POLÍTICA GESTIÓN INTEGRAL DEL RIESGO

El Gerente de la Empresa Social del Estado Hospital Universitario de Santander y sus colaboradores se comprometen a gestionar los riesgos de los 13 subsistemas implementados en la ESE HUS que pueden impedir el cumplimiento de los objetivos institucionales, orientados a la toma de decisiones oportunas para minimizar efectos adversos al interior de la entidad efectuando su control y seguimiento a los riesgos por subsistema.

Los subsistemas de gestión del riesgo implementados en la ESE HUS son:

1. Procesos Operacional
2. Subsistema de Administración de Riesgo de Corrupción, Opacidad y Fraude – SICOF
3. Seguridad Digital, Seguridad de la Información y Protección de Datos
4. Subsistema de Administración del Riesgo de Lavado de Activos, de la Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva – SARLAFT/PADM
5. Seguridad y Salud en el Trabajo
6. Defensa Jurídica
7. Gestión del Riesgo Clínico – GRC
8. Estratégicos
9. Estándares y Ejes del Sistema Único de Acreditación – SUA
10. Impactos Ambientales
11. Emergencias y Desastres
12. Braquiterapia
13. Gestión Documental

VALORES

- Honestidad
- Compromiso
- Responsabilidad

PRINCIPIOS

- Trabajo en Equipo
- Transparencia

OBJETIVOS DE LA POLÍTICA

1. Efectuar seguimiento a los planes de acción de los riesgos por subsistema.
2. Medir la cultura del riesgo en los funcionarios y ejecutores del proceso que laboran en la E.S.E. Hospital Universitario de Santander.
3. Efectuar auditorías basadas en riesgos verificando la efectividad de los controles de los temas auditados y la identificación de posibles nuevos riesgos.

INDICADORES / MEDICIÓN DEL OBJETIVO

- Porcentaje de eficacia planes de acción de los riesgos priorizados.
- Porcentaje de apropiación de la cultura del riesgo en los colaboradores de la ESE HUS.
- Cumplimiento del plan anual de auditorías.

ALCANCE

La política de gestión integral del riesgo es aplicable a todos los subsistemas y procesos de la E.S.E. Hospital Universitario de Santander y a todas las acciones ejecutadas por los funcionarios y ejecutores de procesos durante el ejercicio de sus funciones, desde identificación, valoración, tratamiento, monitoreo, revisión, seguimiento de los riesgos y planes de mejora, así como la divulgación, capacitación y cultura en Gestión Integral del Riesgo.

RESPONSABILIDADES

El control y monitoreo de los diferentes subsistemas de gestión de riesgos implementados en la ESE HUS establece con base en el Modelo Integrado de Planeación y Gestión – MIPG denominado “Líneas de Defensa” las cuales incluyen línea de defensa, responsables y responsabilidades frente a los riesgos identificados en la institución.

Línea de defensa	Responsables	Responsabilidades
Línea Estratégica	Alta dirección. Comité Institucional de Coordinación de Control Interno. Comité de Gestión y Desempeño.	Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. Definir y aprobar la política de gestión del riesgo. Garantizar el cumplimiento de los planes de la entidad. Designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica. Designar un responsable y su suplente como oficial de cumplimiento del Subsistema de Administración del Riesgo de Lavado de Activos, de la Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva – SARLAFT/PADM, y el Subsistema de Administración de Riesgo de Corrupción, Opacidad y Fraude – SICOF, los cual deben pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica. Impulsar a nivel institucional la cultura en materia de prevención de la Corrupción, Opacidad y Fraude. Designar el Oficial de Protección de Datos Personales.
1° Línea de defensa	Líderes de procesos de la ESE HUS	Desarrollar e implementar procesos de control, y gestión de riesgo a través de sus etapas: identificación, medición, control y monitoreo, así como a las acciones de mejora. Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Orientar el desarrollo e implementación de políticas y

