

PLAN ESTRATÉGICO DE LA POLÍTICA DE SEGURIDAD DIGITAL



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 (Esta en documento de Política)	6
6. DIAGNÓSTICO INSTITUCIONAL DEL PLAN ESTRATÉGICO	6
7. PROGRAMAS DERIVADOS DEL PLAN ESTRATÉGICO	6
8. METODOLOGÍAS Y ESTRATEGIAS	7
9. DETECCION DE DESVIACIONES	8
10. EVALUACIÓN Y SEGUIMIENTO	9
10.2.1 Nivel de implementación del SGSI	10
10.2.2 Nivel de fortalecimiento de la cultura organizacional de seguridad de la información	10
10.2.3 Nivel de gestión de accesos y control de identidades	10
10.2.4 Nivel de protección de la infraestructura tecnológica	10
10.2.5 Nivel de atención oportuna de incidentes de seguridad de la información	11
10.2.6 Nivel de revisión y actualización de la Política de Seguridad Digital	11
10.2.7 Controles de acceso implementados para datos personales	11
11. CONCLUSIONES Y PRÓXIMOS PASOS	12
11.1. Resumen de puntos clave	12
11.2. Recomendaciones y acciones a seguir	13
12. ANEXOS	13
13. TABLA DE CONTROL DE REGISTROS	14
14. CONTROL DE CAMBIOS	14

1. INTRODUCCIÓN

La seguridad digital constituye un pilar estratégico 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 caracterizado por la transformación digital y el incremento de amenazas a los sistemas de información. La información y los datos personales se reconocen como activos estratégicos esenciales para el cumplimiento de la misión institucional y la prestación segura de los servicios de salud.

El presente **Plan Estratégico de la Política de Seguridad Digital** define la visión, los objetivos generales y las líneas de acción prioritarias que orientan la gestión de la seguridad digital en el mediano y largo plazo, en coherencia con la norma ISO/IEC 27001, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la normatividad vigente. Este plan establece los criterios que guiarán las decisiones institucionales, fortaleciendo la gestión del riesgo, la cultura de seguridad y la sostenibilidad operativa del Hospital

2. JUSTIFICACIÓN

La implementación del Plan Estratégico de la Política de Seguridad Digital se justifica en la necesidad de proteger la información, los datos personales y los sistemas de información del Hospital Universitario San José de Popayán ESE frente a riesgos y amenazas que pueden afectar la continuidad de los servicios, la atención en salud y el cumplimiento de la normatividad vigente.

Este plan permite establecer una orientación estratégica clara para la gestión de la seguridad digital, fortalecer la cultura organizacional, prevenir incidentes de seguridad y garantizar un uso responsable y seguro de los recursos tecnológicos, contribuyendo al buen gobierno, la confianza institucional y la sostenibilidad del Hospital

3. MARCO NORMATIVO Y POLÍTICO

El Plan Estratégico de la Política de Seguridad Digital se fundamenta en el marco normativo y en los lineamientos técnicos vigentes que regulan 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:

N°	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	Resolución 1995 de 1999	Ministerio de Salud y Protección Social	Reglamenta el manejo de la historia clínica.

8	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

Fortalecer de manera integral y sostenible la seguridad digital del Hospital Universitario San José de Popayán, mediante la definición de lineamientos estratégicos que orienten la protección de la información, los datos personales y los sistemas de información, la gestión del riesgo y la continuidad de los servicios, en coherencia con la normatividad vigente y los objetivos estratégicos institucionales.

