

**PLAN ESTRATÉGICO DE TRATAMIENTO DE RIESGOS DE SEGURIDAD
Y PRIVACIDAD DE LA INFORMACIÓN**



Elaboró:

Pedro Alejandro Bonilla Valencia

Profesional SGSI de Administración y Almacenamiento de la información Afiliado
participe Assesalud.oc

Revisó:

Juan David Uribe Ordoñez

Coordinador de Administración y Almacenamiento de la información - Afiliado
participe Assesalud.oc

Martha Isabel Andrade Jiménez

Subgerente Administrativo y Financiero Gr-1

Aprobó:

JUAN CARLOS ARTEAGA CIFUENTES

Gerente HUSJ

POPAYAN, 2026

Contenido

1. INTRODUCCIÓN	3
2. JUSTIFICACIÓN	3
3. MARCO NORMATIVO Y POLÍTICO	3
4. OBJETIVOS	5
4.1 OBJETIVO GENERAL	5
4.2 OBJETIVO ESPECIFICOS	5
5. ALINEACIÓN ESTRATÉGICA	6
6. DIAGNÓSTICO INSTITUCIONAL DEL PLAN ESTRATÉGICO	6
7. PROGRAMAS DERIVADOS DEL PLAN ESTRATÉGICO	6
8. METODOLOGÍAS Y ESTRATEGIAS	7
Metodologías	7
9. DETECCION DE DESVIACIONES	8
10. EVALUACIÓN Y SEGUIMIENTO	8
11. CONCLUSIONES Y PRÓXIMOS PASOS	10
11.1. Resumen de puntos clave	10
11.2. Recomendaciones y acciones a seguir	11
12. ANEXOS	11
13. TABLA DE CONTROL DE REGISTROS	12
14. CONTROL DE CAMBIOS	12

1. INTRODUCCIÓN

La gestión de los riesgos de seguridad y privacidad de la información constituye un elemento fundamental para la protección de los activos de información y la continuidad de los servicios del Hospital Universitario San José de Popayán ESE. En un entorno digital caracterizado por el incremento de amenazas cibernéticas, la dependencia de los sistemas de información y el tratamiento intensivo de datos personales y sensibles, resulta indispensable contar con un plan que permita identificar, evaluar y tratar de manera sistemática los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece los lineamientos, metodologías y estrategias para la gestión del riesgo, en coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27005 y la normatividad vigente, contribuyendo a la protección de la información institucional y al cumplimiento de los objetivos misionales del Hospital.

2. JUSTIFICACIÓN

La formulación e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se justifica en la necesidad de gestionar de manera preventiva y controlada los riesgos que puedan generar afectaciones a los procesos misionales y de apoyo del Hospital, comprometer la atención en salud, vulnerar la confidencialidad de la historia clínica y generar incumplimientos normativos.

Este plan permite priorizar los riesgos, definir acciones de tratamiento, reducir su impacto y probabilidad, y establecer mecanismos de seguimiento que faciliten la toma de decisiones informadas, fortaleciendo la resiliencia institucional y la sostenibilidad operativa.

3. MARCO NORMATIVO Y POLÍTICO

El Plan Estratégico de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se fundamenta en el marco normativo y en los lineamientos técnicos vigentes que regulan la gestión de riesgos, la protección de la información, los datos personales y la seguridad digital en las entidades públicas del sector salud.

A continuación, se presenta la normatividad vigente que sustenta la formulación, implementación y seguimiento del presente plan estratégico.

**PLAN ESTRATÉGICO DE
TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

Código: PLA-AAI-05

Versión: 01

Página 4 de 13



	NORMA	EXPEDIDA POR	DESCRIPCIÓN
1	Constitución Política de Colombia (1991)	Congreso de la República	Establece los derechos fundamentales, incluido el derecho a la intimidad y el habeas data.
2	Ley 1581 de 2012	Congreso de la República	Por la cual se dictan disposiciones generales para la protección de datos personales.
3	Ley 23 de 1981	Congreso de la República	Normas en materia de ética médica que regulan la confidencialidad de la información del paciente.
4	Ley 527 de 1999	Congreso de la República	Define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales.
5	Decreto 1377 de 2013	Presidencia de la República	Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales.
6	ISO/IEC 27001:2013 (adoptada en Colombia como NTC-ISO/IEC 27001:2013)	ICONTEC	Norma que especifica los requisitos para un sistema de gestión de seguridad de la información.
7	ISO/IEC 27005: Gestión del riesgo de seguridad de la información	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)	Norma que proporciona directrices para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, como apoyo a la ISO/IEC 27001.