Línea de defensa	Responsables	Responsabilidades
		procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la ESE HUS y emprender acciones de mejoramiento para su logro. Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. Informar a la oficina de planeación (segunda línea) 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 y en la herramienta diseñada para ello.
2° Línea de defensa	Oficina Asesora de Desarrollo Institucional, así como todos los líderes de los subsistemas de gestión riesgo y el Comité de Gestión y Desempeño de la ESE HUS	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. Actualizar la documentación que soporta la Gestión del Riesgo del subsistema liderado. Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, este diseñados apropiadamente y funcionen como se pretende. Elaborar informe de Gestión del riesgo del Subsistema a cargo. Presentar al Comité Institucional de Coordinación de Control Interno el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los subsistemas de gestión del riesgo implementados. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, medición, control y monitoreo del riesgo. Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, media, controle y monitorice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. Promover ejercicios de autocontrol, autorregulación,

Línea de defensa	Responsables	Responsabilidades
		autogestión y autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del Comité Institucional de Coordinación de Control Interno.
3° Línea de defensa	Oficina Asesora de Control Interno	Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Desarrollo Institucional, en la identificación de los riesgos y diseño de controles. Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno. Recomendar mejoras a la política de operación para la gestión del riesgo.

De igual manera, la Oficina Asesora de Desarrollo Institucional lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología de Gestión de riesgo, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta designada para la gestión del riesgo.
- Liderar las mesas de trabajo de identificación del riesgo.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.
- Recordar, a los líderes de proceso y de subsistema de riesgo, la importancia de socializar los mapas de riesgos.
- Revisar que el cargue de información en el Sistema de Gestión de la Información esté acorde con lo aprobado.
- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de Riesgos de Proceso y SICOF, con los riesgos altos y extremos.

En cuanto al responsable de Seguridad Digital deberá cumplir respecto a la gestión del riesgo de seguridad digital lo siguiente:

- Definir el procedimiento para la Identificación y Valoración de Activos
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento)
- Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.
- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.

A continuación, se relaciona el responsable de segunda línea de defensa por cada subsistema de riesgo:

SUBSISTEMA DE GESTIÓN DE RIESGO	RESPONSABLE 2DA LÍNEA DE DEFENSA
Procesos Operacional	Jefe Oficina Asesora Desarrollo Institucional
Subsistema de Administración de Riesgo de Corrupción, Opacidad y Fraude – SICOF	Subgerente Administrativa y Financiera
Seguridad Digital, Seguridad de la Información y Protección de Datos	Profesional Especializado Unidad Funcional de Apoyo Tecnológico y de Información
Subsistema de Administración del Riesgo de Lavado de Activos, de la Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva – SARLAFT/PADM	Subgerente Administrativo y Financiero
Seguridad y Salud en el Trabajo	Profesional Especializado Unidad Funcional de Talento Humano
Defensa Jurídica	Jefe Oficina Asesora Jurídica
Gestión del Riesgo Clínico – GRC	Subgerencias técnico – científicas
Estratégicos	Jefe Oficina Asesora Desarrollo Institucional
Estándares y Ejes del Sistema Único de Acreditación – SUA	Jefe Oficina Asesora de Calidad
Impactos Ambientales	Profesional Especializado Unidad Funcional de Recursos Físicos y Servicios Básicos
Emergencias y Desastres	Profesional Especializado Unidad Funcional de Recursos Físicos y Servicios Básicos
Braquiterapia	Subgerente de Servicios de Alto Costo

SUBSISTEMA DE GESTIÓN DE RIESGO	RESPONSABLE 2DA LÍNEA DE DEFENSA
Gestión documental	Profesional Especializado Unidad Funcional de Apoyo Tecnológico y de Información

ETAPAS DE LA GESTIÓN DEL RIESGO

Identificación
El punto de partida para esta etapa es la identificación y documentación de todos los procesos, puesto que se debe revisar, evaluar, analizar el contexto interno y externo que permita identificar los factores de riesgo, riesgo asociados, entre otros. Así como, tener en cuenta el historial de riesgo materializados en la institución.

