

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

Contenido

Introducción	2
Objetivo General	2
Objetivos Específicos	3
Marco Normativo	3
Articulación con el Modelo Integrado de Planeación y Gestión – MIPG	5
Alcance	6
Responsables	7
Diagnóstico	8
Estrategias y líneas de acción	10
Plan de Acción	12
Indicadores	13
Recursos	15
Seguimiento y evaluación	16
Riesgos asociados al Plan	17
Vigencia	19
Modificaciones	20
Aprobación	20

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital 2026 del Hospital San Juan de Dios de Yarumal constituye un instrumento estratégico de gestión institucional orientado a garantizar la protección, integridad, disponibilidad y confidencialidad de la información generada, procesada y almacenada por la entidad. Este plan se enmarca dentro del Modelo Integrado de Planeación y Gestión – MIPG, apoyando la planeación, ejecución, seguimiento y mejora continua de los procesos misionales, administrativos y de apoyo, con un enfoque preventivo frente a riesgos de seguridad de la información.

El plan tiene como finalidad identificar, evaluar, tratar y monitorear los riesgos asociados a la seguridad y privacidad de la información, asegurando que las decisiones estratégicas, operativas y administrativas se tomen con base en información confiable y oportuna. Asimismo, busca minimizar las afectaciones a la operación institucional en caso de materialización de riesgos, proteger la información de pacientes y usuarios, y fortalecer la cultura organizacional de gestión del riesgo y seguridad digital en la entidad.

Para su implementación, el plan se fundamenta en la Norma ISO 31000, las Guías 7 y 8 del MINTIC sobre gestión de riesgos y controles de seguridad de la información, la Guía de Riesgos del DAFP y las directrices de la Unidad Nacional para la Gestión del Riesgo de Desastres, integrando buenas prácticas de gobierno corporativo, control interno y mejoramiento continuo.

Este instrumento considera de manera transversal los criterios de valor estratégico, criticidad de los activos de información, cumplimiento legal y reglamentario, confidencialidad, integridad y disponibilidad, así como las expectativas de los grupos de interés, permitiendo al Hospital San Juan de Dios de Yarumal contar con un marco sólido para la gestión de riesgos de seguridad y privacidad de la información, contribuyendo al logro eficiente de sus objetivos institucionales y a la protección de la información en entornos digitales y físicos.

Objetivo General

Garantizar la gestión integral de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital en el Hospital San Juan de Dios de Yarumal, mediante la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos asociados, fortaleciendo la protección de la información institucional y de los usuarios, asegurando la continuidad operativa, el cumplimiento normativo y la mejora continua de los procesos misionales, administrativos y de apoyo.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

Objetivos Específicos

- Identificar y clasificar los activos de información y procesos críticos del Hospital, estableciendo su valor estratégico y su criticidad frente a la operación institucional.
- Detectar, analizar y evaluar los riesgos asociados a la seguridad, privacidad y disponibilidad de la información, considerando factores internos y externos, amenazas, vulnerabilidades y consecuencias potenciales.
- Diseñar y aplicar controles y medidas de mitigación efectivas para reducir la probabilidad e impacto de los riesgos identificados, alineados con estándares nacionales e internacionales (ISO 31000, MINTIC, DAFP).
- Monitorear y evaluar continuamente los riesgos residuales y la efectividad de los controles implementados, asegurando la actualización del mapa de riesgos y la información para la toma de decisiones.
- Fortalecer la cultura institucional en seguridad de la información y seguridad digital, promoviendo la sensibilización, capacitación y compromiso del talento humano en la protección de los datos y sistemas de la entidad.
- Garantizar el cumplimiento de la normativa legal y reglamentaria vigente, incluyendo la protección de datos personales y la seguridad digital, reduciendo sanciones y riesgos legales para la institución.
- Establecer mecanismos de comunicación, consulta y reporte de los riesgos a los niveles directivos y operativos, para favorecer la transparencia y la toma de decisiones oportunas.

Marco Normativo

El presente plan se fundamenta en el marco legal, reglamentario y de lineamientos institucionales que garantizan la gestión de riesgos de seguridad y privacidad de la información, así como la continuidad de la operación de los procesos misionales, administrativos y de apoyo.

