



**PLAN DE  
SEGURIDAD Y  
PRIVACIDAD  
DE LA  
INFORMACIÓN**



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

Su salud, Nuestra razón de ser

**SALAMINA-CALDAS**  
2021

	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	Fecha: Enero 2021
	SALAMINA -CALDAS	Página 2

## CONTENIDO

INTRODUCCIÓN .....	3
1. DEFINICIONES .....	4
2. OBJETIVOS .....	5
3. ALCANCE .....	6
4. MARCO LEGAL .....	7
5. MARCO REFERENCIAL .....	8
6. METODOLOGÍA.....	9
7. DESARROLLO METODOLÓGICO .....	10
8. RESUMEN DE ETAPAS .....	11
9. OPORTUNIDAD DE MEJORA.....	12
10. RECURSOS .....	13

 <p>Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser</p>	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E SALAMINA -CALDAS	Fecha: Enero 2021
		Página 3

## 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 2021.

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.

 <p>Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser</p>	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E SALAMINA -CALDAS	Fecha: Enero 2021
		Página 4

## 1. 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.

	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	Fecha: Enero 2021
	SALAMINA -CALDAS	Página 5

## 2. OBJETIVOS

### GENERAL

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

### ESPECIFICOS

Cumplir con todos los requisitos legales y reglamentarios referentes a la temática del plan contenidos 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.

	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	Fecha: Enero 2021
	SALAMINA -CALDAS	Página 6

### 3. 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.

 <p>Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser</p>	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E SALAMINA -CALDAS	Fecha: Enero 2021
		Página 7

#### 4. 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).

 <p>Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser</p>	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E SALAMINA -CALDAS	Fecha: Enero 2021
		Página 8

## 5. 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 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 algunas 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 (MinTIC:2016).

 Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E SALAMINA -CALDAS	Fecha: Enero 2021
		Página 9

## 6. 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 (MinTIC:2016), de la siguiente manera:

GESTIÓN	ACTIVIDAD	TAREA	RESPONSABLE
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Definir lineamientos	Definir políticas y metodologías de gestión	Equipo de tecnologías
	Realizar sensibilización	Socialización de medidas al interior de la institución	Equipo de tecnologías
	Identificar riesgos	Identificación, análisis y evaluación de situaciones adversas	Equipo de tecnologías con colaboración de todo el personal
	Intervenir riesgos encontrados	Desarrollar planes de tratamientos de riesgos	Equipo de tecnologías
	Realizar seguimiento	Seguimiento y verificación de evidencias encontradas	Equipo de tecnologías
	Desarrollar iniciativas de mejora	Realización de planes de calidad y mejora continua	Equipo de tecnologías
	Realizar monitoreo y control	Identificar y seguir plan de indicadores	Área de Planeación y equipo de tecnologías

 <p>Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser</p>	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E SALAMINA -CALDAS	Fecha: Enero 2021
		Página <b>10</b>

## 7. 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.

 <p>Hospital Departamental <b>Felipe Suárez</b> E.S.E. Su salud, Nuestra razón de ser</p>	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	Fecha: Enero 2021
	SALAMINA -CALDAS	Página 11

## 8. 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.

	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	Fecha: Enero 2021
	SALAMINA -CALDAS	Página <b>12</b>

## 9. 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.

	GESTION DOCUMENTAL	Código: GD: HFS.P-03
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 02
	HOSPITAL DEPARTAMENTAL FELIPE SUÁREZ E.S.E	Fecha: Enero 2021
	SALAMINA -CALDAS	Página 13

## 10. 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.

RECURSOS	DESCRIPCIÓN
Humanos	La Oficina de Gestión de tecnología con supervisión del área de planeación, son responsables de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	-Guía para la administración del riesgo y el diseño de controles en entidades públicas -Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI) - ISO 27001 y 31000
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías.