



ESE HOSPITAL SAN CARLOS AIPE-HUILA	CODIGO	GDE-GTH-PL-FO-13
	VERSION	05
	VIGENCIA	2026
PLANES INSTITUCIONALES	PAGINA	1 de 5


ESE HOSPITAL SAN CARLOS DE AIPE

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



VIGENCIA 2026 AIPE – HUILA

Proyecto: LIDER SISTEMAS	Reviso: LIDER SUBGERENCIA ADMINISTRATIVA	Aprobó: GERENCIA
Nombre: DEICY LIZCANO	Nombre: JHON MAILER SAAVEDRA V.	Nombre: ALVARO E. DIAZGRANADOS YAGUAR
Telefono: 3208404626	Av. Nuevo Milenio N. 12ª-13 Aipe (H)	Email: esehospitalsancarlos@yahoo.es


	ESE HOSPITAL SAN CARLOS AIPE-HUILA	CODIGO	GDE-GTH-PL-FO-13
		VERSION	05
		VIGENCIA	2026
	PLANES INSTITUCIONALES	PAGINA	2 de 5

1. Introducción

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSI) se formula para la ESE Hospital San Carlos de Aipe, con el propósito de identificar, analizar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional, especialmente aquella relacionada con datos personales y datos sensibles en salud.

Este plan se alinea con los lineamientos del CONPES 3995 de 2020 sobre Seguridad y Confianza Digital, así como con el marco normativo colombiano vigente, reconociendo que el entorno digital del sector salud está expuesto a amenazas cibernéticas que pueden impactar la continuidad del servicio, la seguridad del paciente y la confianza de los ciudadanos.

Proyecto: LIDER SISTEMAS	Reviso: LIDER SUBGERENCIA ADMINISTRATIVA	Aprobó: GERENCIA
Nombre: DEICY LIZCANO	Nombre: JHON MAILER SAAVEDRA V.	Nombre: ALVARO E. DIAZGRANADOS YAGUAR
Telefono: 3208404626	Av. Nuevo Milenio N. 12ª-13 Aipe (H)	Email: esehospitalsancarlos@yahoo.es

	ESE HOSPITAL SAN CARLOS AIPE-HUILA	CODIGO	GDE-GTH-PL-FO-13
		VERSION	05
		VIGENCIA	2026
	PLANES INSTITUCIONALES		PAGINA

2. Objetivo

Definir las acciones necesarias para tratar los riesgos de seguridad y privacidad de la información en la ESE Hospital San Carlos de Aipe, mediante la implementación de controles administrativos, técnicos y operativos que permitan proteger los activos de información y cumplir con la normatividad vigente.

3. Alcance

El PTRSI aplica a todos los procesos, sistemas de información, bases de datos, infraestructuras tecnológicas y activos de información de la ESE Hospital San Carlos de Aipe, así como a todos los funcionarios, contratistas y terceros que tengan acceso a información institucional.

3.1 Dirigido a

Todos los colaboradores de la ESE Hospital San Carlos de Aipe involucrados en el uso, administración o custodia de la información y de los recursos TIC.

3.2 Responsable


Coordinador del Área de Sistemas o quien haga sus veces, con el apoyo de la Gerencia de la ESE.

4. Marco Normativo

El presente plan se fundamenta, entre otras, en las siguientes disposiciones:

- J Constitución Política de Colombia – Artículo 15
- J Ley 1581 de 2012 – Protección de Datos Personales
- J Decreto 1377 de 2013
- J Ley 1712 de 2014 – Ley de Transparencia
- J Decreto 1008 de 2018 – Gobierno Digital
- J CONPES 3995 de 2020 – Seguridad y Confianza Digital
- J Norma Técnica Colombiana NTC ISO/IEC 27001

Proyecto: LIDER SISTEMAS	Reviso: LIDER SUBGERENCIA ADMINISTRATIVA	Aprobó: GERENCIA
Nombre: DEICY LIZCANO	Nombre: JHON MAILER SAAVEDRA V.	Nombre: ALVARO E. DIAZGRANADOS YAGUAR
Telefono: 3208404626	Av. Nuevo Milenio N. 12ª-13 Aipe (H)	Email: esehospitalsancarlos@yahoo.es

	ESE HOSPITAL SAN CARLOS AIPE-HUILA	CODIGO	GDE-GTH-PL-FO-13
		VERSION	05
		VIGENCIA	2026
	PLANES INSTITUCIONALES		PAGINA

5. Identificación de Riesgos de Seguridad y Privacidad

Los principales riesgos identificados para la ESE Hospital San Carlos de Aipe son:

- J Ataques de phishing y suplantación de identidad a través de correo electrónico o mensajería instantánea.
- J Infección por malware y ransomware que afecte sistemas clínicos y administrativos.
- J Accesos no autorizados a historias clínicas y bases de datos de pacientes.
- J Pérdida o alteración de información por fallas tecnológicas o errores humanos.
- J Falta de conocimiento del personal en seguridad de la información y protección de datos personales.
- J Interrupción de servicios TIC que afecten la atención en salud.

