PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026 - 2028

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

Contenido

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

1. INTRODUCCIÓN

La E.S.E. Hospital San Jerónimo de Montería, en cumplimiento de lo establecido en el Decreto 1078 de 2015, el Decreto 612 de 2018 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, formula el presente Plan de Seguridad y Privacidad de la Información para la vigencia 2026–2028.

El presente plan consolida y fortalece la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), adoptando un enfoque progresivo y alineado con los lineamientos actuales de Gobierno Digital, el Sistema de Control Interno y el PETI 2026–2028. En consecuencia, el enfoque adoptado para el periodo 2026–2028 es progresivo, estructurado y ejecutable, priorizando el cumplimiento obligatorio del modelo sector público y su integración con el Sistema de Control Interno, el Sistema Integrado de Gestión y el PETI 2026–2028.

2. OBJETIVO DEL PLAN

Establecer el marco estratégico, técnico y administrativo que permita implementar y fortalecer el Modelo de Seguridad y Privacidad de la Información – MSPI, garantizando la protección de los activos de información institucionales bajo los principios de confidencialidad, integridad y disponibilidad, así como el adecuado tratamiento de datos personales conforme a la normativa vigente.

2.1 Objetivos Específicos

1. Identificar y clasificar los activos de información institucionales.
2. Implementar la gestión integral de riesgos de seguridad de la información.
3. Formalizar y aplicar políticas de seguridad y privacidad alineadas al MSPI.
4. Fortalecer los controles técnicos y administrativos de protección de información.
5. Implementar procedimiento formal de gestión de incidentes de seguridad.
6. Garantizar el cumplimiento normativo en protección de datos personales.
7. Desarrollar cultura institucional en seguridad digital.
8. Realizar seguimiento y mejora continua del MSPI.

3. ALCANCE

El presente plan aplica a todos los procesos misionales, estratégicos y de apoyo de la E.S.E. Hospital San Jerónimo de Montería.

Incluye:
- Sistemas de Información en Salud (HIS) y aplicativos administrativos.
- Infraestructura tecnológica (servidores, redes, equipos de cómputo, dispositivos móviles).
- Información en medio físico y digital.
- Servicios tercerizados que involucren tratamiento de información.

Es de obligatorio cumplimiento para funcionarios, contratistas, proveedores y terceros que accedan a activos de información institucionales.

4. DEFINICIONES

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- Antivirus: Software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- Ataques Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido

creados para atacar intencionalmente a los usuarios de ésta.

- Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados.
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).
- Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.
- Firewall: Es una aplicación de seguridad física y/o lógica diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
- Malware: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.
- Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Vulnerabilidad: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

5. MARCO NORMATIVO Y DOCUMENTOS DE REFERENCIA

El presente plan se fundamenta en:

- Constitución Política de Colombia.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1377 de 2013.
- Ley 1273 de 2009 – Delitos Informáticos.

- Decreto 1078 de 2015 – Decreto Único TIC.
- Decreto 612 de 2018 – Integración de planes institucionales.
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC).
- Guía para la implementación del MSPI – MinTIC.

6. METODOLOGÍA DE IMPLEMENTACIÓN – MODELO MSPI

La implementación del presente plan se desarrollará conforme a las fases establecidas en el Modelo de Seguridad y Privacidad de la Información:

6.1 Fase de Diagnóstico: Se realizará un diagnóstico institucional para evaluar el nivel de madurez actual en seguridad de la información, identificando brechas frente a los requerimientos del MSPI (Modelo de Seguridad y Privacidad de la Información).

6.2 Fase de Identificación y Valoración de Activos Se elaborará el inventario de activos de información, clasificándolos según su criticidad y nivel de sensibilidad.

6.3 Fase de Gestión del Riesgo Se construirá la matriz de riesgos de seguridad de la información, identificando amenazas, vulnerabilidades, impactos y controles existentes.

6.4 Fase de Plan de Tratamiento Se definirá el plan de tratamiento de riesgos priorizados, estableciendo responsables, plazos y recursos.

6.5 Fase de Implementación de Controles Se adoptarán controles administrativos, físicos y tecnológicos acordes a los riesgos identificados.