Medición
En esta etapa debe medirse la probabilidad de ocurrencia como el impacto de las consecuencias, para así determinar el perfil de riesgo de la entidad. Considerando un horizonte de tiempo de un año.
Cabe resaltar que las escalas de medición dependen de la metodología o norma de cada subsistema de riesgo.

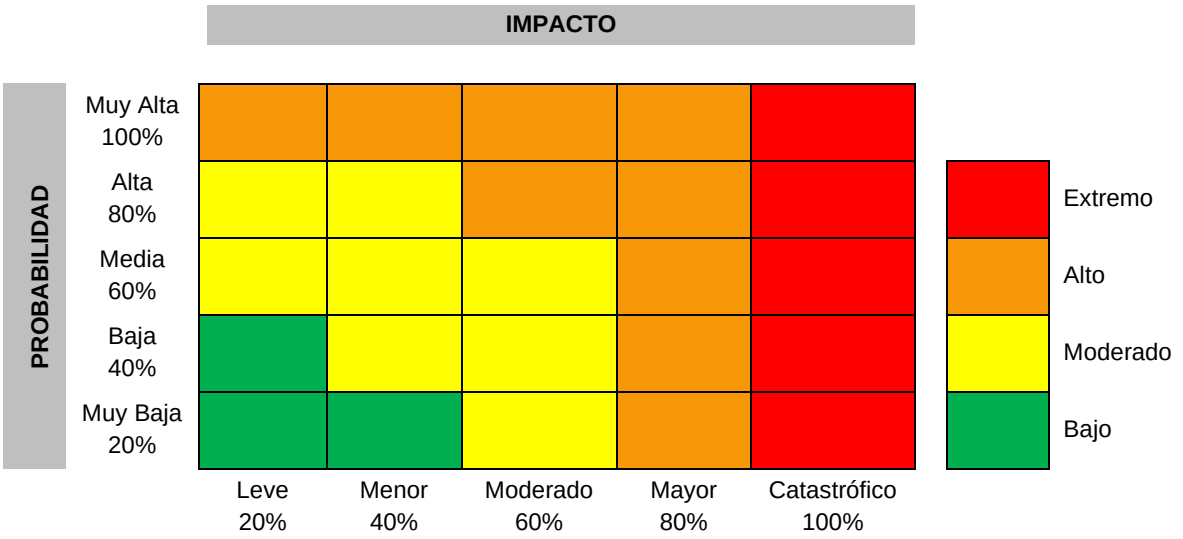
Control
Para esta etapa se debe establecer el tratamiento de los riesgos identificados, así mismo en los subsistemas que corresponda se deben diseñar e implementar controles que mitiguen la probabilidad, el impacto o ambos.

Monitoreo
En esta etapa se debe efectuar un seguimiento a todos los riesgos por subsistema para evitar la materialización de los mismos. Verificando el cumplimiento de los controles y las acciones que se definan para cada riesgo.

NIVEL DE ACEPTACIÓN DEL RIESGO

Subsistemas de Riesgos de Procesos Operacional, Estratégicos y SARLAFT/ PADM

Los subsistemas de riesgos implementados en la ESE HUS bajo la normatividad del Departamento Administrativo de la Función Pública – DAFP son: Procesos Operacional, Estratégicos; y Subsistema de Administración del Riesgo de Lavado de Activos, de la Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva – SARLAFT/PADM, para ellos se define el nivel de riesgo a partir del análisis de la probabilidad de ocurrencia del riesgo y el impacto de sus consecuencias, se determina la zona de riesgo definida en cuatro (4) escalas de severidad como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en los niveles Bajo y Moderado.



