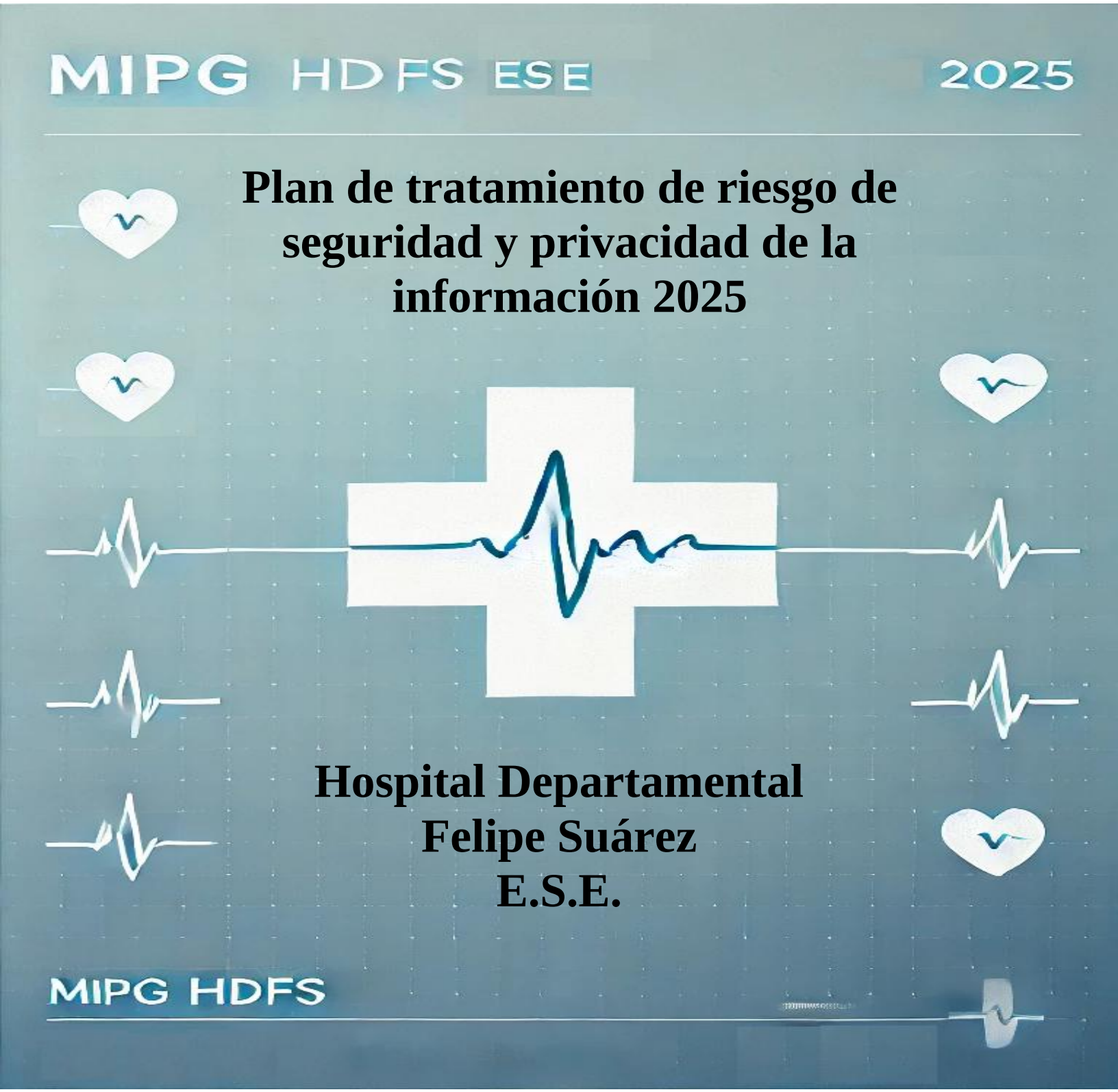

MIPG HDFS ESE
2025
Plan de tratamiento de riesgo de seguridad y privacidad de la información 2025
Hospital Departamental Felipe Suárez E.S.E.
MIPG HDFS

Tabla de contenido

1. Introducción

El Hospital Departamental Felipe Suarez E.S.E en busca de mejorar continuamente, implementa un método sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados al manejo de la información institucional.