4.2 OBJETIVO ESPECIFICOS

- **Establecer y consolidar** un marco estratégico de seguridad digital que oriente la toma de decisiones institucionales y la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- **Fortalecer la gestión del riesgo** de seguridad de la información, mediante la identificación, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- **Promover una cultura organizacional de seguridad digital**, orientada al uso responsable de la información y de los recursos tecnológicos por parte de funcionarios, contratistas y terceros.
- **Fortalecer la protección de los datos personales y datos sensibles**, en cumplimiento de la normatividad vigente y los principios de legalidad, confidencialidad y responsabilidad.
- **Asegurar la continuidad de los servicios institucionales**, fortaleciendo la resiliencia frente a incidentes de seguridad digital que puedan afectar los procesos misionales y de apoyo.
- **Alinear la seguridad digital con el direccionamiento estratégico institucional**, contribuyendo al buen gobierno, la sostenibilidad operativa y la confianza de las partes interesadas.

5. ALINEACIÓN ESTRATÉGICA

El Plan Estratégico de la Política de Seguridad Digital se encuentra alineado con el direccionamiento estratégico del Hospital Universitario San José de Popayán, al contribuir al fortalecimiento del buen gobierno, la sostenibilidad institucional y la protección de los activos estratégicos de información, elementos fundamentales para la toma de decisiones y la continuidad de los servicios asistenciales y administrativos.

Así mismo, el plan se articula con el Plan de Desarrollo Institucional, la línea estratégica de buen gobierno y equilibrio financiero, la gestión de la tecnología y la información, y la Dimensión de Direccionamiento Estratégico y Planeación del Modelo Integrado de Planeación y Gestión (MIPG). Esta alineación contribuye a que la seguridad digital sea un eje transversal que apoye el logro de los objetivos institucionales y la mejora continua de la gestión.

6. DIAGNÓSTICO INSTITUCIONAL DEL PLAN ESTRATÉGICO

El Hospital Universitario San José de Popayán ESE cuenta con una Política de Seguridad Digital definida y con lineamientos orientados a la protección de la información, los datos personales y los sistemas de información. No obstante, el entorno digital actual, caracterizado por el aumento de amenazas cibernéticas, la dependencia tecnológica y las exigencias normativas, demanda fortalecer la gestión estratégica de la seguridad digital de manera integral y sostenible.

El diagnóstico institucional evidencia la necesidad de consolidar la gestión del riesgo de seguridad de la información, fortalecer la cultura organizacional, asegurar la continuidad de los servicios y mejorar la articulación entre la seguridad digital y el direccionamiento estratégico institucional. Así mismo, se identifica la importancia de contar con un plan estratégico que oriente prioridades, defina líneas de acción y facilite el seguimiento y la mejora continua de la seguridad digital en el mediano y largo plazo.

7. PROGRAMAS DERIVADOS DEL PLAN ESTRATÉGICO

No se derivan programas.

8. METODOLOGÍAS Y ESTRATEGIAS

El Plan Estratégico de la Política de Seguridad Digital se implementará mediante metodologías y estrategias orientadas a una gestión integral, sistemática y sostenible de la seguridad digital, alineadas con el direccionamiento estratégico institucional y la normatividad vigente.

8.1. 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.
- **Ciclo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar):** Como enfoque transversal para asegurar la evaluación periódica del desempeño y la mejora continua de la seguridad digital.

8.2. Estrategias

- 1. Implementar el Sistema de Gestión de Seguridad de la Información (SGSI)**
Definir el contexto interno y externo, el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), identificar, analizar y evaluar los riesgos de seguridad de la información, establecer procedimientos e instructivos, y asegurar su operación conforme al ciclo PHVA (Planificar, Hacer, Verificar y Actuar).
- 2. Capacitar y sensibilizar continuamente al personal:**
Implementar programas de formación, campañas de concientización y capacitaciones periódicas dirigidas a funcionarios, contratistas, proveedores y terceros autorizados sobre seguridad de la información, uso seguro de contraseñas, protección de datos personales, phishing y buenas prácticas digitales.
- 3. Administrar adecuadamente los accesos y el control de identidades:**
Implementar procedimientos formales para la creación, modificación, revisión y revocación de accesos a los sistemas de información, garantizando la

