E.S.E. HOSPITAL PADRE CLEMENTE GIRALDO

POLÍTICA DE ADMINITRACIÓN DEL RIESGO

ELABORÓ	REVISO	APROBÓ
Adriana María Pérez Z. Asesora Control Interno	Comité Institucional de Gestión y Desempeño	Victor Raúl Hoyos Hoyos Gerente

CONTENIDO

1. INTRODUCCION:

La Política de Administración del Riesgo, es la capacidad que tiene una entidad, para emprender acciones necesarias que le permitan el manejo de los eventos que pueden afectar negativamente el logro de los objetivos institucionales y protegerlos de los efectos ocasionados por su ocurrencia.

La Función Pública, dice que esta política: "*establece los lineamientos acerca del tratamiento, manejo y seguimientos de los riesgos, a través de la Alta Dirección de la entidad, del representante legal y con la participación del Comité Institucional de Coordinación de Control Interno".*

La Política de administración del riesgo, se encuentra en cabeza de la Alta dirección de las entidades, ya que constituye la base para la gestión del riesgo en todos los niveles organizacionales.

Es importante adoptar esta política de administración del riesgo, para dar respuesta a los requerimientos legales y permitir la administración de aquellos eventos que puedan llegar afectar el cumplimiento de metas y objetivos institucionales.

2. OBJETIVO:

Establecer los lineamientos y criterios institucionales que permitan la correcta identificación, análisis, valoración y tratamiento de los riesgos de gestión, de corrupción y seguridad digital, minimizando los efectos al interior de la ESE y asegurar el logro de la misión y los objetivos institucionales dentro de los procesos, procedimientos y actividades.

3. ALCANCE

La Política de Administración de Riesgos es aplicable a todos los procesos de la entidad y a los riesgos de seguridad digital y privacidad de la información de la E.S.E. Hospital Padre Clemente Giraldo.

4. BENEFICIOS DE LA GESTION DEL RIESGO

*Servir de apoyo en la toma de decisiones
*Garantizar la operación normal de la organización
* Minimizar la probabilidad de impacto de los riesgos
*Mejorar la calidad de los procesos y sus servidores

*Incrementar la capacidad de la entidad para alcanzar sus objetivos
*Dotar de herramientas de control para hacer una administración más eficaz y eficiente

5. DEFINICIONES

ANALISIS DEL RIESGO: Es el conjunto de acciones, recursos y métodos para comprender la naturaleza del riesgo. Este proceso soporta la evaluación del riesgo y las relacionadas con el tratamiento del riesgo.

IMPACTO: Son las consecuencias que puedan ocasionar a la organización la materialización de un riesgo. (EL QUE)

CONTROL: Es la medida que modifica el riesgo. Los controles pueden ser procesos, políticas, practicas u otras acciones dentro del sistema de administración del riesgo

EL CONTEXTO: Son los parámetros internos y externos que deben ser tenidos en cuenta en la gestión del riesgo y el punto de partida para la evaluación y el estable cimiento de políticas de gestión del riesgo.

EVALUACIÓN DEL RIESGO: Es el proceso utilizado para determinar las prioridades del sistema de administración del riesgo y su tratamiento para determinar si el riesgo, su magnitud o ambos se puedan considerar aceptables o tolerables.

EVENTO: Incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado, este puede ser una o más ocurrencias y atribuido a una o más causas.

GESTIÓN DEL RIESGO. Son los principios y metodología para gestión eficaz del riesgo, es decir, un conjunto de actividades coordinadas para dirigir y controlar los riesgos de la E.S.E. Hospital Padre Clemente Giraldo.

NIVEL DE RIESGO: Es la magnitud del riesgo de acuerdo a las consecuencias que se derivan del riesgo y la probabilidad de ocurrencia

CAUSA: Son aquellos factores internos y externos que solo o con combinación de otros pueden producir la materialización del riesgo.

CAUSA RAIZ: Es la causa principal o básica, o las razones por las que se produce el riesgo

CAUSA INMEDIATA: Son las circunstancias bajo las cuales se presenta el riesgo sin ser la causa principal para que se presente el riesgo

CONSECUENCIA: Son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, grupos de valor o partes interesadas.

