiento de indicadores de seguridad
- Auditorías periódicas
- Evaluación de efectividad de controles
- Ajustes y mejoras continuas

RECURSOS FÍSICOS

Infraestructura de Seguridad:

- Equipo FortiGate para ciberseguridad (nuevo contrato de renta)
- Servidor principal de dominio (renovación)
- Infraestructura de red para ampliación del scope DHCP
- Centro de datos principal y respaldo

Infraestructura Cloud:

- Servicios de Microsoft Azure para almacenamiento en la nube
- Plataforma Office 365 para servicios de correo y colaboración
- Sistemas de respaldo híbrido (local y nube)

RECURSOS ECONÓMICOS

- Inversiones Prioritarias 2025:
- Renta de equipo FortiGate para ciberseguridad (actualmente)
- Renovación de licencias WithSecure Premium Endpoint (2Q-2025)
- Renovación del servidor principal de dominio
- Implementación de ampliación DHCP
- Migración de correos a Office 365
- Plan de almacenamiento en Microsoft Azure
- CRONOGRAMA DE IMPLEMENTACIÓN
- Q1 2025:
- Implementación de FortiGate
- Renovación de licencias WithSecure
- Inicio de migración a Office 365
- Capacitación inicial del personal
- Q2 2025:

- Renovación del servidor de dominio
- Ampliación del scope DHCP
- Configuración de servicios Azure
- Desarrollo de políticas y procedimientos cloud
- Q3 2025:
- Finalización de migración a Office 365
- Optimización de servicios cloud
- Evaluación de efectividad de controles
- Capacitación en herramientas cloud
- Q4 2025:
- Auditoría general de seguridad incluyendo entorno cloud
- Planificación para el siguiente año
- Actualización de documentación
- Evaluación de rendimiento de servicios cloud
- BENEFICIOS ESPERADOS DE LA MIGRACIÓN CLOUD
- Mayor seguridad en el manejo de correos electrónicos
- Respaldo automático de información crítica
- Acceso seguro desde cualquier ubicación
- Mejora en la colaboración entre equipos
- Reducción de costos de mantenimiento de infraestructura local
- Escalabilidad según las necesidades institucionales

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.	Implementación de FortiGate	Dispositivo de ciberseguridad funcionando en la red corporativa	Sistemas		X										
2.	Inicio de migración a Office 365	Correos en el tenant de Microsoft office 365, funcionando	Sistemas			X									
3.	Configuración de servicios Azure	Tenant de copia de seguridad de Microsoft azure listo	Sistemas		X										
4.	Ampliación del scope DHCP Renovación del	Actividades ejecutadas sobre la red	Red empresarial con nuevo servidor				X								

	servidor de dominio Inicio de migración a Office 365	empresarial	de dominio y capacidad para mas de 1.000 dispositivos en la red (DHCP)												

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:

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	Ingeniero de Telecomunicaciones (TI)

11. CONTROL DE CAMBIOS

ELABORÓ	Sergio León Ramírez – Subgerente Administrativo y Financiero; Mauricio Pulgarin – Ingeniero de telecomunicaciones
ACTUALIZÓ	Sergio León Ramírez – Subgerente Administrativo y Financiero; Mauricio Pulgarin – Ingeniero de telecomunicaciones
APROBÓ	Comité de Gestión y Desempeño
VERSIÓN	02
MOTIVO DE ACTUALIZACIÓN	Se actualiza el cronograma para el presente período de vigencia y ejecución.
FECHA DE ACTUALIZACIÓN	28/01/2025