8	Modelo de Seguridad y Privacidad de la Información (MSPI)	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Establece lineamientos, buenas prácticas y controles para gestionar la seguridad y privacidad de la información en las entidades públicas, alineado con estándares internacionales.
9	Resolución 1995 de 1999	Ministerio de Salud y Protección Social	Reglamenta el manejo de la historia clínica.
10	Circular Externa 005 de 2017	Superintendencia de Industria y Comercio	Instrucciones sobre la implementación de medidas para la protección de datos personales.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Gestionar y tratar de manera sistemática los riesgos de seguridad y privacidad de la información del Hospital Universitario San José de Popayán ESE, reduciéndolos a niveles aceptables y garantizando la protección de los activos de información y la continuidad de los servicios.

4.2 OBJETIVO ESPECIFICOS

- Identificar los riesgos de seguridad y privacidad que afectan los activos de información.
- Evaluar los riesgos en términos de impacto y probabilidad.
- Definir y ejecutar acciones de tratamiento para los riesgos identificados.
- Gestionar y documentar el riesgo residual.
- Realizar seguimiento y actualización periódica del tratamiento de riesgos.

5. ALINEACIÓN ESTRATÉGICA

El presente plan se encuentra alineado con la Política de Seguridad Digital del Hospital, el Plan de Desarrollo Institucional, el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando coherencia con el direccionamiento estratégico y los objetivos misionales de la entidad. Esta alineación permite articular la gestión de la seguridad y privacidad de la información con los procesos institucionales, la administración del riesgo y la mejora continua, contribuyendo al fortalecimiento del buen gobierno, la sostenibilidad institucional y la protección de los activos estratégicos de información. Asimismo, el plan promueve el cumplimiento de la normatividad vigente, la continuidad de los servicios y la confianza de los usuarios y demás partes interesadas.

6. DIAGNÓSTICO INSTITUCIONAL DEL PLAN ESTRATÉGICO

El diagnóstico institucional del Plan Estratégico de Tratamiento de Riesgos de Seguridad y Privacidad de la Información permite identificar el estado actual de la gestión de la seguridad de la información y la protección de los datos personales en el Hospital, teniendo en cuenta los procesos, los sistemas de información y el cumplimiento normativo vigente.

Este análisis evidencia la existencia de riesgos asociados al acceso a la información, al tratamiento de datos personales y datos sensibles, a la gestión de incidentes de seguridad y a la dependencia de los activos tecnológicos, así como la necesidad de fortalecer la cultura organizacional en seguridad y privacidad de la información.

El diagnóstico sirve como base para definir las estrategias y acciones del plan, orientadas a mejorar el tratamiento de los riesgos identificados y a fortalecer la protección de los activos de información, en coherencia con la Política de Seguridad Digital y los lineamientos institucionales

7. PROGRAMAS DERIVADOS DEL PLAN ESTRATÉGICO

N/A

8. METODOLOGÍAS Y ESTRATEGIAS

El Plan Estratégico de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se implementará mediante metodologías y estrategias orientadas a una gestión sistemática, continua y basada en riesgos, en coherencia con la Política de Seguridad Digital, el direccionamiento estratégico institucional y la normatividad vigente.

Metodologías

- **ISO/IEC 27001:** Como marco metodológico para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), con enfoque basado en riesgos.
- **ISO/IEC 27002 – Controles de Seguridad de la Información** Referente de buenas prácticas y controles técnicos, administrativos y organizacionales que apoyan la implementación del SGSI y el fortalecimiento de la seguridad digital institucional.
- **ISO/IEC 27005:** Como metodología para la gestión del riesgo de seguridad de la información, orientada a la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Como lineamiento técnico para la gestión de la seguridad y privacidad de la información en entidades públicas, en coherencia con la gestión del riesgo institucional.