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, así:

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo dos veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	10%

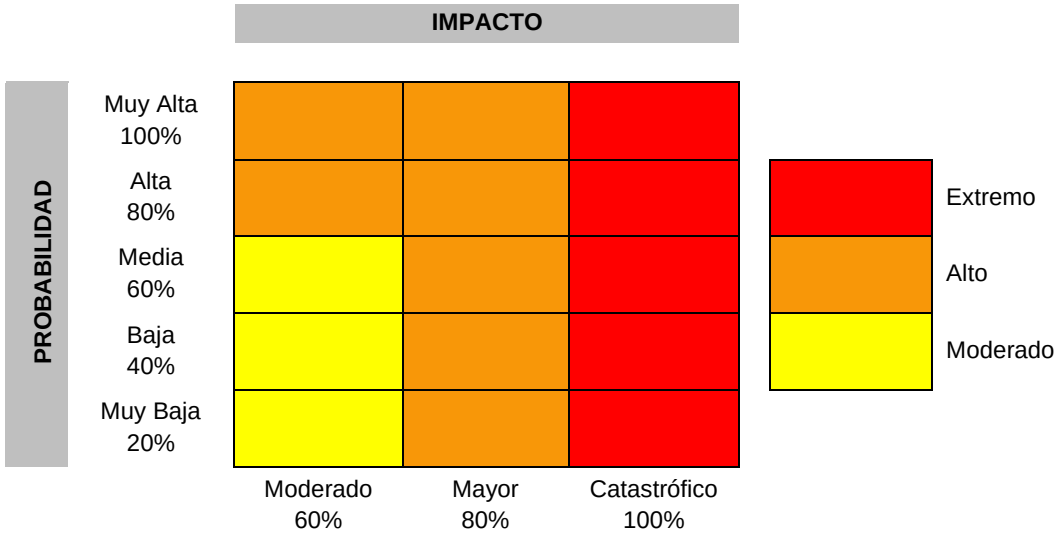
Los criterios que definen el impacto son de tipo: económicos y reputacionales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. Los niveles para calificar los impactos son:

	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.

	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto sostenido a nivel país.

Subsistema de Riesgos de SICOF

El Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude – SICOF implementado en la ESE HUS se rige bajo la normatividad del Departamento Administrativo de la Función Pública – DAFP, para este se define el nivel de riesgo a partir del análisis de la probabilidad de ocurrencia del riesgo y el impacto de sus consecuencias, se determina la zona de riesgo definida en tres (3) escalas de severidad como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en el nivel Moderado.



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, así:

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

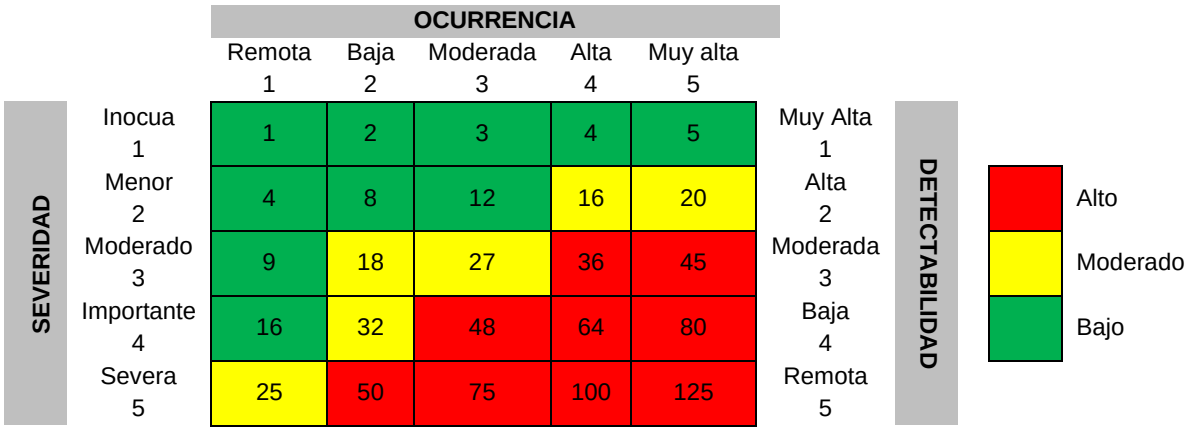
Para los riesgos de Corrupción, Opacidad y Fraude, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos

siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos:

No	Pregunta: Si el riesgo de Corrupción, Opacidad y Fraude se materializa 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 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 recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía 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	¿Genera pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Subsistemas de Riesgos de Estándares y Ejes del Sistema Único de Acreditación; y Gestión del Riesgo Clínico – GRC.

