



Gobernación
MAGDALENA



E.S.E.HOSPITAL
NUESTRA SEÑORA
DEL CARMEN
DEPARTAMENTO DEL MAGDALENA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA: 2026



MADELEINE FRANCO DÍAZ
Gerente

E.S.E HOSPITAL NUESTRA SEÑORA DEL CARMEN - GUAMAL, MAGDALENA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2026 E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN

TABLA DE CONTENIDO

1. Introducción

  Gobernación del MAGDALENA	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 2 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

2. Objetivos del Plan
3. Marco Normativo
4. Articulación con MIPG y Programa de Transparencia y Ética Pública
5. Plataforma Estratégica de la E.S.E.
6. Alcance del Plan
7. Diagnóstico Institucional – Matriz DOFA
8. Sistemas de Información Implementados
9. Gestión de Seguridad y Privacidad de la Información
10. Plan de Acción – Vigencia 2026
11. Matriz de Riesgos de Seguridad de la Información
12. Seguimiento, Indicadores y Mejora Continua
13. Vigencia

1. INTRODUCCIÓN

La seguridad y privacidad de la información se ha consolidado como uno de los pilares fundamentales de la gestión pública moderna, especialmente en el sector salud, donde la información clínica, administrativa y financiera constituye un activo crítico para la continuidad del servicio y la protección de los derechos de los usuarios.

  Gobernación del MAGDALENA	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 3 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

La E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, reconoce que la información es un recurso estratégico que debe ser gestionado bajo criterios de confidencialidad, integridad y disponibilidad, garantizando su uso adecuado y protegiendo los datos personales y sensibles de pacientes, funcionarios y terceros.

El presente Plan de Seguridad y Privacidad de la Información para la vigencia 2026 actualiza y fortalece el documento adoptado en la vigencia 2025, incorporando las lecciones aprendidas, los cambios tecnológicos y las nuevas exigencias normativas aplicables a la entidad.

La transformación digital del sector salud ha incrementado el uso de sistemas de información asistenciales y administrativos, lo que exige una gestión más robusta de los riesgos asociados a la seguridad de la información.

Actualmente, la E.S.E. cuenta con tres sistemas de información: dos asistenciales (DNA PLUS e INFOSALUD) y uno financiero (APOLO), los cuales operan de manera independiente, generando riesgos asociados a la dispersión, duplicidad y falta de consolidación de la información.

Se observan entre otros contextos:

- Importancia de la información clínica
- Riesgos actuales de la E.S.E.
- Uso de **DNA PLUS, INFOSALUD y APOLO**
- Falta de software integral de historia clínica
- Ausencia de responsable del SGSI
- Articulación con MIPG y Transparencia
- Enfoque PHVA

Adicionalmente, la entidad no cuenta con un sistema especializado para la gestión integral de la historia clínica electrónica que garantice su custodia, trazabilidad y organización conforme a la normatividad vigente, lo cual representa un riesgo crítico para la confidencialidad y disponibilidad de la información clínica.

	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 4 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

Así mismo, se evidencia la ausencia de un responsable formal del Sistema de Gestión de Seguridad y Privacidad de la Información, situación que limita la gobernanza, el control y la mejora continua del proceso.

Este Plan se estructura conforme al Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio TIC, el Modelo Integrado de Planeación y Gestión – MIPG, la norma ISO/IEC 27001 y la normatividad colombiana vigente en materia de protección de datos personales, transparencia y acceso a la información pública.

El documento adopta el enfoque del ciclo PHVA (Planear, Hacer, Verificar y Actuar), permitiendo una implementación progresiva, medible y sostenible de las acciones definidas.

La actualización del Plan responde también a la necesidad de articular las acciones de seguridad de la información con el Programa de Transparencia y Ética Pública, fortaleciendo la confianza institucional, la rendición de cuentas y la lucha contra la corrupción.

En este sentido, la seguridad de la información no se concibe como una responsabilidad exclusiva del área de sistemas, sino como un compromiso transversal que involucra a todos los servidores públicos y contratistas de la entidad.

El Plan establece lineamientos claros para el uso de los sistemas de información, el manejo de dispositivos, la gestión de copias de seguridad, el control de accesos y la atención de incidentes de seguridad.

Así mismo, incorpora un diagnóstico institucional detallado, una matriz DOFA y un plan de acción con actividades normadas, responsables, indicadores y cronograma de ejecución.