Constitución Política de Colombia de 1991

- Establece los principios de transparencia, publicidad y acceso a la información pública, así como el deber del Estado de garantizar la gestión eficiente de los recursos públicos y la protección de la información.
- Los artículos relativos a derechos fundamentales (por ejemplo, derecho a la información y privacidad) constituyen la base para las obligaciones de gestión de la información y seguridad digital en las entidades públicas.

Leyes

- **Ley 1581 de 2012 – Ley de Protección de Datos Personales**

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

Regula la recolección, almacenamiento, uso y circulación de datos personales, garantizando la protección de la privacidad de los ciudadanos y usuarios de los servicios de salud.

- **Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública**

Garantiza el acceso de los ciudadanos a la información pública, obligando a las entidades a mantener sistemas seguros de gestión de la información que permitan disponibilidad y consulta de los datos sin comprometer la confidencialidad.

- **Ley 1341 de 2009 – Ley de Tecnologías de Información y Comunicaciones**

Establece principios y lineamientos para el uso de tecnologías de la información en el sector público, con implicaciones directas en la seguridad de la información y la protección de los sistemas digitales.

- **Ley 1437 de 2011 – Código de Procedimiento Administrativo y de lo Contencioso Administrativo**

Contiene disposiciones que impactan la gestión de información en procesos administrativos, especialmente en el uso de tecnologías de la información para asegurar validez, integridad y conservación de los registros electrónicos.

Decretos y Reglamentos

- **Decreto 1499 de 2017**

Establece la Política de Gobierno Digital y lineamientos sobre la gestión de riesgos en entidades públicas, fortaleciendo la integración de la seguridad de la información con el Modelo Integrado de Planeación y Gestión – MIPG.

- **Decreto 612 de 2018**

Regula la integración de los planes institucionales al Plan de Acción Anual y establece directrices para la publicación de información pública, incluyendo la gestión segura de información sensible.

- **Decreto 1074 de 2015**

Reglamenta aspectos relacionados con la seguridad de la información y la gestión de sistemas tecnológicos en el sector salud, asegurando continuidad operativa y protección de datos clínicos y administrativos.

Normas Internacionales

- **ISO 31000 – Gestión de Riesgos**

Proporciona principios y directrices para la gestión de riesgos, incluyendo la identificación, análisis, evaluación y tratamiento de riesgos en organizaciones públicas.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- **ISO 27000 – Seguridad de la Información**

Define buenas prácticas para la gestión de la seguridad de la información, asegurando confidencialidad, integridad y disponibilidad de los datos.

Lineamientos y Directrices Técnicas

- **Guías 7 y 8 del Modelo de Seguridad y Privacidad de la Información – MINTIC**
Establecen la metodología de gestión de riesgos de seguridad y privacidad de la información, así como los controles que deben implementarse en las entidades públicas.
- **Guía de Riesgos – Departamento Administrativo de la Función Pública (DAFP)**
Define criterios para la identificación, evaluación, tratamiento y monitoreo de riesgos de información, alineada con la gestión institucional y el MIPG.
- **Protocolos internos del Hospital San Juan de Dios de Yarumal**
Incluyen procedimientos, controles y medidas de protección aplicables a la custodia, uso y tratamiento de información institucional y de los usuarios, asegurando la continuidad operativa y cumplimiento normativo.

Articulación con el Modelo Integrado de Planeación y Gestión – MIPG.

Dimensiones del MIPG a las que aporta el plan

El plan 2026 contribuye principalmente a las siguientes dimensiones del MIPG, manteniendo la coherencia con la planificación 2025:

- **Dimensión de Planeación**
 - Aporta a la definición de objetivos estratégicos claros y a la integración de los planes sectoriales en la planeación institucional.
 - Mantiene la continuidad con el Plan 2025, donde se establecieron lineamientos para la gestión del talento humano, la integridad institucional y la eficiencia de los recursos.
- **Dimensión de Gestión y Desempeño**
 - Fortalece la ejecución, seguimiento y evaluación de los procesos institucionales, garantizando la articulación con los objetivos estratégicos y los indicadores de gestión, resultado, producto e impacto definidos en 2025.
- **Dimensión de Control y Evaluación**

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- Permite establecer mecanismos de supervisión y seguimiento, asegurando que las acciones planificadas se ajusten a los objetivos estratégicos y cumplan con la normatividad vigente, tal como se venía aplicando en la versión del plan 2025.

