

E.S.E. HOSPITAL

SAGRADO CORAZÓN DE JESÚS

Su salud, nuestra razón de ser

NIT. 812.000.300-0

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

2024 -2026

ALBERTO SEGUNDO VIDAL DIAZ

GERENTE

MAURICIO CONEO ROMERO

INGENIERO DE SISTEMAS

2024



CONTENIDO

INTRODUCCION.....	3
1. DEFINICIONES.....	4
2. OBJETIVOS.....	4
3. ALCANCE.....	5
4. MARCO REFRENCIAL.....	5
4.1 POLITICA DE ADMINISTRACION DE RIESGOS.....	5
5. METODOLOGIAS.....	7
6. DESARROLLO METODOLOGICO.....	8
6.1 OPORTUNIDAD DE MEJORA.....	10
7. RECURSOS.....	10
8. PRESUPUESTO.....	10
9. MEDICION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.....	10
9.1 MEDICION.....	11
10 CIBERGRAFIA.....	12

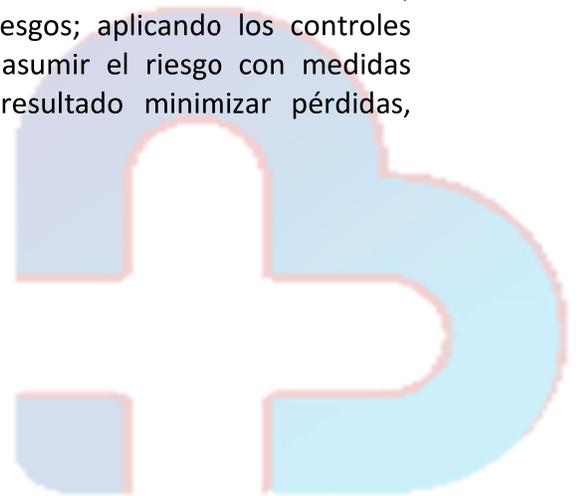


INTRODUCCIÓN

La información que genera constantemente el Hospital Sagrado Corazón de Jesús de Valencia Córdoba, es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), 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 planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente 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 para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que el Hospital Sagrado Corazón de Jesús de Valencia Córdoba adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Pública y como herramienta metodológica la utilizada por la Unidad Nacional para la Gestión del Riesgo de Desastres de la Presidencia de la República, además ha incorporado como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos. El Hospital Sagrado Corazón de Jesús de Valencia Córdoba acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.

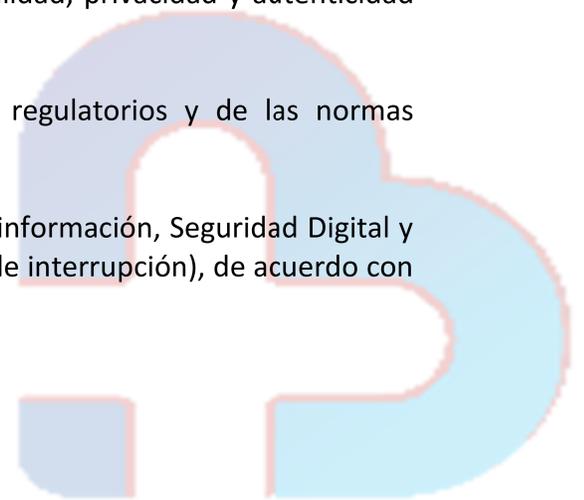


1. DEFINICIONES

- *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 posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- *Impacto:* son las consecuencias que genera un riesgo una vez se materialice.
- *Control o 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

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que el Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.
- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.
- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), de acuerdo con los contextos establecidos en la Entidad.



3. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad con buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)1: se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Hospital Sagrado Corazón de Jesús de Santa Fe de Antioquia.

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

4. MARCO REFERENCIAL

4.1 POLITICA DE ADMINISTRACION DE RIESGOS

El Hospital Sagrado Corazón de Jesús de Santa Fe de Antioquia, se compromete a mantener una cultura de la gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos, en las actividades desarrolladas por la Entidad asociadas con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas, iniciativas y proyectos del sector TIC, mediante mecanismos, sistemas y controles que detecten hechos asociados, de manera Integral, con la estrategia, la corrupción, seguridad y privacidad de la información, seguridad digital y continuidad de la operación, aspectos ambientales y de seguridad y salud en el trabajo, que puedan afectar el cumplimiento de los objetivos institucionales, el aprovechamiento al máximo los recursos destinados y la atención a nuestros grupos de interés El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) le permite al Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.