Estrategias

- Identificación periódica de los riesgos de seguridad y privacidad de la información asociados a los procesos, sistemas y activos de información del Hospital.
- Implementación de controles para el tratamiento de los riesgos, mediante la aplicación de medidas administrativas, técnicas y organizacionales que permitan reducir los niveles de riesgo identificados.
- Documentación y aceptación del riesgo residual, una vez aplicados los controles definidos, conforme a los criterios institucionales de aceptación del riesgo.

- Actualización continua de la matriz de riesgos, incorporando cambios normativos, tecnológicos, organizacionales e incidentes de seguridad relevantes.

9. DETECCION DE DESVIACIONES

La detección de desviaciones del Plan Estratégico de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizará a través de los siguientes mecanismos:

- Revisión periódica de la matriz de riesgos, para identificar variaciones en el nivel de riesgo, riesgos emergentes o riesgos no tratados adecuadamente.
- Análisis de los indicadores definidos, con el fin de detectar desviaciones frente a las metas establecidas y al comportamiento esperado de los riesgos.
- Evaluación del estado de los controles implementados, verificando su efectividad y el nivel de cumplimiento frente a los riesgos identificados.
- Seguimiento a los incidentes de seguridad de la información, considerando su impacto como un indicador de desviaciones en el tratamiento de los riesgos.
- Revisión de los resultados de auditorías internas y externas, que puedan evidenciar debilidades o incumplimientos en la gestión de riesgos de seguridad y privacidad de la información.
- Identificación de cambios normativos, tecnológicos u organizacionales, que puedan modificar el contexto del riesgo y requieran ajustes en su tratamiento.

La identificación de desviaciones permitirá actualizar el análisis y tratamiento de los riesgos, fortalecer los controles existentes y aplicar acciones de mejora, conforme al ciclo de mejora continua del plan.

10. EVALUACIÓN Y SEGUIMIENTO

10.1. Mecanismos de Seguimiento

El seguimiento al Plan Estratégico de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizará mediante mecanismos que permitan verificar periódicamente la adecuada gestión de los riesgos, el avance en la

implementación de los controles definidos y la efectividad de las estrategias establecidas.

Los mecanismos de seguimiento serán:

- Seguimiento al Plan de Acción del tratamiento de riesgos, mediante la revisión periódica del cumplimiento de las actividades, responsables y cronogramas definidos.
- Monitoreo de los indicadores de riesgos, definidos en la Política de Seguridad Digital y en el Plan de Tratamiento de Riesgos, para medir el nivel de avance y efectividad de los controles implementados.
- Revisión periódica de la matriz de riesgos, con el fin de verificar la vigencia de los riesgos identificados, los niveles de riesgo residual y la necesidad de ajustes en su tratamiento.
- Seguimiento a los incidentes de seguridad de la información, como insumo para evaluar la efectividad del tratamiento de los riesgos y detectar nuevas amenazas o vulnerabilidades.
- Revisión de auditorías internas y externas, relacionadas con la gestión de riesgos, la seguridad de la información y la protección de datos personales.
- Articulación con los mecanismos de seguimiento del MIPG, garantizando coherencia con la gestión del riesgo institucional y la planeación estratégica.

10.2. Indicadores del Plan

El seguimiento se realizará semestralmente por la Oficina Asesora de Planeación y el Comité de Gestión y Desempeño, a través de indicadores definidos en el Plan de Acción del Tratamiento de riesgos de seguridad y privacidad de la información

10.3. Frecuencia de Evaluación del PLAN DE ACCIÓN (Formato Anexo)

La evaluación del Plan de Acción del Tratamiento de riesgos de seguridad y privacidad de la información se realizará de manera periódica, con el fin de verificar el avance en la ejecución de las actividades, el cumplimiento de los indicadores definidos y la efectividad de las estrategias establecidas en el Plan Estratégico.