En el quehacer diario de la institución, se usan tecnologías de la información en cuanto a: captura, procesamiento y reporte de datos, tanto interna como externamente para comunicarse con los diferentes actores del sistema de salud. Esto implica que la Entidad sea vulnerable a ataques mal intencionados o pueda existir mala manipulación de la información, lo que acarrea problemas económicos, legales, y administrativos, por tal razón, este documento busca establecer una línea de trabajo que permita al Hospital Departamental Felipe Suarez

E.S.E sortear los riesgos que lo rodean y proteger la integridad de su información.

2. Objetivos

Objetivos objetivo general

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que se convierta en guía para el control y minimización de los de las acciones negativas y de esta manera, proteger la integridad de los datos tanto de los procesos como de las personas vinculadas con la institución.

Objetivos específicos

• Realizar un diagnóstico de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información.

• Desarrollar metodologías, prácticas y recomendaciones dadas por la función pública y Min tic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

• Optimizar los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Alcance y limitaciones alcance

El plan de Riesgos de Seguridad y Privacidad de la Información aplica a todos los procesos de la institución en los cuales se manejen, procesen o interactúen con datos sensibles.

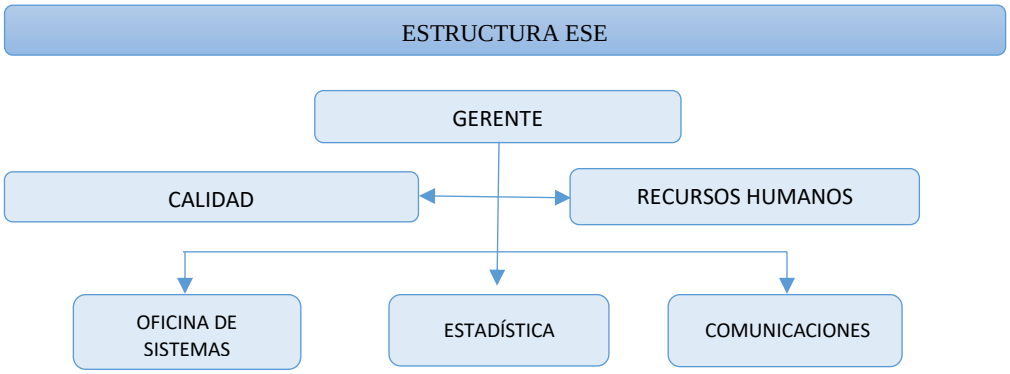
Limitaciones

Se fundamentan en la destinación del presupuesto necesario para permitir la implementación del Plan de Gestión del Riesgo de la Seguridad de la Información en la institución. Esto debido, a que los recursos económicos que ingresan al Hospital Departamental Felipe Suárez

E.S.E son reducidos.

Responsables

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:



- Gerente
- Auditora de calidad
- Jefe de recurso humano
- Ingeniero De Sistemas
- Auxiliar administrativo estadístico.

3. Marco conceptual

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).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza y determinar el nivel de riesgo.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias del grado en el que se cumplen los criterios de evaluados.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Ámbito o espacio hipotético de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI de la organización, tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación.

Gestión de incidentes de seguridad de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados e interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

4. Marco normativo

• Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
• Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública.
• Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.
• Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.
• Ley 594 de 2000 - Ley General de Archivos.
• Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
• Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.
• Ley Estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.
• Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
• Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
• Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
• Decreto 2364 de 2012 - Firma electrónica.

• Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.
• Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.
• Ley 527 de 1999 - Ley de Comercio Electrónico.
• Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
• Ley Estatutaria 1581 de 2012 - Protección de datos personales.
• Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

5. Descripción del plan

Identificación del riesgo:
El propósito de la identificación del riesgo es determinar factores que causen una perdida potencial y llegar a comprender el cómo, donde, y por qué podría ocurrir este suceso, las siguientes etapas recolectan datos de entrada para esta actividad.

Categorías de riesgos:
ET: Estratégicos: Relacionados a los lineamientos, políticas, estrategias o directrices no adecuadas o convenientes para la Entidad.
OP: Operativo: Relacionado a los procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presenten una posible brecha frente a la calidad esperada.
FA: Financiero: Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.
TEC: Tecnológico: Relacionado al uso, manejo o disposición de equipos biomédicos, industriales, de cómputo y periféricos.
CL: Clínico: Relacionados a condiciones patológicas de pacientes atendidos en el HCI. Considerar la aplicación de la metodología AMFE según lo definido en el MP- 0266

Identificación de riesgos:
Reconocer eventos o situaciones no deseadas que se pretenden evitar, por tal razón el descubrimiento de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del mismo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a emprender. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

Descripción de Causas:

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

Consecuencias:

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, pérdidas económicas, perjuicio de la imagen, sanciones legales, reproceso, demoras, insatisfacción, entre otras.