RIESGO: Es el efecto que se causa sobre los objetivos de las entidades debido a eventos potenciales o sea la posibilidad de en incurrir en pérdidas por deficiencias, fallas en el recurso humano, los procesos, la tecnología, la infraestructura y las ocurrencias de acontecimientos externos.

RIESGO DE CORRUPCIÓN: Es la probabilidad de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado

RIESGO DE GESTIÓN: Es la posibilidad que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias

RIESGO DE SEGURIDAD INFORMATICA: Es la posibilidad de causar una perdida en un activo de información. Se combina con la probabilidad de un evento y sus consecuencias

RIESGO INHERENTE: Es el riesgo propio de la actividad desarrollada en una entidad en ausencia de acciones de dirección para modificar su probabilidad o impacto.

RIESGO RESIDUAL: Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Resulta después de aplicar los controles

TRATAMIENTO DEL RIESGO: Es el proceso para modificar el riesgo, que implica tomar decisiones para evitar o tomar el riesgo, retirar la fuente del riesgo, cambiar la probabilidad de ocurrencia del riesgo, cambiar las consecuencias del riesgo, compartir o trasferir el riesgo que se afectan con el riesgo y retener el riesgo a través de una decisión informada.

IDENTIFICACION DEL RIESGO: Facilita el análisis de la causa raíz, con el fin de evitar errores o riesgos, que se deben hacer de acuerdo a los factores de riesgo y a las tipologías de riesgos

VALORACION DEL RIESGO. Se establecen criterios para el análisis de la probabilidad e impacto del riesgo identificado y su severidad de acuerdo a unas tablas para el análisis de la probabilidad con enfoque en la exposición al riesgo que

le permiten a los líderes de procesos contar con elementos objetivos para su definición

6. ETAPAS PARA LA ADMINISTRACIÓN DE RIESGOS

6.1 RESPONSABILIDADES PARA LA GESTIÓN DE RIESGOS

La responsabilidad para la administración del riesgo está definida mediante el siguiente ESQUEMA DE LÍNEAS DE DEFENSA del Modelo estándar de control interno MECI:

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Gerente y Comité institucional de coordinación de control interno	• Define el marco para la gestión del riesgo y el control. • Analiza los riesgos al cumplimiento de planes (objetivos, metas, indicadores). • Define y adopta la política de administración de riesgos. • Garantizar el cumplimiento de los planes.
Línea de defensa 1	Subgerentes y líderes de procesos	• Identificar, evaluar, controlar y mitigar los riesgos. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos operativos identificados y proponer mejoras para su gestión. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Ejecutar procedimientos de control de riesgos. • Informar a la segunda línea defensa sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
Línea de defensa 2	Responsables de planeación, supervisores de contratos, líderes de procesos transversales (ambiental, calidad SGSST, seguridad	• Socializar la metodología de administración de riesgos y la herramienta para su gestión. • Asegurar que los controles y la gestión de riesgos por parte de Subgerentes y líderes de procesos sean adecuados y funcione adecuadamente. • Ejercer el control a la gestión de riesgos, a las funciones de cumplimiento, de seguridad y calidad.

	de pacientes) y comités	• Ayudar a los líderes de procesos a distribuir la información sobre riesgos a todos los servidores de la entidad.
Línea de defensa 3	Oficina de control interno o quien haga sus veces	• Informa sobre la efectividad del sistema de control interno y de la operación de primera y segunda línea de defensa, con enfoque basado en riesgos. • Realiza las auditorias con enfoque basado en riegos. • Informa a la alta dirección sobre la eficacia de la gestión de riesgos y del control interno. • Informa a la alta dirección acerca del funcionamiento de la primera y segunda línea de defensa.