- asignación de permisos conforme a los roles y funciones de cada usuario.
4. **Implementar controles técnicos y de infraestructura:**
Aplicar mecanismos de protección como antivirus, firewalls, segmentación de red, cifrado, copias de seguridad, monitoreo de eventos e implementación de medidas de seguridad física para proteger equipos e instalaciones críticas y planes de continuidad y recuperación ante desastres.
 5. **Responder oportunamente ante incidentes de seguridad:**
Establecer e implementar un procedimiento formal para la detección, reporte, clasificación, análisis, respuesta y cierre de incidentes de seguridad, asegurando la documentación, análisis de causas y aplicación de acciones correctivas y preventivas.
 6. **Revisar y actualizar periódicamente la política:**
Revisar y actualizar anualmente la presente política o cuando existan cambios tecnológicos, incidentes relevantes, auditorías o modificaciones normativas que lo requieran.
 7. **Proteger los datos personales:**
Fortalecer la protección de los datos personales y datos sensibles tratados por el Hospital, mediante la implementación de medidas administrativas, técnicas y organizacionales que aseguren su uso adecuado y el cumplimiento de la normatividad vigente.

9. DETECCION DE DESVIACIONES

La detección de desviaciones del Plan Estratégico de la Política de Seguridad Digital del Hospital Universitario San José de Popayán ESE tiene como propósito identificar de manera oportuna cualquier diferencia entre lo planificado y lo efectivamente ejecutado, así como cambios, riesgos o eventos que puedan influir en el logro de los objetivos y estrategias institucionales.

La detección de desviaciones se realizará mediante el seguimiento sistemático de los indicadores definidos para cada una de las estrategias, la revisión periódica de los informes de avance del Plan de Acción, y la revisión de eventos relevantes que puedan impactar la seguridad digital institucional.

Los mecanismos y fuentes para la identificación de desviaciones incluirán, entre otros:

- El análisis periódico de los indicadores de desempeño definidos para cada estrategia del plan.
- La comparación de los resultados reales con las metas establecidas en el plan.

- Los informes de avance del Plan de Acción, con sus respectivos hitos y cronogramas.
- Los resultados de auditorías internas y externas relacionadas con los controles de seguridad digital.
- Los reportes de incidentes de seguridad de la información y otras alertas operativas relevantes.
- La identificación de cambios normativos, tecnológicos u organizacionales que puedan afectar el contexto de ejecución.

La detección de desviaciones permitirá activar oportunamente las acciones correctivas y preventivas necesarias, apoyar la toma de decisiones estratégicas y fomentar la mejora continua del desempeño institucional en materia de seguridad digital.

10. EVALUACIÓN Y SEGUIMIENTO

10.1. Mecanismos de Seguimiento

El seguimiento al Plan Estratégico de la Política de Seguridad Digital se realizará mediante la revisión periódica del Plan de Acción, el monitoreo de los indicadores definidos, la elaboración de informes de avance, la revisión de auditorías y el análisis de incidentes de seguridad, permitiendo identificar desviaciones y aplicar acciones de mejora.

Para tal fin, se establecen los siguientes mecanismos de seguimiento:

- **Seguimiento al Plan de Acción de la Política de Seguridad Digital**, mediante la revisión periódica del cumplimiento de las actividades, responsables y cronogramas definidos.
- **Monitoreo de los indicadores de desempeño**, definidos en la Política de Seguridad Digital, que permiten medir el nivel de avance y cumplimiento de las estrategias.
- **Elaboración y análisis de informes periódicos de avance**, presentados a las instancias de dirección y control correspondientes.
- **Revisión de los resultados de auditorías internas y externas**, relacionadas con la seguridad digital y la gestión de la información.
- **Análisis de los reportes e incidentes de seguridad de la información**, como insumo para la identificación de desviaciones y oportunidades de mejora.
- **Seguimiento a cambios normativos, tecnológicos u organizacionales**, que puedan afectar la ejecución del plan.