11. CONCLUSIONES Y PRÓXIMOS PASOS

11.1. Resumen de puntos clave

- La entidad cuenta con una matriz de riesgos de seguridad y privacidad de la información que permite identificar, analizar y priorizar los riesgos asociados a los activos de información, considerando amenazas, vulnerabilidades, impacto y probabilidad.
- Se definieron lineamientos institucionales claros orientados a fortalecer la identificación de riesgos, el tratamiento mediante controles adecuados, la documentación del riesgo residual y la actualización continua de la matriz de riesgos.
- El Plan de Tratamiento de Riesgos establece controles técnicos, administrativos y físicos alineados con buenas prácticas y referentes como ISO/IEC 27001, con responsables y plazos definidos para su implementación.
- Se identificó la necesidad de documentar explícitamente el riesgo residual, como resultado de la aplicación de controles, garantizando la trazabilidad entre riesgos, controles y decisiones de aceptación.
- Se establecieron indicadores de seguimiento que permiten medir el nivel de cumplimiento de los lineamientos del tratamiento de riesgos de seguridad y privacidad de la información y la efectividad de las acciones implementadas, con frecuencias de evaluación definidas (anual y trimestral).
- El Plan Estratégico promueve la mejora continua de la gestión de la seguridad y privacidad de la información, asegurando que los riesgos se mantengan en niveles aceptables y alineados con los objetivos institucionales.
- Se refuerza la importancia de la articulación entre política, plan de acción, indicadores y seguimiento, como elementos clave para la sostenibilidad del sistema de gestión de seguridad de la información.

11.2. Recomendaciones y acciones a seguir

- **Mantener actualizada la matriz de riesgos**, incorporando de manera sistemática los cambios normativos, tecnológicos, organizacionales y los incidentes de seguridad relevantes, como insumo clave para la toma de decisiones estratégicas.
- **Fortalecer la documentación y gestión del riesgo residual**, garantizando que los riesgos tratados cuenten con una reevaluación posterior a la aplicación de controles y con una decisión formal de aceptación cuando corresponda.
- **Asegurar la implementación progresiva y priorizada de los controles definidos en el Plan de Tratamiento de Riesgos**, orientando los recursos hacia la reducción de los riesgos con mayor impacto para la entidad.
- **Promover la mejora continua del Plan Estratégico**, utilizando los resultados del seguimiento, auditorías internas e incidentes de seguridad como insumos para su actualización y fortalecimiento.
- **Garantizar el compromiso de la alta dirección**, mediante la presentación periódica de resultados y el apoyo en la asignación de recursos necesarios para la implementación del Plan Estratégico.

12. ANEXOS

Plan de acción del Tratamiento de riesgos de seguridad y privacidad de la información

13. TABLA DE CONTROL DE REGISTROS

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN		Anexo al procedimiento OPL-PD04 FORMATO DE CONTROL DE REGISTROS		OPL-PD04-FO11	
			Tiempo de retención		
Nombre del registro	Código	Recuperación	Almacenamiento	Conservación	Disposición
Formato de Plan de acción	OPL-PD04-FO31	Personal Administrativo del subproceso AAI	Según TRD del del subproceso AAI	Según TRD del del subproceso AAI	Según TRD del del subproceso AAI

14. CONTROL DE CAMBIOS

 HOSPITAL UNIVERSITARIO SAN JOSÉ EMPRESA SOCIAL DEL ESTADO POPAYÁN		Anexo al procedimiento OPL-PD04 FORMATO DE CONTROL DE CAMBIOS		OPL-PD04-FO12
Código	Versión	Fecha	Descripción del Documento	
PLA-AAI-04	01	29 de enero del 2026	Se realizan ajustes al contenido del Plan Estratégico para incorporar cambios normativos, resultados del seguimiento y mejoras en la gestión de riesgos.	

**PLAN ESTRATÉGICO DE
TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

Código: PLA-AAI-05

Versión: 01

Página 13 de 13



Elaboró y/o actualizó	Pedro Alejandro Bonilla Valencia	Revisó	Juan David Uribe Ordoñez Martha Isabel Andrade Penagos	Aprobó	Juan Carlos Arteaga Cifuentes
Cargo	-Profesional SGSI de la administración y almacenamiento de la información – Afiliado participe Assesalud.OC	Cargo	-Coordinador de administración y almacenamiento de la información –Afiliado participe Assesalud.OC Subgerente Administrativo y Financiero Gr-1	Cargo	Gerente Gr-2 / HUSJ
Firma		Firma	 	Firma	
Fecha	30 ENE 2026	Fecha	30 ENE 2026	Fecha	30 ENE 2026
GESTIÓN DOCUMENTAL					
Nombre	Jesús Hernán Guerrero Erazo	Cargo	Auxiliar Administrativo Gr-3	Firma	