

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

Contenido

Introducción	2
Objetivo General	2
Objetivos Específicos	2
Marco Normativo	3
Articulación con el Modelo Integrado de Planeación y Gestión – MIPG	4
Alcance	5
Responsables	6
Diagnóstico	7
Estrategias y líneas de acción	8
Plan de Acción	9
Indicadores	10
Recursos	12
Seguimiento y Evaluación	13
Riesgos asociados al Plan	14
Vigencia	15
Modificaciones	15
Aprobación	16

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04 FECHA: 25/01/2026

Introducción

El Plan de Seguridad y privacidad de la Información 2026 de la E.S.E. Hospital San Juan de Dios de Yarumal tiene como finalidad garantizar la protección, integridad, confidencialidad y disponibilidad de la información institucional, reconociéndola como un activo estratégico para la gestión administrativa, clínica y operativa de la entidad.

Este plan responde a los desafíos actuales en materia de seguridad de la información, incluyendo ciberataques, malware, ingeniería social, pérdida de información, robo, sabotaje, incendios, inundaciones y otras amenazas internas y externas que podrían afectar la continuidad de los procesos críticos de la institución.

El documento establece lineamientos, responsabilidades y procedimientos dirigidos a servidores públicos, contratistas, proveedores y terceros que interactúan con la información institucional, asegurando la gestión adecuada de los riesgos asociados y el cumplimiento de la normativa vigente en materia de seguridad y protección de datos.

La ESE mantiene su compromiso con un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los estándares internacionales ISO/IEC 27001:2013, asegurando la mejora continua y la actualización de políticas, procesos y controles de seguridad conforme a las necesidades de la vigencia 2026.

Objetivo General

Garantizar la seguridad y privacidad de la información institucional de la E.S.E. Hospital San Juan de Dios de Yarumal, mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) actualizado, que minimice riesgos asociados a la pérdida, alteración o divulgación no autorizada de información, asegurando la disponibilidad, integridad y confidencialidad de los activos de información y contribuyendo a la continuidad operativa de los procesos administrativos y asistenciales en la vigencia 2026.

Objetivos Específicos

- Proteger los activos de información de la E.S.E., frente a amenazas internas y externas, deliberadas o accidentales, asegurando confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio.
- Mantener actualizado y operativo el plan de seguridad y privacidad de la información, adaptándolo a los riesgos emergentes, tecnologías nuevas y cambios en los procesos institucionales.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04 FECHA: 25/01/2026

- Definir roles y responsabilidades claras para la gestión de la seguridad de la información, incluyendo servidores públicos, contratistas y terceros vinculados a la E.S.E.
- Implementar estrategias de gestión de riesgos, identificando, evaluando y mitigando los riesgos asociados a la información y los sistemas institucionales.
- Fortalecer la cultura de seguridad de la información, mediante capacitación y sensibilización continua a todo el personal de la E.S.E., proveedores y usuarios externos.
- Asegurar la recuperación ante contingencias y la continuidad de los servicios, mediante planes de respaldo, recuperación y retorno a la normalidad frente a incidentes de seguridad de la información.
- Alinear el plan con las normas legales y los estándares internacionales, incluyendo ISO/IEC 27001:2013 y la normativa nacional vigente en seguridad de la información y protección de datos personales.

Marco Normativo

El presente plan se fundamenta en las disposiciones legales, decretos y lineamientos nacionales e internacionales que regulan la seguridad y privacidad de la información, la gestión de activos de información y la continuidad operativa de las entidades públicas.

Normas constitucionales y legales:

- **Constitución Política de Colombia**, Artículos 15, 20, 23 y 74 (protección de datos, derecho de acceso a la información y garantía de la privacidad).
- **Ley 1581 de 2012 y Decreto 1377 de 2013** sobre protección de datos personales.
- **Ley 1266 de 2008** sobre habeas data financiero y crediticio.
- **Ley 527 de 1999** sobre mensajes de datos, comercio electrónico y firma digital.
- **Ley 1712 de 2014** de Transparencia y Derecho de Acceso a la Información Pública.
- **Ley 1341 de 2009** sobre TIC, sociedad de la información y organismos reguladores.
- **Ley 1273 de 2009** sobre delitos informáticos y protección de sistemas de información.

