PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD y PRIVACIDAD DE LA INFORMACION

2026 – 2028

Revisado: Subgerente Administrativo y Financiero.	Firma:	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

INTRODUCCION

La gestión de los riesgos digitales constituye un componente esencial para garantizar la continuidad de la prestación de los servicios de salud y la protección de la información institucional. La E.S.E. Hospital San Jerónimo de Montería adopta el presente Plan de Tratamiento de Riesgos Digitales como instrumento operativo para controlar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

El plan se desarrolla bajo los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI y las buenas prácticas de gestión de riesgos definidas por el Estado Colombiano, integrándose al Sistema de Control Interno, al Plan Estratégico de Tecnologías de la Información – PETI y al Plan de Seguridad y Privacidad de la Información institucional.

Su enfoque es preventivo y continuo, orientado a identificar riesgos reales asociados a la operación tecnológica, implementar controles, realizar seguimiento periódico y establecer acciones de mejora, garantizando la protección de los sistemas de información clínicos y administrativos de la entidad.

1. OBJETIVO

Establecer las acciones necesarias para tratar los riesgos digitales que puedan afectar la operación tecnológica de la E.S.E. Hospital San Jerónimo de Montería, mediante la implementación de controles técnicos, administrativos y físicos que reduzcan la probabilidad de incidentes de seguridad de la información y garanticen la continuidad de los servicios institucionales.

El plan orienta la ejecución de actividades concretas para proteger los sistemas de información clínicos y administrativos, priorizando los riesgos asociados al acceso no autorizado, pérdida de información, indisponibilidad de los sistemas y fuga de datos personales, en concordancia con el Modelo de Seguridad y Privacidad de la Información – MSPI y la normatividad vigente.

2. ALCANCE

El presente Plan de Tratamiento de Riesgos Digitales aplica a todos los activos tecnológicos y de información de la E.S.E. Hospital San Jerónimo de Montería que soportan los procesos misionales, estratégicos y de apoyo.

Incluye:

- Sistemas de Información en Salud (HIS) y aplicativos administrativos.
- Servidores institucionales y bases de datos locales.
- Infraestructura de red, firewall y conectividad.
- Equipos de cómputo y dispositivos de almacenamiento.
- Copias de seguridad y mecanismos de recuperación.
- Información digital clínica y administrativa.
- Usuarios internos, contratistas y terceros con acceso a los sistemas.

El plan cubre riesgos derivados de fallas técnicas, errores humanos, accesos no autorizados, software malicioso, interrupciones eléctricas y cualquier evento que pueda afectar la disponibilidad, integridad o confidencialidad de la información institucional.

3. METODOLOGIA

La E.S.E. Hospital San Jerónimo de Montería gestionará los riesgos digitales mediante un ciclo operativo continúo basado en identificación, control y seguimiento, alineado con el Modelo de Seguridad y Privacidad de la Información – MSPI.

La metodología se ejecutará a través de actividades periódicas definidas, con responsables y evidencias verificables.

3.1 Identificación de activos críticos

Semestralmente el área de Tecnologías de la Información actualizará el inventario de activos tecnológicos e información institucional, identificando:
Servidores locales
Sistemas de información clínicos y administrativos
Bases de datos
Equipos de usuario
Equipos de red
Copias de seguridad

- Evidencia: Inventario actualizado de activos.

3.2. Identificación de riesgos

Con base en los activos identificados, el área TIC identificará eventos que puedan afectar la operación, tales como:
Accesos no autorizados
Fallas de hardware
Ataques informáticos
Eliminación accidental de información
Indisponibilidad de servicios
Fuga de información

- Evidencia: Matriz de riesgos actualizada

3.3. Valoración del riesgo
Cada riesgo será evaluado según:
Probabilidad de ocurrencia
Impacto en la operación del servicio
El resultado permitirá priorizar los riesgos a tratar durante la vigencia.

- Evidencia: Clasificación Alto – Medio – Bajo en matriz

3.4. Implementación de controles

Se aplicarán controles según el tipo de riesgo:
Controles técnicos
Antivirus corporativo
Configuración de firewall
Bloqueo de usuarios
Restricción de dispositivos externos
Controles administrativos
Políticas de seguridad
Acuerdos de confidencialidad
Capacitación de usuarios

Controles operativos
Pruebas de restauración de backups

Auditoría de cuentas
Seguimiento de accesos

- Evidencia: Registros, reportes, actas

3.5. Seguimiento y verificación
Trimestralmente se revisará:
Cumplimiento de controles
Incidentes presentados
Efectividad del tratamiento
Se documentará en informe de seguridad de la información.

- Evidencia: Informe trimestral TIC

3.6. Mejora continua
Los riesgos y controles serán actualizados:
Cuando ocurra un incidente
Cuando cambie la infraestructura
En revisión anual del plan

- Evidencia: Nueva versión matriz de riesgos.