La implementación efectiva de este Plan permitirá a la E.S.E. Hospital Nuestra Señora del Carmen reducir los riesgos asociados a la pérdida, alteración o divulgación no autorizada de la información, garantizando la continuidad operativa y el cumplimiento de los objetivos misionales.

   	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 5 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

Finalmente, este documento se consolida como un instrumento estratégico que contribuye al fortalecimiento institucional, al mejoramiento del desempeño en MIPG y FURAG y a la protección de los derechos fundamentales de los ciudadanos.

2. OBJETIVOS DEL PLAN

Objetivo General

Diseñar, implementar y fortalecer la gestión de la seguridad y privacidad de la información de la E.S.E. Hospital Nuestra Señora del Carmen, garantizando la protección de los activos de información y la continuidad de los servicios durante la vigencia 2026.

Objetivos Específicos

- Proteger la información clínica, administrativa y financiera.
- Garantizar el cumplimiento de la normatividad sobre protección de datos personales.
- Fortalecer la gobernanza de la seguridad de la información.
- Reducir los riesgos asociados a los sistemas de información.
- Articular la seguridad de la información con MIPG y el Programa de Transparencia y Ética Pública.

7. DIAGNÓSTICO INSTITUCIONAL – MATRIZ DOFA

   Gobernación del MAGDALENA	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 6 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

Fortalezas	Oportunidades
Sistemas de información implementados	Lineamientos MSPI y MIPG
Compromiso gerencial	Apoyo del MinTIC
Debilidades	Amenazas
No hay responsable del SGSI	Fugas de información
Sistemas no integrados	Sanciones legales
No hay software de historia clínica integral	Pérdida de datos

10. PLAN DE ACCIÓN – VIGENCIA 2026

Actividad	Indicador	Responsable	Fecha
Designar responsable de seguridad de la información	Acto administrativo expedido	Gerencia	I Trimestre
Inventario de activos de información	Inventario actualizado	Sistemas	I Trimestre
Política de seguridad la información actualizada	Política adoptada	Gerencia	I Trimestre
Integración prioritaria de sistemas asistenciales	Análisis técnico realizado	Sistemas	II Trimestre
Implementar controles de acceso	% accesos controlados	Sistemas	II Trimestre

   Gobernación del MAGDALENA	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 7 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

Definir lineamientos de historia clínica	Documento aprobado	Calidad	II Trimestre
Implementar plan de backups	Backups periódicos	Sistemas	Permanente
Capacitación al personal	% personal capacitado	Talento Humano	II Trimestre
Gestión de incidentes	Incidentes atendidos	Sistemas	Permanente
Articulación con Transparencia	Actividades integradas	Asesor Planeación	III Trimestre
Seguimiento MSPI	Informes elaborados	Control Interno	Semestral
Evaluación de riesgos	Matriz actualizada	Calidad	Semestral
Actualización procedimientos	Procedimientos vigentes	Sistemas	III Trimestre
Auditoría interna	Auditoría realizada	Control Interno	IV Trimestre
Informe FURAG	Reporte enviado	Asesor Planeación	IV Trimestre
Plan de mejora	Plan formulado	Control interno	IV Trimestre
Evaluación final del plan	Informe final	Comité de gestión y desempeño	IV Trimestre

13. VIGENCIA ANÁLISIS

   	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 8 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

La E.S.E. Hospital Nuestra Señora del Carmen de Guamal presenta un nivel de madurez en desarrollo en la Política de Seguridad Digital, identificando de manera clara sus brechas actuales y formulando un Plan de Seguridad y Privacidad de la Información 2026 con acciones concretas, medibles y normadas, lo cual permite cumplir progresivamente con los requisitos evaluados en el FURAG y fortalecer su desempeño institucional.

14. MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La identificación y gestión de riesgos de seguridad de la información se realiza articulados con el Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC y el enfoque de Gestión del Riesgo del MIPG.