Políticas de gestión y desempeño institucional relacionadas

El plan 2026 mantiene la relación con las siguientes políticas y lineamientos institucionales, en continuidad con el plan 2025:

- **Política de Planeación Institucional:** asegura que los objetivos y acciones del plan estén alineados con la estrategia institucional.
- **Política de Talento Humano:** garantiza que la gestión del personal y los programas de bienestar se articulen con los objetivos del plan, tal como se implementó en 2025.
- **Política de Integridad:** contribuye al fortalecimiento de la ética, la transparencia y la gestión eficiente de los recursos públicos.
- **Política de Gestión Documental y Tecnologías de la Información:** asegura la disponibilidad, seguridad y trazabilidad de la información utilizada en la ejecución del plan.

Contribución del plan al cumplimiento de los objetivos estratégicos institucionales

El Plan 2026 se articula con los objetivos estratégicos definidos en 2025, garantizando continuidad y coherencia en la gestión institucional:

- **Optimización de los procesos internos:** consolidando los procedimientos y protocolos establecidos en el plan anterior.
- **Fortalecimiento del control y seguimiento institucional:** mediante la implementación de indicadores de gestión y mecanismos de evaluación que retoman los aprendizajes y resultados del plan 2025.
- **Mejora del bienestar y desempeño del talento humano:** alineado con las estrategias de incentivos y bienestar definidas en el plan 2025.
- **Garantía de integridad, transparencia y cumplimiento normativo:** reforzando los lineamientos de gestión documental, acceso a la información y seguridad de los datos establecidos previamente.

Alcance

El Plan 2026 se aplica a todas las áreas, dependencias y procesos de la ESE Hospital San Juan de Dios de Yarumal que participan en la gestión institucional, la planeación

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

estratégica, el seguimiento de los objetivos y la ejecución de programas de bienestar y estímulos para el talento humano, así como la implementación de instrumentos de gestión documental y tecnológica.

Dependencias involucradas

El plan compromete la coordinación y participación activa de:

- Dirección General
- Subdirección Administrativa y Financiera
- Área de Talento Humano
- Área de Planeación y Control Interno
- Área de Tecnologías de la Información
- Coordinaciones de Servicios de Salud
- Otras dependencias que participen en la ejecución de los programas, proyectos o procesos relacionados con los objetivos del plan

Población objetivo

- **Interna:** Todo el personal vinculado a la ESE, incluyendo directivos, administrativos, profesionales de la salud, técnicos y operativos.
- **Externa** (cuando aplique): Ciudadanía beneficiaria de los servicios institucionales y usuarios de los programas de gestión documental, acceso a la información y bienestar.

Responsables

Dependencia líder del plan

- **Dirección General del Hospital San Juan de Dios de Yarumal** responsable de la coordinación global del plan, de garantizar la asignación de recursos, de supervisar la ejecución de actividades estratégicas y de evaluar el cumplimiento de objetivos a nivel institucional.

Dependencias de apoyo

- **Subdirección Administrativa y Financiera:** Brinda soporte en la planificación de recursos, control presupuestal y ejecución financiera del plan.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- **Área de Talento Humano:** Gestiona la capacitación, sensibilización y participación del personal en los programas definidos por el plan, asegurando el cumplimiento de los objetivos relacionados con bienestar, incentivos y seguridad de la información.
- **Área de Planeación y Control Interno:** Realiza el seguimiento, evaluación y reporte de avances del plan, asegurando la coherencia con el MIPG, los lineamientos normativos y la mejora continua.
- **Área de Tecnologías de la Información:** Garantiza el soporte técnico para la implementación de herramientas digitales, sistemas de gestión documental y monitoreo de riesgos de seguridad y privacidad de la información.
- **Coordinaciones de Servicios de Salud y otras áreas operativas:** Participan en la implementación de acciones específicas según sus procesos misionales y la interacción con los usuarios.