4. IDENTIFICACION Y VALORIZACION DEL RIESGO

Escala utilizada	
Probabilidad	**Valor**
Baja	1
Media	2
Alta	3
Impacto	**Valor**
Bajo	1
Medio	2
Alto	3

Nivel de riesgo = Probabilidad × Impacto	
Resultado	**Nivel**
1–2	Bajo
3–4	Medio
6–9	Alto

Revisado: Subgerente Administrativo y Financiero	Firma: E.S.E Hospital San Jerónimo SUBGERENTE ADMINISTRATIVO Y FINANCIERO	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

Matriz de riesgos institucional

Código	Activo	Riesgo	Causa	Prob.	Impacto	Nivel	Prioridad
RD-01	Servidor HIS	Acceso no autorizado	Contraseñas débiles	2	3	6	Alto
RD-02	Base de datos clínica	Ransomware	Descargas maliciosas	2	3	6	Alto
RD-03	Servidor	Falla eléctrica	Daño UPS o corte prolongado	1	3	3	Medio
RD-04	Red institucional	Intrusión externa	Puertos expuestos	2	3	6	Alto
RD-05	Información clínica	Fuga de información	Error humano	2	3	6	Alto
RD-06	Sistemas administrativos	Eliminación accidental	Manipulación indebida	2	2	4	Medio
RD-07	Backups	Pérdida de respaldo	Almacenamiento incorrecto	1	3	3	Medio
RD-08	Equipos usuario	Malware	Uso de USB	2	2	4	Medio
RD-09	Archivo clínico físico	Acceso indebido	Control insuficiente	1	3	3	Medio
RD-10	Plataforma institucional	Caída del sistema	Sobrecarga o fallo	1	3	3	Medio

Interpretación

Riesgos ALTOS → tratamiento inmediato
Riesgos MEDIOS → tratamiento programado
Riesgos BAJOS → monitoreo

Revisado: Subgerente Administrativo y Financiero	Firma: E.S.E Hospital San Jerónimo SUBGERENTE ADMINISTRATIVO Y FINANCIERO	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

5. PLAN DE TRATAMIENTO DE RIESGOS

Criterio de intervención:

Riesgos Altos ⟶ implementación inmediata (vigencia actual)
Riesgos Medios ⟶ implementación programada
Riesgos Bajos ⟶ monitoreo

Tabla de tratamiento

Código	Riesgo	Nivel	Acción de Control	Responsable	Frecuencia	Evidencia
RD-01	Acceso no autorizado al HIS	Alto	Política de contraseñas + bloqueo automático de usuario	TIC	Permanente	Configuración sistema
RD-02	Ransomware en base de datos	Alto	Antivirus corporativo actualizado + restricción USB	TIC	Diario	Reporte consola antivirus
RD-03	Falla eléctrica servidor	Medio	Revisión funcionamiento UPS	TIC	Semestral	Registro mantenimiento
RD-04	Intrusión externa	Alto	Revisión reglas firewall y cierre de puertos	TIC	Trimestral	Backup configuración
RD-05	Fuga de información clínica	Alto	Acuerdo confidencialidad y capacitación usuarios	Talento Humano / TIC	Anual	Actas firmadas

Revisado: Subgerente Administrativo y Financiero	Firma:	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

RD-06	Eliminación accidental	Medio	Restricción permisos por roles	TIC	Permanente	Listado usuarios
RD-07	Pérdida de backups	Medio	Copia externa offline semanal	TIC	Semanal	Registro backup
RD-08	Malware por USB	Medio	Bloqueo puertos USB	TIC	Permanente	Política aplicada
RD-09	Acceso indebido archivo físico	Medio	Control préstamo historias clínicas	Archivo Clínico	Diario	Registro préstamo
RD-10	Caída sistema	Medio	Prueba mensual restauración	TIC	Mensual	Formato restauración

Resultado esperado

Con la ejecución del plan:
Los riesgos altos quedan mitigados
Los medios controlados
Los bajos monitoreados

Indicador de cumplimiento del plan

Indicador	Fórmula	Meta
Riesgos altos tratados	Tratados / identificados	≥ 90%
Controles ejecutados	Ejecutados / planificados	≥ 85%
Incidentes críticos repetidos	Nº incidentes	0

6. SEGUIMIENTO Y EVALUACION DEL PLAN

La E.S.E. Hospital San Jerónimo de Montería realizará seguimiento periódico al cumplimiento del Plan de Tratamiento de Riesgos Digitales con el fin de verificar la efectividad de los controles implementados y asegurar la reducción de los riesgos identificados.

Revisado: Subgerente Administrativo y Financiero	Firma:	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

El seguimiento permitirá detectar desviaciones, establecer acciones correctivas y actualizar las medidas de seguridad conforme a los cambios tecnológicos o normativos.

6.1. Seguimiento operativo

El área de Tecnologías de la Información verificará el cumplimiento de las actividades definidas en el plan mediante revisión de evidencias y controles implementados.