6. Valoración del Riesgo

La valoración del riesgo se realiza de manera cualitativa, teniendo en cuenta:

- J **Probabilidad:** Baja, Media o Alta.
- J **Impacto:** Bajo, Medio o Alto, considerando efectos legales, operativos, financieros y reputacionales.

A partir de esta valoración se define el nivel de riesgo y la estrategia de tratamiento más adecuada.

7. Estrategias de Tratamiento del Riesgo


La ESE Hospital San Carlos de Aipe adoptará las siguientes estrategias:

- J **Mitigar:** Reducir la probabilidad o el impacto del riesgo mediante controles.
- J **Evitar:** Suspender actividades que generen riesgos inaceptables.
- J **Transferir:** Trasladar el riesgo a terceros (seguros, contratos).
- J **Aceptar:** Asumir el riesgo cuando se encuentre dentro del nivel tolerable.

7.1 Estrategia orientada al conocimiento

- J Capacitación anual al personal en seguridad de la información y protección de datos personales.
- J Sensibilización sobre uso seguro del correo electrónico, contraseñas y dispositivos.

Proyecto: LIDER SISTEMAS	Reviso: LIDER SUBGERENCIA ADMINISTRATIVA	Aprobó: GERENCIA
Nombre: DEICY LIZCANO	Nombre: JHON MAILER SAAVEDRA V.	Nombre: ALVARO E. DIAZGRANADOS YAGUAR
Teléfono: 3208404626	Av. Nuevo Milenio N. 12ª-13 Aipe (H)	Email: esehospitalsancarlos@yahoo.es

	ESE HOSPITAL SAN CARLOS AIPE-HUILA	CODIGO	GDE-GTH-PL-FO-13
		VERSION	05
		VIGENCIA	2026
	PLANES INSTITUCIONALES	PAGINA	5 de 5

-) Socialización de políticas institucionales de seguridad de la información.

7.2 Estrategia orientada a la continuidad

-) Fortalecimiento de la infraestructura tecnológica (servidores, red, energía).
-) Implementación y actualización de planes de contingencia y continuidad del negocio.
-) Definición de procedimientos para recuperación ante desastres.

7.3 Estrategia orientada al control de acceso

-) Definición de roles y perfiles de acceso a los sistemas de información.
-) Implementación de acuerdos de confidencialidad para funcionarios y contratistas.
-) Inventario actualizado de usuarios, accesos y privilegios.

7.4 Estrategia de controles tecnológicos

-) Uso de antivirus y herramientas de seguridad perimetral.
-) Realización periódica de copias de seguridad y verificación de su restauración.
-) Aplicación de parches de seguridad y actualizaciones de software.
-) Monitoreo de eventos de seguridad en la infraestructura TIC.

8. Plan de Trabajo PTRSI – Vigencia 2026

<i>Actividad</i>	Responsable	Periodicidad
<i>Capacitación en seguridad de la información</i>	Sistemas / Talento Humano	Anual
<i>Revisión de políticas de seguridad</i>	Sistemas	Anual
<i>Actualización de inventario de activos de información</i>	Sistemas	Semestral
<i>Verificación de copias de seguridad</i>	Sistemas	Mensual
<i>Revisión de accesos y usuarios</i>	Sistemas	Trimestral
<i>Actualización de antivirus y parches</i>	Sistemas	Permanente

9. Aprobación

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información rige a partir de su aprobación por la Gerencia de la ESE Hospital San Carlos de Aipe y será revisado anualmente o cuando se presenten cambios significativos en los procesos o en la infraestructura tecnológica.

Proyecto: LIDER SISTEMAS	Reviso: LIDER SUBGERENCIA ADMINISTRATIVA	Aprobó: GERENCIA
Nombre: DEICY LIZCANO	Nombre: JHON MAILER SAAVEDRA V.	Nombre: ALVARO E. DIAZGRANADOS YAGUAR
Telefono: 3208404626	Av. Nuevo Milenio N. 12ª-13 Aipe (H)	Email: esehospitalsancarlos@yahoo.es