La valoración se realiza considerando probabilidad, impacto y nivel de riesgo, definiendo controles preventivos, detectivos y correctivos

Activo de Información	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	Control ISO 27001	Responsable
Historia Clínica	Acceso no autorizado	No existe sistema integral	Alto	Alta	Crítico	Control de accesos, cifrado	Sistemas
Historia Clínica	Pérdida de información	Falta de backups estructurados	Alto	Media	Alto	Copias de seguridad	Sistemas
Sistemas asistenciales (DNA PLUS / INFOSALUD)	Información inconsistente	Sistemas no integrados	Alto	Alta	Crítico	Integración / validación	Sistemas
Información financiera (APOLO)	Manipulación de datos	Roles no formalizados	Alto	Media	Alto	Segregación de funciones	Financiera
Infraestructura TIC	Fallas técnicas	Falta de plan de contingencia	Alto	Media	Alto	Plan de continuidad	Sistemas

   	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 9 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

Usuarios internos	Uso indebido de información	Falta de capacitación	Media	Alta	Alto	Capacitación y sensibilización	Talento Humano
Dispositivos físicos	Pérdida o robo	Falta de inventario	Media	Media	Medio	Inventario y custodia	Sistemas
Datos personales	Incumplimiento legal	Falta de política de datos	Alto	Media	Alto	Política de protección de datos	Jurídica
Accesos a sistemas	Credenciales compartidas	Falta de controles	Alto	Alta	Crítico	Autenticación y perfiles	Sistemas
Información pública	Alteración indebida	Falta de control de cambios	Media	Media	Medio	Gestión de cambios	Planeación

ARTICULACIÓN FURAG			
Pregunta FURAG	Qué evalúa	Respuesta Institucional	Evidencia
¿La entidad cuenta con un Plan de Seguridad y Privacidad de la Información?	Existencia formal del plan	Sí, actualizado para la vigencia 2026	Plan SPI 2026
¿El Plan está formalmente adoptado?	Acto administrativo	En proceso de adopción mediante Resolución	Resolución
¿El Plan cubre información clínica, administrativa y financiera?	Alcance	Sí	Alcance del Plan
¿Se revisa y actualiza periódicamente?	Mejora continua	Sí, revisión anual	Cronograma
GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN			
¿Existe un responsable de la seguridad de la información?	Gobernanza	No actualmente, se define como acción prioritaria 2026	Plan de Acción
¿Están definidos roles y responsabilidades?	Organización	Parcial, en proceso de formalización	Matriz RACI
¿La Alta Dirección participa?	Liderazgo	Sí	Actas / Plan
PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA			

 E.S.E HOSPITAL NUESTRA SEÑORA DEL CARMEN DEPARTAMENTO DEL MAGDALENA  Gobernación del MAGDALENA	VERSION:	04
	FECHA DE ACTUALIZACION:	30-ENE-2026
	CÓDIGO:	HNSC-GG-M-011
	PAGINA	Página 10 de 10
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		

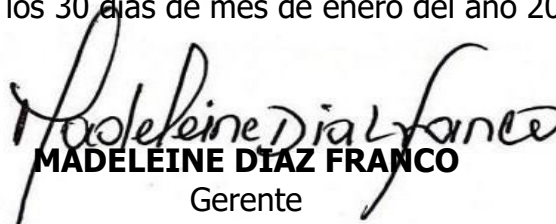
¿La entidad cumple la Ley 1581 de 2012?	Legalidad	Parcial, con plan de fortalecimiento 2026	Plan SPI
¿Existe política de protección de datos?	Formalización	En proceso de adopción	Plan de Acción
¿Se protege la información sensible?	Seguridad	Parcial, con controles básicos	Diagnóstico
GESTIÓN DE ACTIVOS DE INFORMACIÓN			
¿La entidad identifica activos de información?	Inventario	No consolidado, se formula en 2026	Plan de Acción
¿Se clasifican los activos?	Riesgo	No	Diagnóstico
¿Se priorizan activos críticos?	Impacto	Sí (historia clínica, financiera)	DOFA
ARTICULACIÓN CON TRANSPARENCIA Y ÉTICA PÚBLICA			
¿La seguridad de la información se articula con Transparencia?	Integración	Sí	Plan de Acción
¿Se previene manipulación de información?	Anticorrupción	Sí	Controles definidos
¿Se garantiza integridad de la información pública?	Confianza	Parcial	Diagnóstico

16. VIGENCIA

El presente Plan de Seguridad y Privacidad de la Información rige del 1 de enero al 31 de diciembre de 2026.

COMUNÍQUESE, NOTIFÍQUESE Y CÚMPLASE.

Dada a los 30 días de mes de enero del año 2026


MADELEINE DÍAZ FRANCO
 Gerente
 E.S.E. Hospital Nuestra Señora del Carmen