Roles y responsabilidades generales

Rol	Responsabilidad principal	Dependencia asignada
Líder del plan	Supervisar la ejecución del plan, coordinar dependencias y asegurar cumplimiento de metas	Gerencia
Responsable de seguimiento	Monitorear indicadores, elaborar informes y proponer ajustes	Planeación y Control Interno
Responsable de recursos	Gestionar los recursos humanos, técnicos y financieros necesarios	Subgerencia Administrativa y Financiera
Responsable de ejecución operativa	Implementar acciones específicas de acuerdo con las líneas de acción del plan	Áreas misionales y soporte (Talento Humano, TIC, Servicios de Salud)

Diagnóstico

Situación institucional vigente

La ESE Hospital San Juan de Dios de Yarumal ha venido fortaleciendo sus sistemas de gestión institucional y planificación estratégica, incluyendo la implementación de instrumentos como el Plan Institucional de Archivos (PINAR), el Plan de Talento Humano, y otros planes sectoriales alineados al MIPG.

En la vigencia 2025, se evidenció un avance significativo en:

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- La organización de la información y gestión documental institucional, con actualización de instrumentos archivísticos y procedimientos de gestión.
- La formalización de estrategias de bienestar, incentivos y desarrollo del talento humano.
- La consolidación de procedimientos internos de control, seguimiento y evaluación de riesgos operativos y financieros.

No obstante, se identifican oportunidades de mejora en:

- Integración transversal de los planes institucionales en los procesos operativos del hospital.
- Actualización permanente de procedimientos de gestión documental frente a la normatividad vigente.
- Fortalecimiento de mecanismos de seguimiento y evaluación de indicadores de desempeño en todas las áreas.

Resultados de evaluaciones internas y externas

- **Auditorías internas:** Han identificado inconsistencias en la depuración y conciliación de información contable y documental, así como la necesidad de reforzar los controles en los procesos críticos.
- **Auditorías externas y observaciones de control:** La Contraloría General de Antioquia reportó deficiencias en procedimientos de supervisión contable y presupuestal, las cuales fueron parcialmente subsanadas mediante la actualización de conciliaciones y registros contables.
- **Evaluación de desempeño institucional:** Los indicadores de gestión muestran avances en cumplimiento de metas, pero persisten brechas en la documentación formal de procesos y la estandarización de registros digitales.

Hallazgos de órganos de control

- Falta de actualización en la clasificación documental y en la implementación completa de tablas de retención.
- Procesos de conciliación contable y financiera que requieren formalización y sistematización.
- Necesidad de reforzar la trazabilidad y disponibilidad de información para auditorías y seguimiento del MIPG.

Necesidades identificadas

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- **Gestión documental:** Consolidar el PINAR y demás instrumentos archivísticos, garantizando la articulación con los planes de acción y la planificación estratégica.
- **Talento humano:** Fortalecer programas de capacitación, incentivos y bienestar para asegurar la participación activa del personal en los planes institucionales.
- **Seguimiento y evaluación:** Implementar mecanismos más robustos de monitoreo de indicadores de desempeño, gestión y resultados para cada plan, alineados al MIPG.
- **Integración institucional:** Mejorar la coordinación interdependencias para garantizar que los planes sectoriales y estratégicos se ejecuten de manera coherente y eficiente.

Este diagnóstico no solo refleja la continuidad con el Plan 2025, sino que fundamenta técnicamente la formulación del Plan 2026, identificando claramente los avances y las brechas que se deben subsanar en la nueva vigencia.

Estrategias y líneas de acción

Estrategias institucionales

Las estrategias definen los enfoques prioritarios para gestionar los riesgos de seguridad y privacidad de la información, asegurando la protección de los activos de información y la continuidad de las operaciones del Hospital San Juan de Dios de Yarumal. Las principales estrategias son:

Prevención y reducción de riesgos tecnológicos y operativos

- Fortalecer la infraestructura tecnológica y la actualización de software y hardware críticos.
- Implementar controles de acceso, permisos y medidas de seguridad en los sistemas de información.
- Garantizar copias de seguridad y planes de recuperación ante desastres.

Gestión integral de riesgos de información y seguridad digital

- Mantener la identificación, evaluación y tratamiento de los riesgos en todos los procesos de la institución.
- Implementar controles preventivos, correctivos y de monitoreo para minimizar la ocurrencia de eventos adversos.
- Aplicar la metodología “Guía de Riesgos” del DAFP y la normativa ISO 31000 para la gestión de riesgos.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

Fortalecimiento de capacidades institucionales y talento humano

- Capacitar al personal en buenas prácticas de seguridad y privacidad de la información.
- Socializar protocolos, procedimientos y políticas de seguridad digital en todas las áreas.
- Promover la cultura de gestión de riesgos y responsabilidad compartida entre líderes y colaboradores.