5. METODOLOGIAS

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)2:

Gestión	Actividades	Tareas	Responsable de la tarea	Fecha Inicio	Fecha Final
Gestión del Riesgo	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Equipo TICS	01-02-2024	30-11-2024
	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo TICS	01-03-2024	30-06-2024
	Identificación de Riesgo de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo TICS	01-03-2024	30-06-2024
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo TICS	01-03-2024	30-06-2024
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo TICS	01-05-2024	31-07-2024
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Equipo TICS	01-06-2024	31-08-2024
	Seguimiento Fase de Tratamiento	Seguimiento controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Equipo TICS	01-01-2024	20-12-2024
	Seguimiento valoración de riesgos residuales	Seguimiento a la valoración de los riesgos residuales	Equipo TICS	01-01-2024	20-12-2024
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de los planes de tratamiento y al seguimiento de la valoración de los riesgos residuales	Equipo TICS	01-01-2024	01-12-2024
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Equipo TICS	01-07-2024	20-12-2024
Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Equipo TICS	01-01-2024	27-12-2024	

6. DESARROLLO METODOLOGICO



Establecimiento del contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Hospital Sagrado Corazón de Jesús. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

Identificación del riesgo

Para la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Hospital Sagrado Corazón de Jesús se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos. La

falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar:

El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), el proceso dueño del riesgo, activo de información afectado, amenazas, vulnerabilidades y consecuencias.

Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

Valoración del riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Hospital Sagrado Corazón de Jesús se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública.

se realizará el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas. A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP

Definición y aprobación de mapas de riesgos y planes de tratamiento.

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio, los líderes de los procesos deberán emitir un memorando de la aprobación de los mapas de riesgos. De igual forma en este memorando aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en la matriz.

6.1 OPORTUNIDAD DE MEJORA

El Hospital Sagrado Corazón de Jesús no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

7. RECURSOS

El Hospital Sagrado Corazón de Jesús de Valencia Córdoba, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través del proceso de seguridad y privacidad de la información es responsable 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 - Riesgos de gestión, corrupción y seguridad digital Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
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

8. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

9. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, del Hospital San Juan de Dios aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del equipo de Seguridad y Privacidad de la Información teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados, así como el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, los profesionales del proceso de Seguridad y Privacidad de la Información realizan la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la información de la ESE Hospital San Juan de Dios de Santa Fe de Antioquia.

9.1 MEDICION

La medición se realiza con un indicador que está orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de la entidad.

HOJA DE VIDA DEL INDICADOR																					
1. Nombre del indicador: Controles del Sistema Integrado de Gestión gestionados																					
2. ¿Cual es el objeto del indicador? Identificar el porcentaje de los controles ejecutados del Sistema Integrado de Gestión El control es la medida que modifica el riesgo (procesos, políticas, ...)																					
3. ¿Cual es la definición del indicador? Controles por cada uno de los sistemas de gestión (SGC, SGSPI, SGSST, SGA) SGC: Sistema de Gestión de Calidad SGSPI: Sistema de Gestión de Seguridad y Privacidad de la Información SGSST: Sistema de Gestión de Seguridad y Salud en el Trabajo SGA: Sistema de Gestión Ambiental																					
4. ¿Cual es la fórmula de cálculo del indicador? (Promedio de controles gestionados del SGC + Promedio de controles gestionados del SGSPI + Promedio de controles gestionados del SGSST + Promedio de controles gestionados del SGA)/4																					
5. ¿Cuáles son las variables para el cálculo del indicador?. Relacione para cada variable la fuente de datos y la entidad responsable																					
	Variables	Fuente de datos para la variable (operación estadística o registro administrativo)	Entidad responsable																		
a.	Promedio de Controles gestionados del SGC	Mapa de Riesgos	MinTIC																		
b.	Promedio de Controles gestionados del SGSPI	Mapa de Riesgos	MinTIC																		
c.	Promedio de Controles gestionados del SGSST	Matriz de identificación de peligro y valoración de riesgo ocupacionales	MinTIC																		
d.	Promedio de Controles gestionados del SGA	Matriz de aspectos e impactos	MinTIC																		
6. ¿Cuál es la unidad de medida del indicador? Porcentaje																					
7. ¿Cuál es la tendencia del indicador? Positiva																					
8. ¿Cuál es el tipo de indicador? Eficacia <input checked="" type="checkbox"/> Eficiencia <input type="checkbox"/>																					
9. Parametrización del indicador																					
<table border="1"> <thead> <tr> <th colspan="3">Metas:</th> </tr> <tr> <th colspan="2">Rango</th> <th>Calificación</th> </tr> <tr> <th>Desde</th> <th>Hasta</th> <th></th> </tr> </thead> <tbody> <tr> <td>81%</td> <td>100%</td> <td>Alto</td> </tr> <tr> <td>61%</td> <td>80,0%</td> <td>Medio</td> </tr> <tr> <td>0%</td> <td>60,0%</td> <td>Bajo</td> </tr> </tbody> </table>				Metas:			Rango		Calificación	Desde	Hasta		81%	100%	Alto	61%	80,0%	Medio	0%	60,0%	Bajo
Metas:																					
Rango		Calificación																			
Desde	Hasta																				
81%	100%	Alto																			
61%	80,0%	Medio																			
0%	60,0%	Bajo																			



10. CIBERGRAFIA

<https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-laCiudadania/Transparencia/135830:Plan-de-seguridad-y-privacidad-de-lainformacion>