RESPONSABILIDAD FRENTE AL RIESGO DE SEGURIDAD DIGITAL

El responsable del riesgo de la Seguridad Digital es el delegado por la Gerencia como líder de sistemas, el cual tiene los siguientes roles:

- Definir el procedimiento para la identificación y valoración de activos.
- Adoptar o adecuar el procedimiento para la gestión de riesgos de seguridad digital (identificación, análisis, evaluación y tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de los riesgos de seguridad digital y realizar recomendaciones sobre los controles para mitigar los riesgos.
- Apoyar el seguimiento a los planes de tratamiento de riesgos definidos.
- Informar a la Línea Estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

6.2 DECLARACIÓN DEL COMPROMISO INSTITUCIONAL PARA LA ADMINISTRACIÓN DEL RIESGO

La Empresa Social del Estado Hospital Padre Clemente Giraldo del Municipio de Granada, coherente con su política de calidad, con la estructura del Sistema de Control Interno definido dentro del Modelo Integrado de Planeación y Gestión (MIPG) y con los objetivos del Sistema Obligatorio de Garantía de la Calidad para la Atención en Salud, busca proteger a sus usuarios, bienes y recursos, de los potenciales riesgos asociados a la prestación del servicio, así mismo se compromete a establecer los mecanismos necesarios para evitar, reducir, compartir, transferir y asumir los riesgos relacionados con el desarrollo de sus procesos y que pudieran afectar negativamente a las personas, las instalaciones, los bienes y los equipos; para tal efecto realizará la identificación, análisis, valoración e intervención de los riesgos inherentes al quehacer institucional,

efectividad, aplicando la metodología que para el efecto recomiende el Departamento Administrativo de la Función Pública, contribuyendo de esta forma al logro de los principios de eficacia, eficiencia, eficacia, transparencia y en general al logro de los objetivos y a la misión de la Empresa.

6.3 IDENTIFICACIÓN DEL RIESGO

La gestión de riesgos comprende las actividades de:

- Análisis del contexto interno y externo.
- Identificación y análisis del riesgo.
- Valoración, evaluación, definición de controles para el tratamiento y seguimiento.

Análisis de objetivos estratégicos y de los procesos: este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

I**dentificación de los puntos de riesgo:** son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Identificación de áreas de impacto: el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos. En la siguiente Tabla se definen los principales factores de riesgo a tener en cuenta en entidad.

FACTOR	DEFINICIÓN		DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades quedeben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos

			Falta de capacitación, temas relacionados con el personal
			Hurto de activos
Talento humano	Incluye seguridad y salud en eltrabajo. Se analiza posible dolo e intención frente a la corrupción.		Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica dela entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con lainfraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público
Seguridad Digital		Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.	
Continuidad del Negocio		Relacionado con la interrupción no deseada o escenarios que afecten la vida de las personas o bienes de la Entidad, interrumpiendo sus funciones criticas parcial o totalmente.	
Grupos de Valor, Productos o servicios y prácticas de la Entidad		Fallas negligentes o involuntarias de las obligaciones frente a los Grupos de Valor y que impiden satisfacer una obligación profesional frente a estos.	
Relaciones Laborales		Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleos, salud o seguridad, del pago de demandas por daños personales o de discriminación.	

ESCENARIOS DE PÉRDIDA DE CONTINUIDAD

Este escenario corresponde a situaciones que agrupa la ocurrencia de uno o más riesgos que generan la pérdida de continuidad en las actividades institucionales.

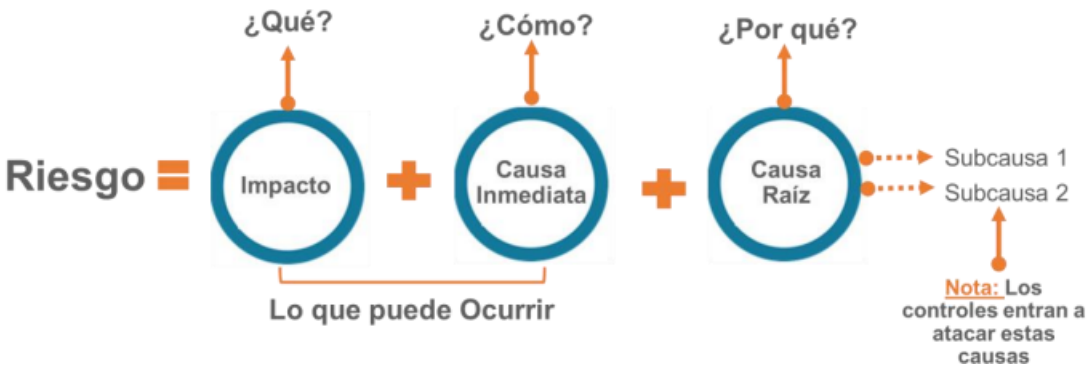
ESCENARIO	DESCRIPCIÓN
Emergencia Social	Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.
Colapso de infraestructura física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor

