1. JUSTIFICACIÓN

Administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

2. OBJETIVO GENERAL

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

3. OBJETIVOS ESPECÍFICOS

- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.

Elaboró:	Revisó:	Aprobó:
Lina María Castaño	Dora Elena Rodriguez A.	Carlos Fredy Carmona R.
Responsable SGSST	Profesional de Calidad	Gerente
Firma:	Firma:	Firma:
Fecha: 2018-07-06	Fecha: 2018-07-09	Fecha: 2018-07-10

- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una metodología confiable para la toma de decisiones y la planificación institucional.

4. ALCANCE

Esta guía, proporciona la metodología establecida por la E.S.E Hospital San Rafael Itagüí para la administración y gestión de los riesgos a nivel de la información de los procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo de seguridad y privacidad de la información.

5. DEFINICIONES

Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: situación externa que no controla la entidad y que puede afectar su operación

Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

Causa: medios, circunstancias y/o agentes que generan riesgos.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Compartir o transferir el riesgo: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.

Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.

Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.

Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

Impacto: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Información: Conjunto de datos procesados que constituyen un mensaje de conocimiento de determinada comunidad de personas.

Riesgo: eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la E.S.E Hospital San Rafael de Itagüí. La Alta Dirección es la responsable del fortalecimiento de los controles de administración del riesgo.

- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la E.S.E Hospital San Rafael de Itagüí al menos una vez al año. Si bien los Líderes que apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- Contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento, los procedimientos y los controles propios de la administración de riesgos

7. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo de seguridad y privacidad de la información; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: determinar los factores externos e internos del riesgo.
- Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Calificación y evaluación del riesgo inherente.
- Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Descripción del tratamiento a seguir

A continuación, se establecen las etapas descritas anteriormente por medio del panorama de riesgos para la seguridad y privacidad de la información.

PANORAMA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Riesgo	Fuente	Causa	Consecuencia	Controles existentes	Recurso afectado	Evaluación del riesgo	Descripción del tratamiento
Legal	Personas, alta Dirección	Divulgación de la información de usuarios, personal vinculado, contratistas, agremiados. Divulgación de información confidencial del Hospital sin previa autorización ni justificación.	Sanciones, demandas	Controles establecidos para la protección de la información y datos personales: Divulgación de la información: Derechos y deberes del personal vinculado, contratista, agremiados y usuarios Política de protección de datos personales Aviso de privacidad y protección de la información Autorizaciones para compartir y tratar la información confidencial y datos personales.	Financiero Reputacional	Critico	Se deben de cumplir a cabalidad los controles establecidos para la protección de la información y datos personales. Auditoria Anual
Planeación	Personas responsables	Falta de análisis previo frente a los cambios que se	Sanciones por incumplimientos o implementacio	Contratación de personal competente para los requerimientos.	Financiero Tiempo	Critico	Siempre que se generen requerimientos legales se debe

		hagan en la E.S.E Hospital San Rafael, de acuerdo a los requerimientos legales aplicables	nes inadecuadas		Reputac ional		hacer control por medio de un grupo interdisciplinario donde se tengan en cuenta todas las posibles variables de los procesos del Hospital
Tecnológi co	Personas responsable s del proceso de tecnología, sistemas e informática	Malos controles para custodiar la información. Fallas en el servidor Falencias en controles de sistemas para evitar intrusos en la red, robos de información.	Perdida de información valiosa del Hospital Filtración de información privada o confidencial	Servidor propio Personal competente vinculado al Hospital para atender todas las novedades y brindar soporte tecnológico permanente.	Financie ro Reputac ional	Critico	Mantenimiento y soporte constante al servidor, computadores y demás herramientas que contribuyen a la protección de la información
Legal	Todos los funcionarios de la E.S.E Hosp. San Rafael que tengan bajo su	No realizar backup necesarios para garantizar la protección de la información	Pedida definitiva de la información. Demandas y acciones legales en contra de la	Política de tratamiento de la información y datos personales.	Financie ro Reputac ional	Critico	Revisiones y mantenimientos al servidor o backup que se realicen.

	responsabilidad custodiar información		E.S.E Hosp. San Rafael				

8. METAS

- Cumplimiento del 100% de la política de tratamiento de bases de datos e información.
- Mantenimiento oportuno a los sistemas de custodia de la información: servidores, backup.
- Cumplir los tratamientos establecidos para prevenir, mitigar o eliminar los riesgos

9. CAMBIOS (*)

FECHA	NATURALEZA DEL CAMBIO	SOLICITANTE