Los subsistemas de gestión del riesgo implementados en la ESE HUS a través de la Metodología de Análisis de Modo de Falla y Efecto – AMFE son: Estándares y Ejes del Sistema Único de Acreditación; y Gestión del Riesgo Clínico – GRC, para ellos se define el nivel de riesgo a partir del análisis de la severidad, ocurrencia y detectabilidad, se determina la zona de riesgo determinada en tres (3) escalas de riesgo como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en el nivel Bajo y Moderado.



La probabilidad de ocurrencia refiere a la estimación de la probabilidad de falla que realmente ocurra:

CALIFICACIÓN	CATEGORIA	CRITERIO
1	Remota	Casi nunca ocurre
2	Baja	Ocurre raramente
3	Moderada	Ocurre poco frecuente
4	Alta	Ocurre frecuentemente
5	Muy alta	Casi siempre ocurre

En cuanto a la severidad se refiere a la estimación de la severidad de cada falla en los desenlaces con los pacientes, si la falla ocurre:

CALIFICACIÓN	CATEGORIA	CRITERIO
1	Inocua	Sin daño al paciente
2	Menor	Daño temporal al paciente; necesita una hospitalización o una prolongación en la hospitalización
3	Moderada	Daño que requiere una intervención médica o quirúrgica para prevenir un daño permanente de una estructura o función corporal, incapacidad permanente parcial.
4	Importante	Daño de una función o estructura corporal.
5	Severa	Daño permanente o muerte.

En la detectabilidad se estima la probabilidad de que la falla no sea detectada:

CALIFICACIÓN	CATEGORIA	CRITERIO
1	Muy alta	El error será siempre detectado (95% – 100%), la causa se detecta en la recepción del producto sanitario cuando ingresa a la institución.
2	Alta	El error será frecuentemente detectado antes de que llegue el paciente (75% – 94%), la causa se detecta en el almacenamiento o instalación del producto sanitario.
3	Moderado	El error no será detectado frecuentemente antes de llegar al paciente (40% – 74%), la causa se detecta en la recepción del producto sanitario en el servicio o durante el mantenimiento o seguimiento del producto sanitario.

CALIFICACIÓN	CATEGORIA	CRITERIO
4	Baja	El error raramente será detectado antes de llegar al paciente (6% – 39%), la causa se detecta en el aislamiento del producto sanitario para su uso.
5	Remota	La detección no será posible en ningún punto del subsistema (0% – 5%), la falla se detecta cuando el producto sanitario entra en contacto con el paciente.

Subsistema de Riesgos de Impactos Ambientales

El subsistema de riesgos de impactos ambientales implementado en la ESE HUS se rige bajo la norma ISO 14001, para este se define el nivel de riesgo a partir del análisis de impacto (I), frecuencia (F), probabilidad (P), alcance (A), recuperación (R), control (C) y legislación (L), con el resultado de dicho análisis se determina la zona de riesgo definida en tres (3) niveles de severidad como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en el nivel Bajo y Medio.

VALORACIÓN TOTAL = I x F x P x A x C x L		
Rango de valoración	**Significancia ambiental**	**Calificación**
> 1 <= 300	Bajo	Impacto ambiental no significativo
>300 <= 700	Medio	Impacto ambiental crítico. Es decir, si no se control, puede llegar a ser un impacto significativo.
>700	Alto	Impacto ambiental significativo.