Monitoreo, seguimiento y mejora continua

- Implementar indicadores de gestión, producto, resultado e impacto para evaluar la efectividad de las medidas de control.
- Establecer informes periódicos de evaluación de riesgos y seguimiento por parte de Control Interno.
- Revisar y actualizar periódicamente el plan de tratamiento de riesgos conforme a nuevas amenazas, brechas y cambios normativos.

Líneas de acción

Las líneas de acción concretan las estrategias anteriores en actividades operativas, responsables y frecuencia de ejecución:

Identificación y valoración de riesgos

- Actualizar el inventario de activos de información críticos.
- Evaluar vulnerabilidades y amenazas tecnológicas y operativas.
- Clasificar los riesgos según probabilidad e impacto.

Implementación de controles y medidas preventivas

- Configurar sistemas de control de accesos y autenticación segura.
- Mantener infraestructura tecnológica con planes de mantenimiento y actualización.
- Generar copias de seguridad periódicas y pruebas de restauración.

Capacitación y sensibilización del personal

- Programar capacitaciones en manejo seguro de información y protocolos de privacidad.
- Difundir políticas de seguridad digital y privacidad de datos.
- Evaluar la adherencia de los colaboradores a los procedimientos de seguridad.

Monitoreo y seguimiento

- Registrar incidentes y evaluar su impacto en la operación.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05
			FECHA: 24/01/2026

- Medir la efectividad de los controles aplicados mediante indicadores específicos (riesgo residual, nivel de madurez de la gestión de riesgos).
- Ajustar las acciones de mitigación según resultados y nuevas evaluaciones de riesgo.

Planes de contingencia y respuesta ante incidentes

- Establecer procedimientos de recuperación ante interrupciones de sistemas críticos.
- Definir roles y responsabilidades ante incidentes de seguridad.
- Probar periódicamente los planes de contingencia y actualizar lecciones aprendidas.

Plan de Acción

Estrategia	Actividad	Responsable	Fecha Inicio	Fecha Final	Producto/Entregable	Indicador
Prevención y reducción de riesgos tecnológicos y operativos	Actualización de software crítico y sistemas operativos	Área de Tecnología	01/03/2026	31/05/2026	Sistemas y aplicaciones actualizados	% de sistemas actualizados vs planificados
Prevención y reducción de riesgos tecnológicos y operativos	Actualización de hardware y dispositivos de seguridad	Área de Tecnología	01/03/2026	30/06/2026	Inventario de equipos actualizado	% de equipos actualizados vs planificados
Prevención y reducción de riesgos tecnológicos y operativos	Configuración de controles de acceso y autenticación multifactor	Área de Tecnología	01/03/2026	30/04/2026	Sistema con permisos y accesos controlados	% de usuarios con acceso adecuado
Gestión integral de riesgos de información	Identificación y evaluación periódica de riesgos de seguridad y privacidad	Coordinador de Riesgos	01/03/2026	31/12/2026	Informe de riesgos actualizado	Número de riesgos identificados y evaluados
Gestión integral de riesgos de información	Implementación de controles preventivos, correctivos y de monitoreo	Todas las áreas involucradas	01/03/2026	31/12/2026	Registro de controles implementados	% de controles implementados efectivamente
Gestión integral de riesgos de información	Pruebas de respaldo y recuperación de información crítica	Área de Tecnología	01/04/2026	30/06/2026	Informe de pruebas de recuperación	% de pruebas satisfactorias vs programadas
Fortalecimiento de	Capacitación en seguridad	Talento Humano	01/04/2026	30/06/2026	Registro de asistencias y	% de personal

