 <p>HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E</p>	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
	ÁREA DE COMUNICACIONES	29-01-2025
		SALAMINA CALDAS
		pág. 1

**MIPG HD FS ESE**


**2025**

# Plan de Seguridad y Privacidad de la Información 2025




**Hospital Departamental  
Felipe Suárez  
E.S.E.**

**MIPG HD FS**

 HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
	ÁREA DE COMUNICACIONES	29-01-2025
		SALAMINA CALDAS
		pág. 2

## Tabla de contenido

1. Introducción .....	3
Justificación .....	<b>¡Error! Marcador no definido.</b>
Propósito del plan .....	<b>¡Error! Marcador no definido.</b>
El plan estratégico de tecnologías de la información y las telecomunicaciones (PETIC):	<b>¡Error! Marcador no definido.</b>
Alcance del documento .....	<b>¡Error! Marcador no definido.</b>
2. Marco normativo.....	<b>¡Error! Marcador no definido.</b>
3. Plataforma estratégica del hospital departamental Felipe Suárez ESE .	<b>¡Error! Marcador no definido.</b>
Misión .....	<b>¡Error! Marcador no definido.</b>
Visión .....	<b>¡Error! Marcador no definido.</b>
4. Objetivos estratégicos .....	<b>¡Error! Marcador no definido.</b>
Valores institucionales .....	<b>¡Error! Marcador no definido.</b>
Principios institucionales.....	<b>¡Error! Marcador no definido.</b>
5. Objetivos del plan estratégico de sistemas de información .....	<b>¡Error! Marcador no definido.</b>
Objetivo general.....	<b>¡Error! Marcador no definido.</b>
Objetivos específicos.....	<b>¡Error! Marcador no definido.</b>
6. Políticas .....	<b>¡Error! Marcador no definido.</b>
Políticas de comunicación e información.....	<b>¡Error! Marcador no definido.</b>
Postulados sobre confidencialidad, elaboración, administración y suministro de información institucional.....	<b>¡Error! Marcador no definido.</b>
Política de seguridad de la información .....	<b>¡Error! Marcador no definido.</b>
Políticas generales de seguridad de la información.....	<b>¡Error! Marcador no definido.</b>
Revisión independiente de la seguridad de la información .....	<b>¡Error! Marcador no definido.</b>
Gestión de activos de información.....	<b>¡Error! Marcador no definido.</b>
Administración de operaciones y comunicaciones .....	<b>¡Error! Marcador no definido.</b>
Control de acceso .....	<b>¡Error! Marcador no definido.</b>
Inventario de equipos informáticos y sistemas operativos .....	<b>¡Error! Marcador no definido.</b>
Red de comunicaciones.....	<b>¡Error! Marcador no definido.</b>
Planes de contingencia.....	<b>¡Error! Marcador no definido.</b>

 HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
		29-01-2025
	ÁREA DE COMUNICACIONES	SALAMINA CALDAS
	pág. 3	

## 1. Introducción

El Plan de Seguridad y Privacidad de la Información se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medidas de seguridad y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad, la institución define medidas que serán aplicadas durante la vigencia 2025.

El Plan de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planeen acciones que reduzcan la afectación que pueda sufrir la entidad en caso de materialización, adicional a ello, se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC dentro de la institución.

Lo anterior, dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC, así como, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas.

### Definiciones

**Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

**Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

**Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

**Probabilidad:** es la Probabilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.


**Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

**Controlo Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

## 2. Objetivos

### Objetivo general

Desarrollar los lineamientos de Seguridad y Privacidad de la Información, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la misma.

	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
	ÁREA DE COMUNICACIONES	29-01-2025
		SALAMINA CALDAS
		pág. 4

### Objetivos específicos

- Cumplir con todos los requisitos legales y reglamentarios referentes a la temática del plan contenido en la legislación colombiana.
- Fortalecer el conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información al interior del Hospital Departamental Felipe Suárez E.S.E.
- Gestionar riesgos de Seguridad y Privacidad de la información, de acuerdo con los contextos establecidos en la Entidad.