10.2. Indicadores del Plan

El seguimiento y evaluación del Plan Estratégico de la Política de Seguridad Digital se realizará a través de los indicadores definidos en la Política de Seguridad Digital institucional, los cuales permiten medir el nivel de avance, cumplimiento y efectividad de las estrategias adoptadas.

El seguimiento se realizará **semestralmente** mediante los siguientes indicadores:

10.2.1 Nivel de implementación del SGSI

- Unidad de medida: Porcentaje (%)
- Fórmula: $(\text{Actividades del SGSI implementadas} / \text{Total de actividades del SGSI definidas}) \times 100$
- Meta: Implementar 100 % las actividades del SGSI

10.2.2 Nivel de fortalecimiento de la cultura organizacional de seguridad de la información

- Unidad de medida: Porcentaje (%)
- Fórmula: $(\text{Personas capacitadas y sensibilizadas en seguridad de la información} / \text{Total de personas vinculadas}) \times 100$
- Meta: Capacitar y sensibilizar al 100 % del personal vinculado

10.2.3 Nivel de gestión de accesos y control de identidades

- Unidad de medida: Porcentaje (%)
- Fórmula: $(\text{Usuarios con accesos gestionados} / \text{Total de usuarios Dinámica}) \times 100$
- Meta: Usuarios del software Dinámica con accesos creados, revisados y revocados conforme al procedimiento al 100 %

10.2.4 Nivel de protección de la infraestructura tecnológica

- Unidad de medida: Porcentaje (%)

- Fórmula: $(\text{Activos tecnológicos con controles de seguridad implementados} / \text{Total de activos tecnológicos críticos}) \times 100$
- Meta: Implementar controles de seguridad en el 100 % de los activos tecnológicos críticos del Hospital

10.2.5 Nivel de atención oportuna de incidentes de seguridad de la información

- Unidad de medida: Porcentaje (%)
- Fórmula: $(\text{Incidentes atendidos oportunamente} / \text{Incidentes reportados}) \times 100$
- Meta: Atender el 100 % de los incidentes de seguridad dentro de los tiempos establecidos

10.2.6 Nivel de revisión y actualización de la Política de Seguridad Digital

- Unidad de medida: Porcentaje (%)
- Fórmula: $(\text{Políticas de seguridad revisadas y actualizadas} / \text{Políticas de seguridad definidas}) \times 100$
- Meta: Revisar y actualizar el 100 % de la Política de Seguridad Digital conforme al periodo establecido

10.2.7 Controles de acceso implementados para datos personales

- Unidad de medida: Porcentaje (%)
- Fórmula: $(\text{Número de sistemas con controles de acceso definidos} / \text{Total de sistemas que tratan datos personales}) \times 100$
- Meta: Alcanzar el 100% de implementación de controles de acceso en los sistemas de información que tratan datos personales y datos sensibles, conforme a los roles y funciones autorizadas.

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

La evaluación del Plan de Acción de la Política de Seguridad Digital 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.

De acuerdo con los indicadores definidos en la Política de Seguridad Digital, la frecuencia de evaluación será la siguiente:

- **Seguimiento semestral**, orientado a evaluar el comportamiento de los indicadores de seguridad digital, el avance en la implementación de las estrategias y el cumplimiento de las metas establecidas.
- **Evaluación anual**, orientada a realizar una revisión integral del Plan de Acción, el nivel de cumplimiento del Plan Estratégico y la necesidad de ajustes a la Política de Seguridad Digital, conforme a los resultados obtenidos y a cambios normativos, tecnológicos u organizacionales.

El seguimiento y la evaluación del Plan de Acción se documentarán en el formato definido como anexo, el cual servirá como evidencia para la toma de decisiones, la detección de desviaciones y la implementación de acciones correctivas y de mejora.