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

capacidades institucionales	y privacidad de la información para todo el personal				evidencia de capacitación	capacitado vs total
Fortalecimiento de capacidades institucionales	Socialización de políticas, procedimientos y protocolos de seguridad	Coordinador de Riesgos	01/03/2026	30/09/2026	Actas de socialización y participación	Número de áreas socializadas / total de áreas
Monitoreo, seguimiento y mejora continua	Monitoreo de indicadores de riesgo y control en seguridad de la información	Control Interno	01/03/2026	31/12/2026	Informes periódicos de seguimiento	Número de informes entregados vs planificados
Monitoreo, seguimiento y mejora continua	Ajuste del plan de tratamiento de riesgos según hallazgos y nuevas evaluaciones	Coordinador de Riesgos	01/07/2026	31/12/2026	Plan de acción actualizado	Número de ajustes realizados
Monitoreo, seguimiento y mejora continua	Auditoría interna y externa de seguridad de la información	Control Interno / Auditoría externa	01/09/2026	31/12/2026	Informe de auditoría y recomendaciones	Número de hallazgos corregidos
Prevención de incidentes de seguridad	Implementación de mecanismos de detección y respuesta ante incidentes	Área de Tecnología	01/03/2026	31/12/2026	Registro de incidentes y acciones correctivas	Tiempo promedio de respuesta ante incidentes
Prevención de incidentes de seguridad	Actualización de planes de contingencia y continuidad del negocio	Coordinador de Riesgos	01/05/2026	30/09/2026	Plan de contingencia actualizado	% de pruebas exitosas de contingencia
Fortalecimiento de cultura de seguridad	Campañas de sensibilización sobre seguridad de la información y privacidad de datos	Talento Humano	01/03/2026	31/12/2026	Materiales de campaña, evidencias de difusión	Número de campañas realizadas / programadas

Indicadores

INDICADORES DE GESTIÓN

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
% de actividades ejecutadas según el plan de acción	$(\text{Número de actividades ejecutadas} / \text{Número de actividades programadas}) \times 100$	Trimestral	Informe de seguimiento del plan de acción	100%
% de capacitación completada del personal en seguridad de la información	$(\text{Número de empleados capacitados} / \text{Total de empleados programados}) \times 100$	Semestral	Registro de asistencia a capacitaciones	95%
% de socializaciones realizadas en las áreas	$(\text{Número de áreas con socialización} / \text{Total de áreas}) \times 100$	Semestral	Actas de socialización	100%

INDICADORES DE RESULTADO

INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Número de sistemas actualizados	Conteo de sistemas actualizados según inventario	Semestral	Inventario de sistemas	Todos los sistemas críticos actualizados
Número de planes de contingencia actualizados	Conteo de planes revisados y actualizados	Anual	Planes de contingencia institucional	100% de planes actualizados
Número de pruebas de recuperación de información realizadas	Conteo de pruebas completadas	Semestral	Informe de pruebas	100% de pruebas satisfactorias

INDICADORES DE PRODUCTO

INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Reducción de incidentes de seguridad de la información	$((\text{Incidentes año anterior} - \text{Incidentes año actual}) / \text{Incidentes año anterior}) \times 100$	Anual	Registro de incidentes	Reducción $\geq$ 20%
Cumplimiento de controles implementados	(Controles implementados efectivamente /	Semestral	Registro de controles	95%

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

	Total de controles planificados) $\times$ 100			
Nivel de cumplimiento de políticas y protocolos	(Número de áreas cumpliendo políticas / Total de áreas) $\times$ 100	Semestral	Auditorías internas	100%
INDICADORES DE IMPACTO				
INDICADOR	FÓRMULA	FRECUENCIA	FUENTE DE VERIFICACIÓN	META SUGERIDA
Nivel de madurez en seguridad de la información	Evaluación del índice de madurez según metodología institucional	Anual	Informe de madurez de seguridad	Nivel alto ($\geq$ 80%)
Confianza y percepción de seguridad digital en la institución	Encuesta interna sobre percepción de seguridad de la información	Anual	Resultados de encuestas internas	$\geq$ 85% de aceptación
Cumplimiento de normatividad de seguridad y privacidad	(Número de requisitos normativos cumplidos / Total de requisitos aplicables) $\times$ 100	Anual	Informes de auditoría y control	100% cumplimiento

Recursos

La implementación del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información y Seguridad Digital 2026 requiere la asignación adecuada de recursos humanos, financieros y técnicos para garantizar su correcta ejecución, seguimiento y sostenibilidad, asegurando que todas las dependencias involucradas puedan cumplir con sus responsabilidades en la gestión de seguridad y privacidad de la información institucional.