Decretos y reglamentación:

- **Decreto 1499 de 2017**: establece lineamientos del Sistema de Gestión en las entidades públicas.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04 FECHA: 25/01/2026

- **Decreto 612 de 2018**, Artículo 1: directrices para la integración de los planes institucionales al Plan de Acción.
- **Decreto 1008 de 2018**: lineamientos de la política de Gobierno Digital.
- **Decreto 338 de 2022**: fortalece la gobernanza de la seguridad digital en las entidades públicas.
- **Decreto 88 de 2022**: lineamientos para digitalización, automatización de trámites y gestión de servicios en línea.

Lineamientos institucionales y sectoriales:

- **Directrices del DAFP** y demás entidades competentes en gestión pública, seguridad de la información y protección de datos personales.
- **Normas internacionales ISO/IEC 27001:2013** para sistemas de gestión de seguridad de la información y buenas prácticas en TI.
- Políticas y procedimientos internos de la E.S.E. Hospital San Juan de Dios relacionados con seguridad, privacidad y continuidad operativa de la información.

Otras normativas complementarias:

- Leyes, decretos y resoluciones relacionadas con derechos de autor, propiedad intelectual, teletrabajo y gestión documental que tengan impacto en la administración de los activos de información de la institución.

Articulación con el Modelo Integrado de Planeación y Gestión – MIPG

Dimensiones del MIPG a las que aporta el plan:

- **Gestión del Talento Humano**: fortalece la cultura de seguridad y sensibilización sobre la protección de la información.
- **Gestión de la Información y la Tecnología**: asegura la integridad, disponibilidad y confidencialidad de los activos de información.
- **Gestión de Riesgos**: contribuye a la identificación, valoración y mitigación de riesgos asociados a la seguridad de la información.
- **Control Interno**: establece mecanismos de control, auditoría y seguimiento de los procesos de información.

Políticas de gestión y desempeño institucional relacionadas:

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

- Política de Seguridad de la Información.
- Política de Gestión de Riesgos Institucionales.
- Política de Continuidad Operativa y Planes de Contingencia.
- Lineamientos de Gobierno Digital y Gobierno en Línea (Decreto 612 de 2018).

Contribución del plan al cumplimiento de los objetivos estratégicos institucionales:

- Garantizar la disponibilidad y confiabilidad de los sistemas de información institucionales.
- Proteger los activos de información frente a amenazas internas y externas.
- Asegurar la continuidad de los procesos críticos administrativos y asistenciales.
- Cumplir con los estándares legales y normativos de protección de datos y seguridad digital.

Alcance

El Plan de Seguridad y Privacidad de la Información 2026 aplica a todas las dependencias y áreas de la ESE Hospital San Juan de Dios de Yarumal que manejan información institucional, incluyendo sistemas administrativos, clínicos, financieros y de talento humano.

- **Dependencias involucradas:**
 - Gerencia General
 - Área de Sistemas y Tecnologías de la Información
 - Área de Talento Humano
 - Área Financiera
 - Área de Atención al Usuario y Archivo
 - Todas las unidades administrativas y asistenciales que generen, procesen o almacenen información institucional.
- **Población objetivo:**
 - Servidores públicos, contratistas y personal temporal que manipulen información institucional en cualquier formato (digital o físico).
 - Usuarios internos que requieren acceso a los sistemas y bases de datos institucionales.
- **Alcance funcional:**

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

- Protección de la confidencialidad, integridad y disponibilidad de la información institucional.
- Implementación de controles físicos, técnicos, administrativos y legales sobre los activos de información.
- Sensibilización y capacitación del personal en prácticas de seguridad y privacidad de la información.

Responsables

Dependencia líder del plan:

- **Área de Sistemas y Tecnologías de la Información (TI)**
 - Responsable de la coordinación general del plan, implementación de controles técnicos, seguimiento de la seguridad de la información y reporte al Comité de Seguridad de la Información.

Dependencias de apoyo:

- **Gerencia General:** Supervisión estratégica, asignación de recursos y toma de decisiones sobre políticas de seguridad de la información.
- **Talento Humano:** Gestión de sensibilización y capacitación del personal en temas de seguridad y privacidad de la información.
- **Área Financiera:** Aseguramiento de la correcta administración de recursos para la implementación de controles y medidas de seguridad.
- **Archivo y Atención al Usuario:** Garantía de manejo adecuado de la información física y digital, así como del acceso a datos sensibles por parte de los usuarios internos y externos.