11. CONCLUSIONES Y PRÓXIMOS PASOS

11.1. Resumen de puntos clave

- El Plan Estratégico de la Política de Seguridad Digital establece el marco general para la protección de la información, los datos personales y los sistemas de información del Hospital, en coherencia con la normatividad vigente y los objetivos institucionales.
- El Plan se encuentra alineado con la Política de Seguridad Digital institucional y con los lineamientos del MIPG, el MSPI y las buenas prácticas internacionales en seguridad de la información.
- Se definieron estrategias claras orientadas a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), el fortalecimiento de la cultura organizacional, la gestión de accesos, la protección de la infraestructura tecnológica, la atención de incidentes, la actualización de la política y la protección de los datos personales.
- El seguimiento del Plan se realizará mediante la revisión periódica del Plan de Acción, el monitoreo de indicadores, la elaboración de informes, la revisión de auditorías y el análisis de incidentes de seguridad.
- Los indicadores del Plan son los definidos en la Política de Seguridad Digital y se evaluarán con una periodicidad semestral, permitiendo medir el avance, el cumplimiento de metas y la efectividad de las estrategias.
- La evaluación del Plan de Acción se realizará de manera semestral y anual, documentándose en los formatos definidos como anexo, como insumo para la detección de desviaciones y la implementación de acciones de mejora.
- El Plan promueve la mejora continua de la seguridad digital, asegurando la disponibilidad, integridad y confidencialidad de la información y la continuidad de los servicios institucionales.

11.2. Recomendaciones y acciones a seguir

Con el fin de contribuir a la adecuada implementación, sostenibilidad y mejora continua del Plan Estratégico de la Política de Seguridad Digital, se formulan las siguientes recomendaciones y acciones a seguir:

- Promover el compromiso de la alta dirección, propiciando el liderazgo institucional, la asignación de recursos y el apoyo necesario para la implementación del Plan Estratégico y del Sistema de Gestión de Seguridad de la Información (SGSI).
- Fortalecer la gobernanza de la seguridad digital, mediante la definición clara de roles, responsabilidades y la articulación entre las áreas involucradas en la gestión de la seguridad de la información.
- Implementar y mantener actualizado el Plan de Acción, facilitando la ejecución oportuna de las actividades, el cumplimiento de los cronogramas y la trazabilidad con los objetivos estratégicos.
- Promover la cultura organizacional de seguridad de la información, a través de programas permanentes de capacitación, sensibilización y concientización dirigidos a funcionarios, contratistas y terceros.
- Monitorear de forma permanente los indicadores definidos, utilizando los resultados como insumo para la toma de decisiones, la identificación de desviaciones y la aplicación de acciones correctivas y de mejora.
- Gestionar de manera oportuna los incidentes de seguridad de la información, promoviendo su registro, análisis, atención y cierre conforme a los procedimientos establecidos.
- Revisar y actualizar periódicamente la Política de Seguridad Digital y el Plan Estratégico, teniendo en cuenta los resultados del seguimiento, los cambios normativos, tecnológicos y organizacionales.
- Fortalecer el cumplimiento normativo en materia de protección de datos personales, mediante la aplicación de controles administrativos, técnicos y organizacionales aplicables.

12. ANEXOS

Plan de acción que desarrolla la política de seguridad digital

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	Elaboración del Plan Estratégico de la Política de Seguridad Digital del Hospital Universitario San José de Popayán ESE, con el fin de definir el direccionamiento estratégico, los objetivos, metodologías, estrategias, mecanismos de seguimiento e indicadores para la gestión de la seguridad digital, en cumplimiento de la normatividad vigente y los lineamientos institucionales.	

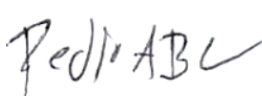
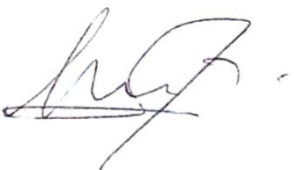
**PLAN ESTRATÉGICO DE LA
POLÍTICA DE SEGURIDAD DIGITAL**

Código: PLA-AAI-04

Versión: 01

Página 15 de 15



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	