Criterio de evaluación	Valoración	Definición
Impacto (I)	-2	Negativo
	1	Positivo
Frecuencia (F)	5	Más de 10 veces al día o de 16 – 24 horas
	4	Diez veces al día o menos de 16 horas
	3	Dos o nueve veces por día u 8 horas
	2	Una vez por día o menos de 8 horas
	1	Una vez cada dos días o más
Probabilidad (P)	3	Alta
	2	Media
	1	Baja
Alcance (A)	3	Departamento o más
	2	Área metropolitana
	1	Sector
Recuperación (R)	3	No recuperación
	2	Se recicla / rehúsa
	1	Recuperación total
Control (C)	2	No existe control
	1	Existe control
Legislación (L)	3	Requisitos legales obligatorios
	2	Requisitos legales voluntarios
	1	No existe requisitos legales

Subsistema de Riesgos de Emergencias y Desastres

El subsistema de riesgos de emergencias y desastres implementado en la ESE HUS se rige bajo la Guía Hospitalaria para la Gestión del Riesgo de Desastres del Ministerio de Salud Colombia y el Manual de Planeamiento Hospitalario para Emergencias del Ministerio de Protección Social, para este se define el nivel de riesgo a partir del análisis de probabilidad de ocurrencia, estimación de impactos y nivel de preparación del centro hospitalario, con el resultado de dicho análisis se determina la zona de riesgo definida en tres (3) niveles de severidad como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en el nivel Bajo y Moderado.

TABLA DE PONDERACIÓN DEL MAPA DE CALOR		
Bajo	Moderado	Alto
3 – 30	31 – 50	51 – 81

Para la obtención de la ponderación del nivel de riesgo y clasificación en el mapa de calor se debe realizar las siguientes operaciones:

Suma de impactos (Humano, propiedad y empresarial) x Probabilidad = Puntaje del riesgo

Puntaje del riesgo x Nivel de preparación del Centro hospitalario = ***Puntaje Global***

ESTIMACIÓN DE IMPACTOS			
Impacto	**Puntaje de calificación de las consecuencias**		
	1	**2**	**3**
Humano o en las personas	Baja – sin víctimas	Moderada – algunas víctimas, pocas víctimas fatales	Alta – gran número de víctimas o muchas víctimas fatales
Propiedad o infraestructura	Poco o ningún daño de las instalaciones, sin pérdida del uso	Daño moderado a las instalaciones, tal vez se requiera una evacuación temporal o selectiva	Pérdida del uso del centro sanitario por un periodo prolongado
Empresarial o continuidad del negocio	Poca o ninguna pérdida del negocio o daño de la reputación	Cierta pérdida del negocio a corto plazo o cierto daño de la reputación	Pérdida importante a largo plazo o irreparable del negocio, o de la reputación

PROBABILIDAD DE OCURRENCIA		
PROBABILIDAD	**DESCRIPCIÓN**	**PUNTAJE**
Posible (Baja)	Fenómeno que puede suceder o que es factible su ocurrencia y del que no existe razones históricas, ni científicas para decir que no sucederá.	1
Probable (Moderada)	Fenómeno esperado, del cual existen razones o argumentos técnicos, científico y antecedentes para creer que sucederá.	2
Inminente (Alta)	Fenómeno esperado que tiene alta probabilidad de ocurrir.	3
NIVEL DE PREPARACIÓN DEL CENTRO HOSPITALARIO		**PUNTAJE**
Los planes existentes y los componentes de la infraestructura (equipos, personal, capacitación y recursos) son adecuados para la gestión de una situación de emergencia o desastre.		1

NIVEL DE PREPARACIÓN DEL CENTRO HOSPITALARIO	PUNTAJE
Los planes existentes o los componentes de la infraestructura o ambos, están presentes, pero tiene una o más deficiencias menores	2
Los planes o componentes de la infraestructura o ambos, faltan o son gravemente deficientes	3