Roles y responsabilidades generales:

- **Líder del plan (TI):**
 - Coordinar la implementación y actualización de las medidas de seguridad de la información.
 - Monitorear y reportar incidentes de seguridad.
 - Elaborar informes periódicos de avance y cumplimiento del plan.
- **Gerencia General:**
 - Aprobar políticas, estrategias y recursos asociados al plan.
 - Supervisar la correcta ejecución y seguimiento del plan en todas las áreas.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

- **Talento Humano:**

- Implementar programas de capacitación y sensibilización del personal.
- Apoyar en la verificación del cumplimiento de los protocolos de seguridad en el manejo de información.

- **Otras dependencias de apoyo:**

- Colaborar en la implementación de controles específicos según su rol funcional.
- Garantizar la correcta custodia y tratamiento de la información bajo su responsabilidad.

Diagnóstico

Situación institucional vigente:

Actualmente, la ESE Hospital San Juan de Dios de Yarumal cuenta con lineamientos básicos de seguridad de la información, soportados en las políticas internas de manejo de datos y los protocolos de protección de información sensible. Sin embargo, se evidencia la necesidad de fortalecer los controles técnicos y administrativos frente a la confidencialidad, integridad y disponibilidad de la información, así como de unificar criterios de privacidad de los datos de pacientes y usuarios.

Resultados de evaluaciones internas y externas:

- Auditorías internas recientes han identificado áreas de oportunidad en la gestión de accesos a sistemas, manejo de contraseñas y respaldo de información crítica.
- Evaluaciones externas realizadas por entidades de control han resaltado la importancia de formalizar políticas claras sobre el manejo de información digital y física, y de establecer procedimientos estandarizados para incidentes de seguridad.

Hallazgos de órganos de control:

- Recomendaciones de la Contraloría General de Antioquia relacionadas con la protección de datos y la documentación de procedimientos de seguridad informática.
- Observaciones de la Secretaría de Salud departamental sobre la necesidad de garantizar la trazabilidad y control de la información clínica.

Necesidades identificadas:

- ❖ Formalizar y actualizar las políticas y procedimientos de seguridad y privacidad de la información.
- ❖ Implementar controles de acceso más robustos y mecanismos de autenticación segura.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

- ❖ Desarrollar un programa de capacitación continua sobre seguridad de la información para todo el personal.
- ❖ Establecer un sistema de monitoreo y gestión de incidentes de seguridad.
- ❖ Garantizar la integración de la gestión de seguridad de la información con los objetivos estratégicos institucionales y con el MIPG.

Conclusión del diagnóstico:

El análisis evidencia que, si bien existen bases para la protección de la información, la ESE requiere un fortalecimiento integral de su seguridad y privacidad de datos, mediante la formalización de políticas, actualización tecnológica, capacitación y establecimiento de controles periódicos, para cumplir con la normatividad vigente y las buenas prácticas de gestión de la información.

Estrategias y líneas de acción

Estrategia 1: Fortalecimiento de la gobernanza de la seguridad de la información

- **Línea de acción 1:** Actualizar y formalizar la política institucional de seguridad y privacidad de la información, alineada con la normatividad vigente y las mejores prácticas internacionales (ISO/IEC 27001, Ley 1581 de 2012, Decreto 1074 de 2015).
- **Línea de acción 2:** Establecer roles y responsabilidades claras para la gestión de seguridad de la información, incluyendo comités de gobernanza y responsables de seguridad por dependencia.
- **Línea de acción 3:** Implementar un marco de control y seguimiento periódico de las políticas y procedimientos de seguridad.
-

Estrategia 2: Gestión de riesgos y controles de seguridad

- **Línea de acción 1:** Identificar, evaluar y priorizar riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información.
-
- **Línea de acción 2:** Implementar controles técnicos y administrativos adecuados para mitigar los riesgos identificados, incluyendo cifrado de datos, gestión de accesos y respaldo seguro de información.
-
- **Línea de acción 3:** Establecer un plan de respuesta a incidentes de seguridad de la información y un sistema de monitoreo continuo.