Desastre Tecnológico	Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos
Pandemia	Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado

Cuando se presentan eventos que materializan uno o más de los escenarios de continuidad del negocio la Entidad evalúa las características de la emergencia para autorizar la activación del plan de continuidad, designar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor, una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en el plan de continuidad de negocio para dar respuesta a la misma.

6.3.1 IDENTIFICACIÓN DE RIESGOS DE GESTIÓN

Describir el riesgo. Se aplicará el siguiente esquema:



Clasificación del riesgo: Finalmente se clasifica el riesgo en alguna de las siguientes opciones: ejecución y administración de procesos, fraude externo, fraude interno, fallas tecnológicas, relaciones laborales, usuarios, productos y prácticas, daños a activos fijos/ eventos externos, seguridad digital, grupos de valor, productos, servicios o prácticas.

6.3.2 IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN

Definición de riesgo de corrupción: Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Para que se configure un riego de corrupción es necesario que en su descripción concurran los componentes: ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Generalidades acerca de los riesgos de corrupción:

El mapa de riesgos de corrupción se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.

Consolidación: la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

Socialización: Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción.

Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

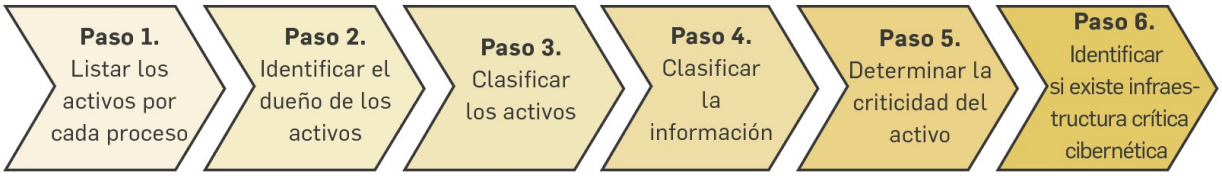
Monitoreo: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

Seguimiento: el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

6.3.3 IDENTIFICACION DE RIESGOS DE SEGURIDAD DIGITAL

Primero se deben identificar los activos de información, es decir, aquellos que tiene un valor relevante en el contexto de la gestión de la seguridad de la información, tales como: servicios web, redes, información física o digital, tecnologías de información TI y tecnologías de operación TO, que utiliza la organización para funcionar en el entorno digital.

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



Para la formulación se deberá considerar la siguiente tabla publicada por el Ministerio de Tecnologías de la Información y las Comunicaciones:

Tipo deactivo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemaslógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricosque por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos porhardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado

	estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Identificación del riesgo: se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para la caracterización de estos riesgos se deben considerar las siguientes tablas, además que se pueda consultar el Modelo Nacional de gestión de riesgos de seguridad de la información.

Amenazas comunes:

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida ala radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F

	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Amenazas dirigidas por el hombre:

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computadorActo fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con	Curiosidad	Asalto a un empleado
Fuente de amenaza	**Motivación**	**Acciones amenazantes**
entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Ganancia monetaria	Chantaje

Fuente: ISO/IEC 27005:2009, citado por Ministerio de Tecnologías de la Información y las Comunicaciones.

Vulnerabilidades Comunes:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
	Uso inadecuado de los controles de acceso al edificio

Lugar	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas comouso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005, citado por Ministerio de Tecnologías de la Información y las Comunicaciones.