Recursos humanos

- **Coordinador de Seguridad de la Información:** Lidera la ejecución y seguimiento del plan, coordina equipos y reporta resultados.
- **Analistas de Seguridad de la Información:** Monitoreo de riesgos, implementación de controles y reporte de incidentes.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- **Especialistas en Tecnologías de la Información:** Soporte técnico en infraestructura, actualización de sistemas y pruebas de recuperación ante incidentes.
- **Responsable de Formación y Capacitación:** Planea y ejecuta programas de sensibilización y formación del personal en seguridad digital y protección de datos.
- **Personal operativo y usuarios finales:** Cumplimiento de políticas y participación en capacitaciones, pruebas y protocolos establecidos.

Recursos financieros

- Presupuesto destinado a la adquisición y actualización de herramientas y sistemas de seguridad de la información.
- Recursos para la capacitación y sensibilización del personal en seguridad digital y manejo seguro de la información.
- Fondos para auditorías internas, pruebas de recuperación de información y consultorías externas especializadas en ciberseguridad.
- Recursos para la documentación, elaboración de protocolos y actualización de manuales de seguridad digital.

Recursos técnicos y tecnológicos

- **Sistemas de gestión de seguridad y protección de datos:** Monitoreo de incidentes, control de accesos, cifrado y supervisión de la información.
- **Infraestructura tecnológica segura:** Servidores, almacenamiento protegido, herramientas de respaldo y recuperación ante incidentes.
- **Plataformas de capacitación digital:** Para formación continua del personal en seguridad de la información y privacidad de datos.
- **Documentación y protocolos institucionales:** Guías, procedimientos y formatos que soportan la implementación y seguimiento del plan.

Seguimiento y evaluación

El seguimiento y evaluación del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información y Seguridad Digital 2026 se realizará mediante un mecanismo institucional estructurado que garantice la verificación periódica de avances, el cumplimiento de las metas establecidas y la implementación de acciones de mejora continua.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

- **Seguimiento periódico:** Se definirán reuniones de seguimiento mensuales y trimestrales entre el equipo responsable del plan y las dependencias involucradas, con el fin de evaluar el estado de las actividades, la implementación de controles y la identificación de desviaciones respecto al plan original.
- **Evaluación de avances y cumplimiento:** Se establecerán indicadores de gestión, producto, resultado e impacto para medir de manera objetiva la ejecución del plan. Los resultados se consolidarán en informes periódicos que reflejen el progreso en la mitigación de riesgos de seguridad y privacidad de la información.
- **Reporte a alta dirección y entes de control:** Los hallazgos, resultados y recomendaciones se presentarán a la alta dirección institucional, asegurando la visibilidad del cumplimiento del plan y su alineación con los objetivos estratégicos. Adicionalmente, se suministrará información a los entes de control cuando sea requerida, garantizando transparencia y trazabilidad de los procesos.
- **Acciones de mejora:** Con base en los resultados del seguimiento y la evaluación, se implementarán ajustes y acciones correctivas oportunas para optimizar la gestión de riesgos de seguridad y privacidad de la información, incluyendo la actualización de protocolos, capacitación del personal y refuerzo de controles tecnológicos y administrativos.

Este mecanismo asegura que el plan se mantenga dinámico, adaptándose a nuevos riesgos y necesidades, y fortalece la cultura institucional de gestión de la seguridad de la información.

Riesgos asociados al Plan

La implementación del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información y Seguridad Digital 2026 está sujeta a la identificación de riesgos que podrían afectar la consecución de sus objetivos. Estos riesgos se articulan con el Sistema de Control Interno y se gestionan mediante acciones de mitigación estructuradas y verificables.