Estrategia 3: Capacitación y sensibilización del talento humano

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

- **Línea de acción 1:** Desarrollar programas de formación periódicos sobre seguridad y privacidad de la información dirigidos a todo el personal.
-
- **Línea de acción 2:** Realizar campañas de sensibilización sobre buenas prácticas de manejo de información sensible y confidencial.
-
- **Línea de acción 3:** Evaluar periódicamente la efectividad de la capacitación mediante encuestas y ejercicios prácticos.
-

Estrategia 4: Integración tecnológica y mejora continua

- **Línea de acción 1:** Implementar herramientas tecnológicas que soporten la seguridad de la información, como sistemas de control de accesos, auditoría de usuarios y protección de bases de datos.
- **Línea de acción 2:** Establecer un sistema de seguimiento y evaluación de incidentes de seguridad, con registro y análisis de tendencias para la mejora continua.
-
- **Línea de acción 3:** Mantener actualización constante de sistemas, software y protocolos de seguridad ante nuevas amenazas.
-

Estrategia 5: Articulación con la estrategia institucional y el MIPG

- **Línea de acción 1:** Alinear el plan con los objetivos estratégicos institucionales y las políticas de gestión y desempeño del MIPG.
-
- **Línea de acción 2:** Incorporar indicadores de desempeño del plan que permitan medir la efectividad de las estrategias implementadas.

Plan de Acción

Estrategia	Actividad	Responsable	Fecha Inicio	Fecha Final	Producto/ Entregable	Indicador
Fortalecimiento de la gobernanza de la seguridad de la información	Actualizar y formalizar la política de seguridad y privacidad de la información	Coordinador de Seguridad de la Información	01/02/2026	30/03/2026	Política institucional actualizada	% de cumplimiento de actualización de políticas
Fortalecimiento de la gobernanza de la	Establecer roles y responsabilidades de	Coordinador de Seguridad de la Información /	01/02/2026	31/03/2026	Matriz de responsabilidades y comités de gobernanza	Número de dependencias con roles definidos

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

seguridad de la información	seguridad por dependencia	Jefes de Área				
Gestión de riesgos y controles de seguridad	Identificar y priorizar riesgos de seguridad de la información	Equipo de Seguridad de la Información	01/03/2026	30/04/2026	Informe de evaluación de riesgos	Número de riesgos identificados y priorizados
Gestión de riesgos y controles de seguridad	Implementar controles técnicos y administrativos	Equipo de Seguridad de la Información / Área de TI	01/04/2026	31/08/2026	Controles implementados (cifrado, accesos, respaldos)	% de controles implementados según plan
Gestión de riesgos y controles de seguridad	Establecer plan de respuesta a incidentes	Equipo de Seguridad de la Información	01/05/2026	30/06/2026	Plan de respuesta a incidentes formalizado	Tiempo promedio de respuesta a incidentes
Capacitación y sensibilización del talento humano	Diseñar programa de formación en seguridad y privacidad	Coordinador de Talento Humano / Coordinador de Seguridad	01/03/2026	30/04/2026	Programa de formación aprobado	Número de programas diseñados
Capacitación y sensibilización del talento humano	Implementar programas de capacitación	Coordinador de Talento Humano / Jefes de Área	01/05/2026	31/12/2026	Personal capacitado	% de personal capacitado
Integración tecnológica y mejora continua	Implementar herramientas de control de accesos y auditoría	Área de TI / Equipo de Seguridad de la Información	01/04/2026	30/09/2026	Herramientas operativas	% de herramientas implementadas
Integración tecnológica y mejora continua	Monitoreo y análisis de incidentes de seguridad	Equipo de Seguridad de la Información	01/05/2026	31/12/2026	Reportes de incidentes y tendencias	Número de incidentes gestionados y reportados
Articulación con la estrategia institucional y el MIPG	Incorporar indicadores de desempeño y seguimiento	Coordinador de Seguridad de la Información / Planeación	01/02/2026	28/02/2026	Tablero de indicadores	Número de indicadores definidos y reportados

Indicadores

INDICADORES DE GESTIÓN				
INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Cumplimiento del plan de acción	(Actividades ejecutadas / Total de actividades planificadas) x	Trimestral	Informe de avance del plan	≥ 90%