6.4 VALORACIÓN DEL RIESGO

Análisis de riesgos: en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Criterios para evaluar la probabilidad en los diferentes tipos de riesgos:

Frecuencia de la Actividad	Nivel de Probabilidad
La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	Muy Baja - 20%
La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	Baja - 40%
La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	Media - 60%
La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	Alta - 80%
La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	Muy Alta - 100%

6.4.1 DETERMINAR EL IMPACTO EN RIESGOS DE GESTÓN Y DE SEGURIDAD DIGITAL

Determinar el impacto: Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Criterios para evaluar el impacto en los riesgos operativos o de gestión y de seguridad digital:

Afectación Económica (o presupuestal)	Pérdida Reputacional	Nivel de impacto
Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización	Leve 20%
Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores	Menor-40%
Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado 60%
Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	Mayor 80%
Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país.	Catastrófico 100%

6.4.2 DETERMINAR EL IMPACTO EN RIESGOS DE CORRUPCIÓN

Criterios para evaluar el impacto en los riesgos de corrupción:

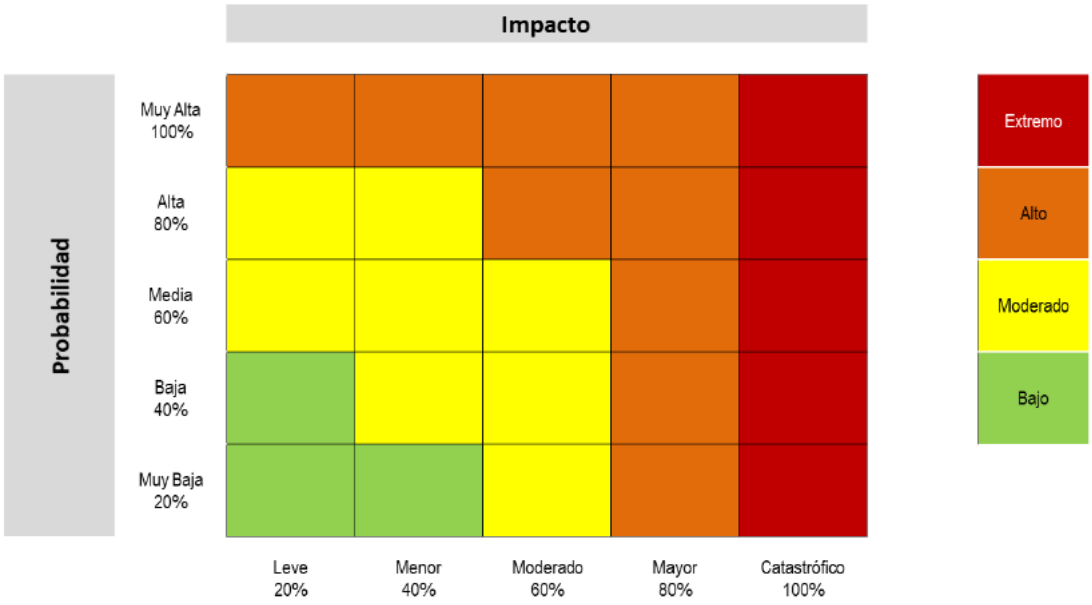
N° PREGUNTA	PREGUNTA: Si el riesgo de corrupción se materializara, podría...	RESPUESTA (SI -NO)
1	¿Afectar al grupo de funcionarios del proceso?	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	
3	¿Afectar el cumplimiento de la misión de la entidad?	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?	
5	¿Generar pérdida de confianza de la entidad afectando su reputación?	
6	¿Generar pérdida de recuros económicos?	
7	¿Afectar la generación de los productos o de la prestación del servicio?	
8	¿Dar lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien o del servicio o los recursos públicos?	
9	¿Generar pérdida de información de la entidad?	
10	¿Generar intervención de los órganos de control, de la Fiscalia u otro ente?	
11	¿Dar lugar a procesos sancionatorios?	
12	¿Dar lugar a procesos disciplinarios?	
13	¿Dar lugar a procesos fiscales?	
14	¿Dar lugar a procesos penales?	
15	¿Generar pérdida de credibilidad del sector?	
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?	
17	¿Afectar la imagen regional?	
18	¿Afectar la imagen nacional?	
TOTAL PREGUNTAS AFIRMATIVAS		
TOTAL PREGUNTAS NEGATIVAS		