### Alcance

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Hospital, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

Realizar una eficiente gestión del Plan de Seguridad y Privacidad de la información, que permita integrar en los procesos de la institución, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

### 3. Marco legal

Acceso a la Información Pública Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).


Archivo Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

### 4. Marco referencial

El Hospital Departamental Felipe Suárez E.S.E a través de su Modelo Integrado de Planeación y Gestión, se compromete a mantener una cultura de la gestión de la seguridad y privacidad de la información, asociada con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos y fortaleciendo las medidas de control y la

 HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E.	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
	ÁREA DE COMUNICACIONES	29-01-2025
		SALAMINA CALDAS
		pág. 5

eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta ante las situaciones adversas.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

**Evitar:** se refiere a eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición o su expresión máxima.

**Prevenir:** corresponde al área de planeación y su objetivo es: proyectar estrategias con el propósito que el evento no ocurra o que disminuya su probabilidad de ocurrencia.

**Reducir o mitigar:** corresponde a la protección en el momento en que se presenta la situación adversa.

**Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo la responsabilidad de un solo encargado


**Compartir:** es involucrar a un tercero para que responda en todo o parte por el riesgo que genera una actividad.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (Min TIC: 2016).

#### 4. Metodología

El Plan de Seguridad y privacidad de la Información contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos intangibles de la institución, estas actividades se estructuraron siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (Min TIC: 2016), de la siguiente manera:

Objetivos específicos	Actividad	Tarea	Ejecución	Responsable	Recursos
Cumplir con todos los requisitos legales y reglamentarios referentes a la temática del plan contenidos en la legislación colombiana	Confirmación y aceptación por parte del paciente de la política de tratamiento de datos del Hospital	Firma del consentimiento por parte del usuario y empleado	Anual	Facturadores y recurso humano	Documento físico
Fortalecer el conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información al interior del Hospital Departamental Felipe Suárez E.S.E.	Copias de seguridad diarias	Copias de seguridad automáticas	Diaria	sistemas	servidor Disco duro
	Seguridad perimetral	Configuración Fortinet	Diaria	sistemas	Interfaz Fortinet
	Antivirus	Instalación antivirus kaspersky	anual	sistemas	renovación anual licencia
Gestionar riesgos de Seguridad y Privacidad de la información, de acuerdo con los contextos establecidos en la Entidad	Implementar capacitaciones y exposición de la política de seguridad y privacidad de la información	Capacitar al personal	semestral	sistemas	Sala de juntas Videobeam computador

 HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
		29-01-2025
	ÁREA DE COMUNICACIONES	SALAMINA CALDAS
	pág. 6	

## Desarrollo metodológico

### Fase 1: Análisis de la información

En esta primera etapa, se realizarán y evaluarán los resultados de las entrevistas proyectadas a los colaboradores del proceso de T.I, por consiguiente, se desarrollarán las actividades necesarias para dar cumplimiento a esta fase.

### Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que conlleven a desarrollar la estructuración de las medidas necesarias para el cumplimiento del Plan de Seguridad y Privacidad de la Información.

### Fase 3: Análisis de los proyectos

En esta etapa, se llevará a cabo la definición de los controles relacionados con cada una de las medidas expuestas y desarrolladas en la fase anterior.

### Fase 4: Definición del organigrama de responsabilidad

En esta fase se realizará una organización funciona y se definirán las responsabilidades respecto a la administración y gestión del Plan de Seguridad y Privacidad de la Información, esta etapa deberá ser definida por la institución teniendo en cuenta su estructura organizacional actualmente constituida.

### Fase 5: Ciclo de vida del tratamiento de riesgos

Finalmente, esta fase permite definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Seguridad y Privacidad de la Información.