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

	100			
Capacitación del personal en seguridad y privacidad	(Número de personas capacitadas / Total de personas en la entidad) x 100	Semestral	Listas de asistencia y certificados	≥ 95%
Actualización de políticas y procedimientos	(Número de políticas actualizadas / Total de políticas programadas) x 100	Anual	Documentos institucionales actualizados	100%

INDICADORES DE RESULTADO

INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Política de seguridad y privacidad formalizada	Número de políticas actualizadas	Anual	Documento oficial de política	1
Matriz de responsabilidades implementada	Número de áreas con roles definidos / Total de áreas x 100	Anual	Matriz de roles	100%
Plan de respuesta a incidentes formalizado	Número de planes implementados	Anual	Documento aprobado por la gerencia	1

INDICADORES DE PRODUCTO

INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Reducción de incidentes de seguridad	(Incidentes reportados año anterior – Incidentes reportados año actual) / Incidentes año anterior x 100	Anual	Reportes de incidentes	≥ 20% reducción
Nivel de cumplimiento de controles de seguridad	(Controles implementados / Controles planificados) x 100	Semestral	Informe de auditoría interna	≥ 90%
Participación en programas de sensibilización	(Número de personas capacitadas / Total de personal) x 100	Semestral	Certificados y listas de asistencia	≥ 95%

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

INDICADORES DE IMPACTO				
INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Reducción de riesgos críticos de seguridad de la información	Número de riesgos críticos mitigados / Total de riesgos críticos identificados x 100	Anual	Informe de gestión de riesgos	≥ 90%
Cumplimiento normativo en seguridad y privacidad	(Número de hallazgos de auditoría / Total de auditorías realizadas) x 100	Anual	Informes de auditoría externa	0 hallazgos críticos
Nivel de confianza de los usuarios en la gestión de la información	Encuesta de satisfacción	Anual	Encuestas aplicadas al personal y usuarios internos	≥ 85% satisfechos

Recursos

Recursos Humanos		
Cargo / Rol	Función en el plan	Cantidad estimada
Responsable de Seguridad de la Información	Coordinar la implementación del plan, supervisar controles y evaluar resultados	1
Analista de Seguridad y Privacidad	Apoyo en la gestión de riesgos, auditorías internas y reportes de incidentes	2
Coordinador de Capacitación	Planificación y ejecución de actividades de sensibilización y formación del personal	1
Personal operativo	Cumplimiento de procedimientos y buenas prácticas de seguridad en su área	Todo el personal de la entidad
Recursos Financieros		
Concepto	Detalle	Presupuesto estimado
Capacitación del personal	Talleres, cursos y certificaciones en seguridad y privacidad	\$15.000.000 anual
Implementación de controles tecnológicos	Software de gestión de accesos, antivirus, cifrado y monitoreo de información	\$30.000.000 anual

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

Auditorías internas y externas	Evaluaciones de cumplimiento y pruebas de vulnerabilidad	\$10.000.000 anual
Materiales de comunicación	Guías, cartillas, afiches y campañas de sensibilización	\$5.000.000 anual
Recursos Técnicos y Tecnológicos		
Recurso		Descripción / Uso
Software de gestión de seguridad		Monitoreo, control de accesos y registro de incidentes
Servidores y almacenamiento seguro		Respaldo y protección de información crítica
Herramientas de cifrado y autenticación		Protección de datos confidenciales y personales
Plataforma de capacitación virtual		Implementación de programas de formación en seguridad y privacidad
Sistemas de alerta y monitoreo		Detección temprana de incidentes de seguridad

Seguimiento y Evaluación

El seguimiento y evaluación del Plan de Seguridad y Privacidad de la Información se realizará mediante un mecanismo institucional estructurado, que permitirá verificar avances, garantizar el cumplimiento de los objetivos y asegurar la mejora continua en la gestión de la información.

Componentes del mecanismo de seguimiento:

Periodicidad de seguimiento

- Seguimiento interno: trimestral, a cargo del responsable de Seguridad de la Información y del Comité de Seguridad.
- Evaluación externa: anual, mediante auditorías internas y externas que validen el cumplimiento de políticas y controles.