Subsistema de Riesgos de Seguridad y Salud en el Trabajo

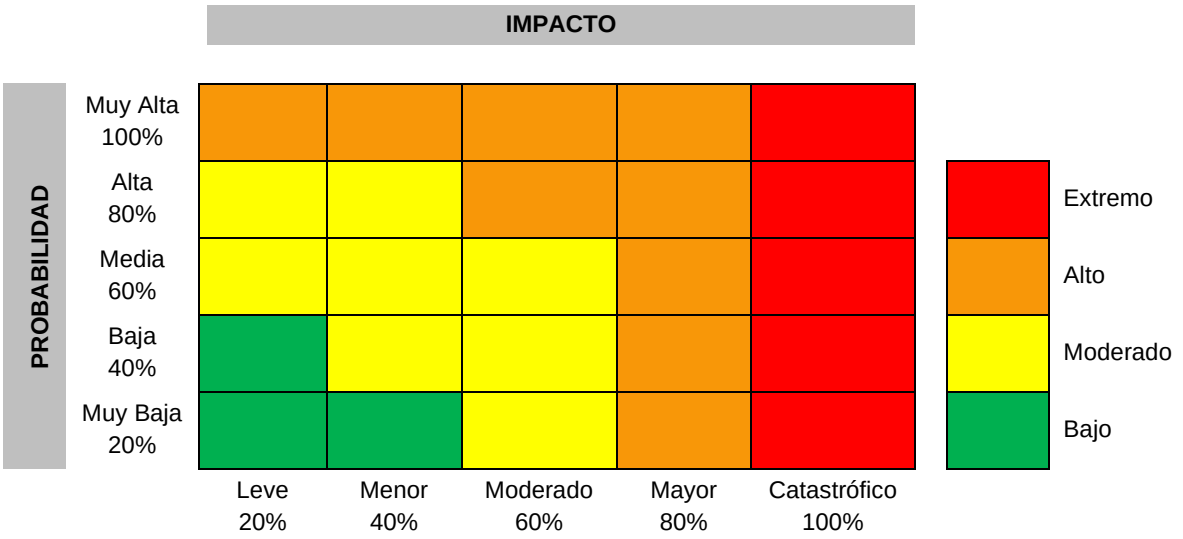
El subsistema de riesgos implementados en la ESE HUS a través de la metodología Guía Técnica Colombiana GTC 45 es Seguridad y Salud en el Trabajo, para se define el nivel de riesgo a partir del análisis de nivel de probabilidad (NP) y nivel de consecuencia (NC), se determina la zona de riesgo definida en tres (3) escalas de riesgo como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en el nivel Aceptable, Aceptable con Control Especifico y Mejorable.

NIVEL DEL RIESGO NR = NP x NC		NIVEL DE PROBABILIDAD (NP)							
		40 – 24		20 – 10		8 – 6		4 – 2	
Nivel de Consecuencias (NC)	100	I 4000 – 2400		I 2000 – 1200		I 800 – 600		II 400 – 200	
	60	I 2400 – 1440		I 1200 – 600		II 480 – 360		II 200	III 120
	25	I 1000 – 600		II 500 – 250		II 200 – 150		III 100 – 50	
	10	II 400 – 240		II 200	III 100	III 80 – 60		III 40	IV 20

NIVEL DEL RIESGO	VALOR NPR	SIGNIFICADO
I	4000 – 600	Situación crítica. Suspender actividades hasta que el riesgo este bajo control. Intervención urgente.
II	500 – 150	Corregir y adoptar medidas de control de inmediato. Sin embargo, suspenda actividades si el nivel del riesgo esta por encima o igual a 360.
III	120 – 40	Mejorar si es posible. Será conveniente justificar la intervención y su rentabilidad.
IV	20	Mantener las medidas de control existentes, pero se deberían considerar soluciones o mejorar y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es aceptable.

Subsistema de Riesgos de Gestión documental

El subsistema de riesgos de gestión documental implementado en la ESE HUS se rige bajo la normatividad del Plan Institucional de Archivos – PINAR del Archivo General de la Nación, para este se define el nivel de riesgo a partir del análisis de la probabilidad de ocurrencia del riesgo y el impactos de las consecuencias, con el resultado de dicho análisis se determina la zona de riesgo definida en cuatro (4) niveles de severidad como se presenta en la siguiente matriz de calor. Para la ESE HUS es aceptable un riesgo en el nivel Bajo y Moderado.