Principales Riesgos y medidas de mitigación

Riesgo	Causas	Consecuencias	Acciones de Mitigación	Responsable
Acceso no autorizado a información sensible	Falta de controles de acceso, credenciales compartidas, dispositivos	Pérdida de confidencialidad, sanciones legales, afectación a la reputación	Implementar políticas estrictas de control de acceso, autenticación multifactor y	Coordinación de TI / Oficina de Seguridad de la Información

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

	inseguros	institucional	registro de accesos	
Pérdida o corrupción de datos electrónicos	Fallas en sistemas tecnológicos, falta de respaldos periódicos, ataques cibernéticos	Interrupción de operaciones, pérdida de información crítica	Realizar respaldos automáticos y periódicos, monitoreo de integridad de la información y actualización de sistemas de seguridad	Coordinación de TI / Archivo y Gestión Documental
Incumplimiento de normatividad y estándares de seguridad	Desconocimiento de lineamientos, falta de capacitación, ausencia de auditorías	Multas, sanciones, deterioro de la confianza institucional	Capacitación continua, auditorías internas, alineación de procedimientos con la legislación vigente	Oficina Jurídica / Coordinación de TI
Fallas en infraestructura tecnológica	Obsolescencia de equipos, interrupciones de red, vulnerabilidades sin parchear	Interrupción de servicios, afectación de procesos críticos	Actualización de infraestructura, monitoreo preventivo, plan de contingencia tecnológica	Coordinación de TI / Gerencia
Riesgo humano (errores o negligencia del personal)	Falta de entrenamiento, baja sensibilización en seguridad	Exposición de información, vulneración de políticas internas	Programas de formación y sensibilización, procedimientos claros y supervisión constante	Talento Humano / Coordinación de TI
Pérdida o deterioro de documentos físicos	Falta de almacenamiento adecuado, humedad, manipulación inadecuada	Pérdida de información, afectación de la memoria institucional, incumplimiento normativo	Implementar condiciones óptimas de almacenamiento, controlar humedad y temperatura, capacitar al personal	Archivo y Gestión Documental / Dirección Administrativa
Incumplimiento de normatividad	Desconocimiento de la normativa, falta de	Sanciones de entes de control, riesgos legales	Capacitar al personal, actualizar	Archivo y Gestión Documental /

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05 FECHA: 24/01/2026

archivística	actualización de TRD y TVD		instrumentos archivísticos y procedimientos, realizar auditorías internas	Oficina Jurídica
Resistencia al cambio por parte del personal	Falta de sensibilización o formación	Aplicación parcial de los procedimientos, incumplimiento del plan	Programas de capacitación, campañas de sensibilización y acompañamiento durante la implementación	Talento Humano / Archivo y Gestión Documental
Falta de recursos financieros o tecnológicos	Limitaciones presupuestales, retrasos en asignación de recursos	Retraso en implementación de sistemas, infraestructura y actividades del plan	Planificación presupuestal anual, priorización de recursos críticos, seguimiento de inversión	Gerencia
Deficiencias en seguimiento y control	Falta de indicadores claros o de monitoreo periódico	Dificultad para medir avances, identificar hallazgos y aplicar mejoras	Establecer indicadores de gestión, producto, resultado e impacto, y calendarizar revisiones periódicas	Archivo y Gestión Documental / Subgerencia Administrativa

Vigencia

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital tendrá vigencia durante el año 2026, iniciando el 1 de enero y finalizando el 31 de diciembre de 2026.

Se prevé que, dentro de este período, el plan podrá actualizarse o ajustarse en función de:

- Resultados del seguimiento y evaluación periódica.
- Cambios en la normatividad vigente o lineamientos institucionales.
- Identificación de nuevos riesgos o modificaciones en los riesgos existentes.

	E.S.E HOSPITAL YARUMAL SAN JUAN DE DIOS NIT 890.980.726.6		
	PLAN DE TRATAMIENTO DE RIESGOS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO GESTIÓN INSTITUCIONAL	CÓDIGO: PL-01-011
			VERSIÓN: 05
			FECHA: 24/01/2026

- Necesidades emergentes derivadas de la gestión operativa y tecnológica de la entidad.

La actualización del plan deberá realizarse de manera formal y documentada, garantizando que los responsables del seguimiento y la alta dirección estén informados de los ajustes realizados, asegurando la continuidad y pertinencia de las acciones del plan durante su vigencia.

Modificaciones

Versión	Fecha	Paginas Afectadas	Descripción del cambio
01	30/04/2019		Creación del documento
02	03/01/2022	Todo el documento	Actualización del contenido
03	04/01/2023	Todo el documento	Actualización y revisión del contenido
04	31/01/2025	Todo el documento	Actualización y revisión del contenido
05	24/01/2026	Todo el documento	Actualización y revisión del contenido

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