Frecuencia: Trimestral

Se revisará:
Implementación de controles
Pruebas de restauración realizadas
Actualización de antivirus
Revisión de usuarios activos
Incidentes registrados

- Evidencia: Informe trimestral de seguridad digital

6.2. Evaluación institucional

La Oficina de Control Interno realizará evaluación del plan para verificar su cumplimiento y efectividad dentro del Sistema de Control Interno.

Frecuencia: Semestral

Se verificará:
Cumplimiento de actividades programadas
Evidencias documentales
Indicadores del plan
Acciones correctivas implementadas

- Evidencia: Informe de evaluación de Control Interno

6.3. Indicadores de evaluación

Indicador	Método de evaluación	Periodicidad
Cumplimiento del plan	% actividades ejecutadas	Trimestral
Efectividad controles	Nº incidentes presentados	Trimestral
Reducción del riesgo	Comparación matriz anual	Anual

6.4. Acciones de mejora

Cuando se identifique incumplimiento o nuevos riesgos se deberán

Revisado: Subgerente Administrativo y Financiero	Firma: SUBGERENTE ADMINISTRATIVO Y FINANCIERO	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

1. Definir acciones correctivas
2. Asignar responsable
3. Establecer fecha de ejecución
4. Actualizar la matriz de riesgos

- Evidencia: Registro de acciones de mejora

6.5. Actualización del plan

El plan será actualizado:

- Al cierre de cada vigencia
- Ante cambios tecnológicos
- Ante incidentes críticos
- Por requerimiento normativo.

7. CRONOGRAMA DE EJECUCION 2026- 2028

Vigencia 2026 – Implementación			
Actividad	**Responsable**	**Periodicidad**	**Evidencia**
Actualización inventario de activos	TIC	Semestral	Inventario actualizado
Actualización matriz de riesgos	TIC	Anual	Matriz firmada
Implementación política de contraseñas	TIC	Única vez	Configuración sistema
Restricción de dispositivos USB	TIC	Permanente	Política aplicada
Configuración y revisión firewall	TIC	Trimestral	Backup configuración
Pruebas de restauración de backups	TIC	Mensual	Formatos firmados
Capacitación en seguridad digital	TIC / Talento Humano	Anual	Actas
Firma acuerdos de confidencialidad	Talento Humano	Anual	Documentos firmados

Vigencia 2027 – Seguimiento y Control			
Actividad	**Responsable**	**Periodicidad**	**Evidencia**
Revisión de usuarios activos	TIC	Trimestral	Informe revisión
Auditoría interna de seguridad	Control Interno	Semestral	Informe auditoría
Evaluación de incidentes	TIC	Trimestral	Registro incidentes
Validación funcionamiento UPS	TIC	Semestral	Bitácora mantenimiento
Control préstamo historias clínicas	Archivo Clínico	Permanente	Registro préstamo
Copia externa de respaldos	TIC	Semanal	Registro backup

Revisado: Subgerente Administrativo y Financiero	Firma: E.S.E Hospital San Jerónimo SUBGERENTE ADMINISTRATIVO Y FINANCIERO	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

Vigencia 2028 – Evaluación y Mejora			
Actividad	**Responsable**	**Periodicidad**	**Evidencia**
Evaluación integral del plan	TIC	Anual	Informe final
Actualización matriz de riesgos	TIC	Anual	Matriz actualizada
Revisión políticas de seguridad	TIC	Anual	Documento actualizado
Informe institucional de cumplimiento	TIC / Gerencia	Anual	Informe firmado
Ajuste del plan siguiente vigencia	TIC	Única vez	Nueva versión plan

Año	Resultado esperado
2026	Implementación de controles básicos
2027	Control y seguimiento institucional
2028	Madurez operativa del plan

Revisado: Subgerente Administrativo y Financiero	Firma: E.S.E Hospital San Jerónimo SUBGERENTE ADMINISTRATIVO Y FINANCIERO	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026

CUADRO DE REVISIONES

Versión	*Elaboró*	*Revisó*	*Aprobó*
01	Profesional Universitario Sistemas de Información y comunicaciones	Planeación y Gestión de Calidad	Gerente
02	**ANGELICA MENCO CONTRERAS**	**DORIS SPATH PORTILLO**	**GUILLERMO HOYOS NADER**
	Profesional Universitario Tecnología Informática y Sistemas	Subgerencia Administrativa y Financiera	Gerente

CONTROL DE COPIAS

Versión	*Tipo de Copia*	*Área o Sección*	*Fecha Elaboración*	*Fecha Revisión*
01	Controlada	Tecnología de la Información y Comunicaciones	Abril 2023	Abril 2025
02	Controlada	Tecnología Informática y Sistemas	Febrero 2026	Febrero 2028

Versión	*Descripción del Cambio*
01	Elaboración del documento PLAN DE TRATAMIENTO DE RIESGOS DIGITALES
02	Actualización del documento

Revisado: Subgerente Administrativo y Financiero	Firma:	Fecha: 16 de enero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de enero de 2026