## Resumen de etapas

Las etapas del Plan de Seguridad y Privacidad de la Información estarán alineadas y fundamentadas en el ciclo de calidad y mejora continua planear, hacer, verificar y actuar – PHVA, estructurado en cuatro fases, así:

**Planear:** Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de gestión del plan.

**Hacer:** En esta fase del ciclo de calidad y mejora continua se desarrollarán las actividades enmarcadas en la etapa 2 de la metodología de gestión de plan.


**Verificar:** En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

**Actuar:** Dentro de esta última fase, se realizarán las mejoras pertinentes teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos arrojadas en la fase anterior.

## Oportunidad de mejora

El Hospital Departamental Felipe Suárez E.S.E, no sólo debe concentrarse en la identificación de los riesgos, sino, que este análisis y reconocimiento del riesgo debe ser el primer avance para descubrir oportunidades. Es por esto, que la oportunidad de mejora será entendida como la consecuencia positiva real, frente al resultado del tratamiento de estas situaciones adversas.



 HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E.	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
	ÁREA DE COMUNICACIONES	29-01-2025
		SALAMINA CALDAS
		pág. 7

## Recursos

El Hospital Departamental Felipe Suárez E.S.E, en el marco de la gestión del plan de seguridad y Privacidad de la información, dispone de los siguientes recursos.

### Aprobación y publicación

El Comité Institucional de Gestión y Desempeño aprobará el Programa estratégico de tecnologías de la información y las comunicaciones (PTIC). En virtud de lo anterior y una vez adoptado mediante acto administrativo expedido por el gerente de la Institución se deberá proceder a la publicación del mismo en la página web, con la finalidad de dar a conocer y socializarlo con los funcionarios, aunado al hecho de que se dará acceso e información a la ciudadanía.

El Hospital Departamental Felipe Suarez E.S.E. de Salamina-Caldas, deberá actualizar el Programa estratégico de tecnologías de la información y las comunicaciones (PTIC) - una vez se cumplan los tiempos de articulación del mismo o cuando las circunstancias lo exijan o cuando en la modificación de funciones requiera, lo anterior siguiendo las instancias de aprobación y publicación.

---

WILSON DIDIER CARMONA DUQUE

Gerente

### Nota aclaratoria sobre documentos publicados en internet

Los documentos institucionales del Hospital Departamental Felipe Suárez ESE publicados en la página web y otros medios digitales son de carácter informativo. Se aclara que los documentos originales son aquellos que llevan la firma del Gerente de la entidad, en cumplimiento de la normatividad vigente sobre gestión documental y validez jurídica de los documentos públicos.

### ★ Normatividad Aplicable:

Ley 594 de 2000 (Ley General de Archivos de Colombia)

Artículo 7: Los documentos de archivo deben ser auténticos, íntegros y fidedignos, asegurando su conservación y disponibilidad en las entidades públicas.

Ley 527 de 1999 (Ley sobre Comercio Electrónico y Firma Digital)


Artículo 6: Un mensaje de datos (documento digital) tiene valor probatorio, pero su autenticidad debe estar garantizada con mecanismos adecuados de validación.

Decreto 1080 de 2015 (Decreto Único Reglamentario del Sector Cultura)

Título 4: Obliga a las entidades públicas a garantizar la autenticidad y conservación de los documentos administrativos.

Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo)

Artículo 17: Los actos administrativos deben estar debidamente firmados por la autoridad competente para que tengan validez legal.

 HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ ESE	HDFS
	ÁREA DE SISTEMAS	Código GD:HFS.P- 01
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión 2
		29-01-2025
	ÁREA DE COMUNICACIONES	SALAMINA CALDAS
	pág. 8	

✦ Importante:

- ✓ Los documentos únicos oficiales y con validez jurídica son los que llevan la firma del Gerente del Hospital.
- ✓ En caso de discrepancia entre la versión digital y el documento físico firmado, prevalecerá este último.
- ✓ Si requiere una copia autenticada del documento original, puede solicitarla en la Oficina de Gestión Documental del hospital.

Hospital Departamental Felipe Suárez ESE

Fecha de emisión: Salamina 29 de enero de 2025.