Evaluación de avances y cumplimiento

- Revisión de indicadores definidos en el plan (gestión, producto, resultado e impacto).
- Monitoreo del estado de implementación de estrategias, líneas de acción y actividades del plan.
- Identificación de desviaciones y brechas frente a lo planificado.

Reporte de resultados

- Informe trimestral a la alta dirección, con hallazgos, logros, dificultades y recomendaciones.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

- Reporte anual consolidado para entes de control y organismos de supervisión pertinentes.

–

Acciones de mejora

- Implementación de planes de acción correctiva ante hallazgos o incumplimientos.
- Actualización periódica de estrategias, procedimientos y controles según resultados de evaluación.
- Retroalimentación al personal mediante capacitaciones y sensibilización continua.

Riesgos asociados al Plan

A continuación, se identifican los principales riesgos que podrían afectar la ejecución y efectividad del Plan de Seguridad y Privacidad de la Información, junto con las acciones generales de mitigación, en articulación con el Sistema de Control Interno:

Riesgo	Causas	Consecuencias	Acciones de Mitigación	Responsable
Acceso no autorizado a información sensible	Falta de controles de acceso, uso inadecuado de credenciales	Pérdida de confidencialidad, vulneración de datos personales, sanciones legales	Implementar autenticación multifactor, revisión periódica de permisos, capacitación al personal	Coordinación de Tecnologías de la Información / Seguridad de la Información
Fuga o pérdida de información	Manejo inadecuado de dispositivos, correo electrónico inseguro, almacenamiento no controlado	Riesgo reputacional, incumplimiento normativo	Encriptación de información, procedimientos de respaldo, sensibilización sobre manejo seguro de información	Coordinación de Tecnologías de la Información / Seguridad de la Información
Incumplimiento normativo	Desconocimiento de la normatividad, ausencia de actualización normativa	Sanciones legales, auditorías negativas	Actualización periódica de procedimientos, seguimiento de cambios legales, asesoría jurídica	Oficina Jurídica / Subgerencia Administrativa
Fallas en sistemas tecnológicos	Errores de software, interrupciones de	Interrupción de operaciones, pérdida de	Actualización y mantenimiento de sistemas,	Coordinación de Tecnologías de la Información /

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

	servicios, vulnerabilidades	información crítica	pruebas de recuperación, monitoreo continuo de vulnerabilidades	Seguridad de la Información
Falta de sensibilización del personal	Capacitación insuficiente, baja cultura de seguridad	Incumplimiento de procedimientos, incidentes de seguridad	Capacitación continua, campañas de concienciación, evaluación de conocimientos del personal	Talento Humano / Coordinación de Tecnologías de la Información
Riesgo de terceros	Proveedores o contratistas con accesos a información sin controles adecuados	Vulneración de datos, incumplimiento contractual	Evaluación de proveedores, seguimiento de cumplimiento contractual, auditorías de seguridad	Coordinación de Tecnologías de la Información / Oficina Jurídica

Vigencia

El presente plan tendrá vigencia durante el año 2026, iniciando el 1 de enero y finalizando el 31 de diciembre de 2026, sin perjuicio de las actualizaciones, ajustes o revisiones que se consideren necesarias durante el período, con el fin de garantizar su efectividad y adecuación a los cambios normativos, tecnológicos y organizacionales que puedan presentarse. La revisión y actualización se realizará de manera periódica y documentada, asegurando la continuidad de la gestión de seguridad y privacidad de la información en la entidad.

Modificaciones

Fecha	Versión	Paginas Afectadas	Descripción del contenido
19/01/2023	01		Creación del documento
03/01/2024	02	Todo el documento	Actualización del documento
04/01/2025	03	Todo el documento	Actualización del documento
25/01/2025	04	Todo el documento	Actualización del documento

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO SISTEMAS DE LA INFORMACIÓN	CÓDIGO: PL-20-001
			VERSIÓN: 04
			FECHA: 25/01/2026

Aprobación

ELABORÓ:	REVISÓ	APROBÓ:
Diego Fernando Hernández	Jorge Armando Patiño Medina Coordinador Oficina Jurídica	Daniel Alcides Vergara
Asesor MIPG	Yenny Alexandra Herrera Coordinadora Calidad	Gerente