6.6 Fase de Seguimiento y Mejora Continua Se realizarán revisiones periódicas del cumplimiento del plan y actualización de la matriz de riesgos.

7. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1 Política de Control de Acceso: El acceso a los sistemas de información se otorgará bajo el principio de mínimo privilegio. Se implementará gestión formal de creación, modificación y eliminación de usuarios.

7.2 Política de Gestión de Usuarios y Contraseñas: Se establecerán lineamientos para la creación de credenciales seguras, periodicidad de cambio de contraseñas y bloqueo por intentos fallidos.

7.3 Política de Copias de Seguridad Se realizarán respaldos periódicos de bases de datos y servidores críticos, documentando pruebas de restauración al menos una vez al año.

7.4 Política de Gestión de Incidentes Se definirá procedimiento formal para el reporte, análisis y cierre de incidentes de seguridad.

7.5 Política de Seguridad Física Se controlará el acceso a áreas críticas como servidores y centros de cableado mediante mecanismos físicos y registros.

7.6 Política de Protección de Datos Personales Se garantizará el tratamiento adecuado de datos personales sensibles conforme a la Ley 1581 de 2012.

7.7 Política de Uso Aceptable Los recursos tecnológicos institucionales deberán ser utilizados exclusivamente para fines laborales.

7.8 Política de Continuidad del Servicio Se articulará el Plan de Continuidad del Negocio con la gestión de seguridad de la información.

7.9 Política de Capacitación y Concientización Se desarrollarán jornadas anuales de sensibilización en seguridad digital dirigidas a funcionarios y contratistas.

8. ROLES Y RESPONSABILIDADES

Gerencia: Aprobar el plan y asignar recursos.

Oficina TIC: Liderar la implementación técnica del MSPI.

Control Interno: Realizar seguimiento y evaluación.

Funcionarios: Cumplir políticas y reportar incidentes.

9. PLAN DE IMPLEMENTACIÓN 2026–2028

El Plan de Implementación del Modelo de Seguridad y Privacidad de la Información establece la ruta de ejecución mediante la cual la E.S.E. Hospital San Jerónimo de Montería desarrollará de manera progresiva los lineamientos definidos en el Plan de Seguridad y Privacidad de la Información para la vigencia 2026–2028.

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

Este plan organiza las actividades, responsables, recursos y tiempos requeridos para fortalecer la protección de los activos de información institucionales, garantizando la confidencialidad, integridad y disponibilidad de la información, así como el adecuado tratamiento de los datos personales conforme a la normativa vigente.

La implementación se realizará bajo un enfoque gradual, priorizando los controles asociados a los riesgos identificados y articulándose con el Plan Estratégico de Tecnologías de la Información (PETI), el Plan Operativo Anual (POA) y el Sistema de Control Interno. De esta manera, la seguridad de la información se integra a la operación institucional como un proceso continuo de mejora y no como una actividad aislada.

El presente Plan de Implementación permitirá realizar seguimiento periódico al avance del modelo, evaluar su efectividad y definir acciones de mejora, garantizando su sostenibilidad en el tiempo.

Año 2026: - Diagnóstico MSPI. - Matriz de riesgos. - Aprobación de políticas.

Año 2027: - Implementación de controles priorizados. - Formalización del procedimiento de incidentes. - Ejecución de capacitaciones institucionales.

Año 2028: - Evaluación de cumplimiento MSPI. - Actualización de matriz de riesgos. - Informe de cierre de vigencia.

10. INDICADORES DE SEGUIMIENTO

- % de riesgos tratados.
- Número de incidentes gestionados.
- % de personal capacitado.

10. SEGUIMIENTO Y CONTROL

El seguimiento del presente plan se realizará de manera trimestral mediante informes presentados a Gerencia y Control Interno, incluyendo avances, brechas identificadas y acciones correctivas.

Revisado: Subgerente Administrativo y Financiero	Firma:	Fecha: 16 de febrero de 2026
Aprobado: Gerente	Firma:	Fecha: 16 de febrero 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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
02	Actualización del documento

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