CLASIFICACIÓN DE LAS RESPUESTAS DEL IMPACTO	IMPACTO	
Si responde afirmativamente de 1 a 5 preguntas	MODERADO	60%
Si responde afirmativamente de 6 a 11 preguntas	MAYOR	80%
Si responde afirmativamente de 12 a 18 preguntas	CATASTRÓFICO	100%

6.5 EVALUACIÓN DEL RIESGO

En la E.S.E. Hospital Padre Clemente Giraldo se establecen cuatro (4) zonas de severidad a partir del esquema de Mapa de calor, a través del cual se define el nivel de riesgo inicial (Riesgo Inherente).

El mapa de calor se presenta en el siguiente esquema:



VALORACIÓN DE CONTROLES

Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Tipologías de controles:

- Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

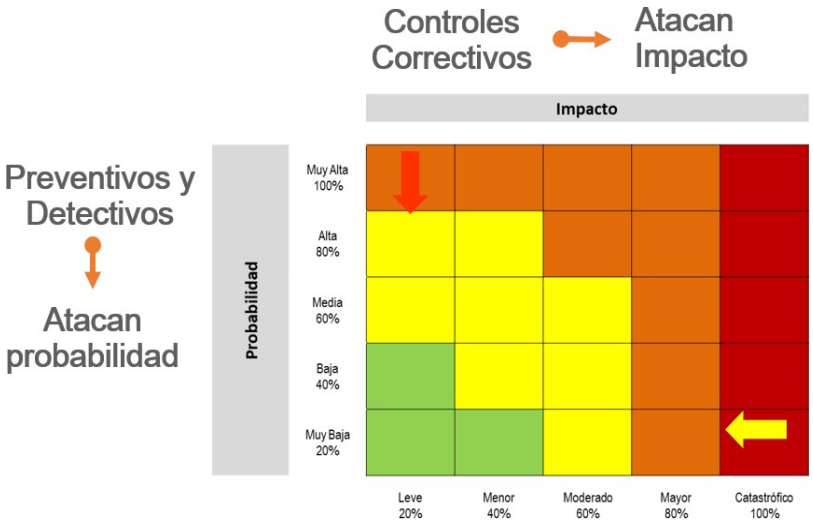
Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

Para la valoración del diseño e implementación de los controles se aplicarán como criterios los siguientes:

CARACTERÍSTICAS			DESCRIPCIÓN	PESO
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

Con la valoración de controles se obtiene el nivel de Riesgo residual, desplazando la calificación en el mapa de calor:



6.6 NIVELES DE RIESGO, TRATAMIENTO Y SEGUIMIENTO

Una vez determinado el nivel de riesgo residual el líder del proceso toma la decisión del tratamiento de sus riesgos, entre Aceptar, Reducir (transferir o mitigar) y Evitar, conforme a la siguiente tabla:

Nota: Cuando se trate de procesos nuevos se procede a partir del riesgo inherente.

NIVEL DE RIESGO ESTRATEGIAS DE TRATAMIENTO

NIVEL DE RIESGO	ESTRATEGIAS DE TRATAMIENTO
BAJO	**ACEPTAR** el riesgo y **ASUMIR** el mismo conociendo los efectos de su posible materialización, dando continuidad a sus controles establecidos. El seguimiento a sus controles es **SEMESTRAL** a través del instrumento definido.
MODERADO	**REDUCIR** el riesgo, estableciendo un plan de acción para fortalecer un control existente o implementar nuevo control que **MITIGUE** el nivel de riesgo. El seguimiento a su plan de acción y controles es **SEMESTRAL** a través del instrumento definido.
ALTO	**REDUCIR** el riesgo, estableciendo un plan de acción para fortalecer un control existente o implementar nuevo control que **MITIGUE** el nivel de riesgo. El seguimiento a su plan de acción y controles es **TRIMESTRAL** a través del instrumento definido. **O**