Barreras de Seguridad Existentes:

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, estos pueden ser encontrados en los protocolos o procedimientos documentados, en las guías de reacción inmediata o en las buenas prácticas de seguridad del paciente.

Valoración del Riesgo:

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración:

Probabilidad		
Remota	**1**	La probabilidad de ocurrencia es muy baja, casi nula
Poco Probable	**2**	Puede ocurrir bajo circunstancias excepcionales
Probable	**3**	Puede ocurrir con cierta frecuencia
Ocasional	**4**	Ocurre algunas veces
Frecuente	**5**	La ocurrencia se da de manera común en circunstancias actuales

Impacto		
Muy bajo	**1**	Los efectos de materialización del riesgo no son significativos
Bajo	**2**	Los efectos de materialización del riesgo son poco significativos
Moderado	**3**	Los efectos de materialización del riesgo pueden significar aspectos moderados
Alto	**4**	Los efectos de materialización del riesgo son significativos e importantes
Muy Alto	**5**	Los efectos son catastróficos, como muerte, lesiones incapacitantes o liquidación de la empresa

Probabilidad						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		Impacto				

Nivel de riesgo	Medidas de respuesta
Baja	Asumir el riesgo y continuar monitorizándolo
Aceptable	Reducir el riesgo para llevarlo a zona baja
Alta	Evitar-compartir-transferir por medio de un plan documentado

Tratamiento y seguimiento del riesgo:

Se implementan los controles o barreras a fin de fortalecer las ya existentes y de esta manera, aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas, pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, debido, a que no es suficiente cumplir las actividades propuestas, sino también, valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del mismo.

Tratamiento de los datos y la finalidad del mismo.

• Tratamiento

Los datos personales de pacientes, estudiantes, trabajadores, contratistas y demás usuarios, proporcionados al Hospital Departamental Felipe Suarez E.S.E a través de los diferentes canales de atención dispuestos por la entidad, serán objeto de tratamiento de recolección, almacenamiento, uso, actualización, rectificación, circulación o supresión, según lo amerite cada caso, bajo el cumplimiento de la constitución y la ley.

• Finalidad

Los datos personales, dispuestos en las bases de información del Hospital Departamental Felipe Suarez E.S.E, serán usados con la finalidad específica para la que fueron suministrados, enmarcados dentro del cumplimiento de la misión institucional como prestador de servicios de salud y en el cumplimiento de las demás funciones administrativas, constitucionales y legales de la Entidad.

Análisis de vulnerabilidades

• En la entidad se presenta incumplimiento del cuidado tanto de los equipos informáticos como de la información física y digital, algunos de estos son: bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los mencionados activos de información, en papel reutilizable se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

• En algunas oficinas del hospital no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.

• La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.
• No hay control para el uso de memorias portátiles en los equipos del hospital, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
• Los documentos físicos que se manejan en la entidad no se han digitalizado, por lo tanto, están expuestos a perdidas y/o daños, esto debido, a que los sitios de almacenamiento en las oficinas no son los adecuados.

Propuesta de seguridad

• Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias y particulares de las oficinas.
• Implementar y socializar las políticas de seguridad y privacidad de la información con el personal de la institución.
• Implementar el sistema de documentación digital en la Entidad, con el propósito de reducir riesgos de pérdida de información física.
• Habilitar y tener en funcionamiento continuo el software para digitalización de documentos y gestión documental.

Plan seguro para la reserva de copias de seguridad

•Obtener una nube dedicada para la información de la institución con el fin de tener un respaldo en caso de accidentes referentes a pérdida de la misma.
•Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.

Implementación de políticas de seguridad para la información

El análisis permitió identificar que el Hospital Departamental Felipe Suárez E.S.E, requiere políticas de seguridad de la información; por lo cual, esto debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:
• Socialización y capacitación de temas de seguridad.
• Ambiente con la seguridad física adecuada.
• Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

Plan de capacitación

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:
• Detectar los requerimientos tecnológicos
• Determinar objetivos de capacitación para personal
• Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.

• Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
• Evaluar los resultados de cada actividad.

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.

📌 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.

Cuadro de indicadores					
Objetivo	**Indicador**	**Fórmula de cálculo**	**Meta**	**Frecuencia de Medición**	**Responsable**
Identificar y mitigar riesgos en la seguridad y privacidad de la información	Porcentaje de riesgos identificados	(Riesgos identificados / Riesgos totales) * 100	100% de los riesgos identificados	Mensual	Área de Sistemas
	Porcentaje de riesgos mitigados	(Riesgos mitigados / Riesgos identificados) * 100	80% de los riesgos mitigados	Trimestral	Área de Sistemas
Mejorar la capacidad de respuesta ante incidentes de seguridad	Tiempo promedio de respuesta ante incidentes	Suma de tiempos de respuesta / Número de incidentes	≤ 4 horas	Mensual	Área de Sistemas
	Número de simulacros realizados	Conteo de simulacros realizados	≥ 2 simulacros al año	Anual	Área de Sistemas
Proteger la integridad de los datos institucionales	Porcentaje de datos respaldados	(Volumen de datos respaldados / Volumen total de datos) * 100	100% de los datos respaldados	Mensual	Área de Sistemas
	Porcentaje de recuperación exitosa de datos	(Casos de recuperación exitosa / Total de casos) * 100	≥ 95% de casos recuperados exitosamente	Trimestral	Área de Sistemas
Incrementar la seguridad en la manipulación de información confidencial	Porcentaje de personal capacitado en ciberseguridad	(Número de personas capacitadas / Total de personales) * 100	100% personal	Semestral	Recursos humanos
Incrementar la trazabilidad en el uso de información institucional.	Porcentaje de sistemas con trazabilidad implementados.	(Sistemas con trazabilidad / Total de sistemas) * 100	100% de los sistemas	Anual	Área de Sistemas
Incrementar la trazabilidad en el uso de información institucional.	Número de auditorías realizadas	Conteo de auditorías realizadas	≥ 1 auditoría al año	Anual	Auditoria interna

Plan de Acción para el Tratamiento de Riesgo de Seguridad y Privacidad de la Información 2025					
Objetivo	**Actividad**	**Tareas**	**Ejecución**	**Responsable**	**Recursos**
Identificar y mitigar riesgos en la seguridad y privacidad de la información	Realizar diagnósticos de vulnerabilidades	Identificar y documentar riesgos en sistemas, equipos y datos.	Mensual	Área de Sistemas	Software de análisis de vulnerabilidades, personal técnico
	Implementar controles preventivos	Diseñar e implementar barreras técnicas y administrativas	Trimestral	Área de Sistemas	Manuales, protocolos, herramientas de monitoreo
	Digitalizar documentos físicos	Escanear y organizar documentos en una plataforma segura	Semestral	Oficina de Gestión Documental	Software de gestión documental, escáneres, personal capacitado
Mejorar la capacidad de respuesta ante incidentes de seguridad	Diseñar un plan de contingencia	Elaborar protocolos de reacción para fallos en sistemas y pérdida de datos.	Anual	Área de Sistemas	Manuales, personal especializado, simulaciones.
	Realizar capacitaciones en ciberseguridad	Sensibilizar al personal sobre buenas prácticas en la gestión de información	Trimestral	Área de Recursos Humanos	Proyector, material didáctico, sala de reuniones.
Proteger la integridad de los datos institucionales	Implementar un sistema de respaldo y recuperación de datos	Contratar un servicio de nube dedicado y establecer políticas de respaldo	Trimestral	Área de Sistemas	Servicio de nube, software de respaldo, presupuesto asignado
	Controlar el uso de dispositivos externos	Crear protocolos para el uso de memorias USB y dispositivos portátiles	Mensual	Área de Sistemas	Políticas escritas, carteles informativos, auditorías
Incrementar la seguridad en la manipulación de información confidencial	Socializar políticas de seguridad y privacidad.	Realizar talleres de sensibilización sobre normativas y protocolos.	Semestral	Área de Comunicaciones	Sala de reuniones, proyector, manuales.
	Monitorear y evaluar la seguridad en tiempo real	Implementar software de monitoreo continuo de accesos y actividad en la red	Mensual	Área de Sistemas	Software especializado, acceso a internet
Incrementar la trazabilidad en el uso de información institucional.	Configurar sistemas para registrar todas las acciones sobre los datos.	Implementar mecanismos de trazabilidad en plataformas informáticas	Anual	Área de Sistemas	Software de trazabilidad, personal técnico
	Evaluar resultados de implementación	Realizar auditorías para verificar el cumplimiento y efectividad de las medidas adoptadas.	Anual	Auditoria interna	Plan de auditoría, personal capacitado