	REDUCIR el riesgo, considerando **TRANSFERIR** el riesgo tercerizando el proceso/ actividad o trasladar el riesgo a través de seguros o pólizas.
EXTREMO	**REDUCIR** el riesgo, estableciendo un plan de acción para fortalecer un control existente o implementar nuevo control que **MITIGUE** el nivel de riesgo. El seguimiento a su plan de acción y controles es **TRIMESTRAL** a través del módulo de riesgos SGI. **O** **REDUCIR** el riesgo, determinando **TRANSFERIR** el riesgo tercerizando el proceso/ actividad o trasladar el riesgo a través de seguros o pólizas. **O** **EVITAR** el riesgo, determinando **NO** realizar la actividad que genera este riesgo.

Nota: en el caso de riesgos de corrupción, estos no pueden ser aceptados.

6.7. REVISIÓN Y MONITOREO DE RIESGOS

- Los riesgos operativos se validan en cada vigencia atendiendo la metodología vigente.

- La periodicidad de seguimiento a los controles y plan de acción de cada riesgo está definida de acuerdo con la zona de severidad, así: Bajo y Moderado, seguimiento semestral; Alto y Extremo, trimestral.

- El líder o delegado de riesgos en cada proceso analiza los resultados del seguimiento y pueden determinar establecer un plan de mejoramiento ante cualquier desviación y socializa al interior de su dependencia las acciones a seguir.

- El líder o delegado de riesgos en cada proceso comunica, revisa y actualiza, el mapa de riesgo ante cualquier modificación en sus controles o plan de acción, derivados del seguimiento o de los eventos (materialización del riesgo).

Para los riesgos de corrupción el seguimiento por los líderes de los procesos en ejercicio del autocontrol y de forma independiente por el jefe de control interno o quien haga sus veces, así:

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

7. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

La E.S.E. Hospital Padre Clemente Giraldo determina que la gestión de riesgos en todos los procesos se realiza en la Matriz dispuesta por el departamento administrativo de la función pública, con los ajustes pertinentes para la entidad.

8. ACCIONES ANTE LA MATERIALIZACIÓN DEL RIESGO

CLASIFICACIÓN DEL RIESGO	RESPONSABLE	ACCIÓN
Corrupción	Líder de Proceso	• Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. • Identificar e implementar las acciones correctivas necesarias y establecer Plan de mejoramiento efectuando el análisis de causas y determinando acciones preventivas y de mejora. • Definir nuevos controles asociados al riesgo teniendo en cuenta el plan de mejoramiento definido.
	Oficina de Control Interno o quien hagas sus veces	• Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso.

Operativos	Líder de Proceso	• Informar inmediatamente por escrito a la segunda línea de defensa (líder de calidad o líder de seguridad del paciente) quienes llevarán un consolidado de eventos. • Identificar e implementar las acciones correctivas necesarias y establecer Plan de mejoramiento efectuando el análisis de causas y determinando acciones preventivas y de mejora. • Verificar los controles y plan de tratamiento del mapa de riesgos y tomar las acciones a que haya lugar. • En casos de eventos relacionados con la continuidad del negocio proceda: • Aplicar inmediatamente el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso). • Identificar e implementar las acciones correctivas necesarias y establecer Plan de mejoramiento efectuando el análisis de causas y determinando acciones preventivas y de mejora. • Definir nuevos controles asociados al riesgo teniendo en cuenta el plan de mejoramiento definido. • Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
De seguridad digital	Oficina de Control Interno o quien haga sus veces	• Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa (líder del sistema de gestión) con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso.
Riesgo no identificado	• Líder del proceso • Líder del sistema de gestión. • Oficina de Control Interno	• Informar a representante de la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso. • Incluir el riesgo en el mapa del proceso correspondiente.

	• Otro.	• Proceder a identificar, valorar y realizar seguimiento según metodología.