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, así:

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo dos veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	10%

Los criterios que definen el impacto son de tipo: económicos y reputacionales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. Los niveles para calificar los impactos son:

	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.

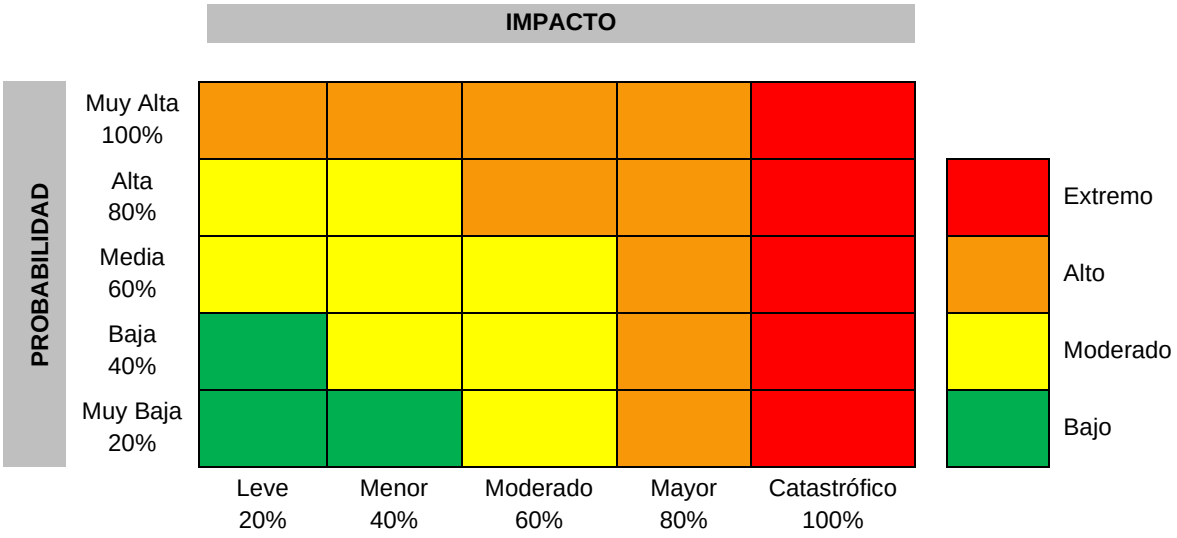
	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto sostenido a nivel país.

Subsistema de Riesgos de Seguridad digital, seguridad de la información y protección de datos

El subsistema de riesgos de Seguridad digital, seguridad de la información y protección de datos implementado en la ESE HUS se rige bajo la norma ISO 31000 e ISO 27005.

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Para este subsistema se define el nivel de riesgo a partir del análisis de la probabilidad de ocurrencia del riesgo y el impacto de las consecuencias, con el resultado de dicho análisis queda definida en cuatro (4) niveles de severidad como se presenta en la siguiente matriz de calor.



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 un (1) año, así:

	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo dos veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%

	Frecuencia de la actividad	Probabilidad
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	10%

Los criterios que definen los impactos son: cuantitativos o cualitativos. Los niveles para calificar los impactos son:

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO	
		Impacto (consecuencias) cuantitativo	Impacto (consecuencias) cualitativo
Insignificante	1	Afectación ≥ X% de la población. Afectación ≥ X % del presupuesto anual de la entidad. No hay afectación medio ambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
Menor	2	Afectación ≥ X% de la población. Afectación ≥ X % del presupuesto anual de la entidad. Afectación leve del medio ambiental requiere de ≥ X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
Moderado	3	Afectación ≥ X% de la población. Afectación ≥ X % del presupuesto anual de la entidad. Afectación leve del medio ambiental requiere de ≥ X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad integridad de la información debido al interés particular de los empleados y terceros.
Mayor	4	Afectación ≥ X% de la población. Afectación ≥ X % del presupuesto anual de la entidad. Afectación importante del medio ambiental requiere de ≥ X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad integridad de la información debido al interés particular de los empleados y terceros.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO	
		Impacto (consecuencias) cuantitativo	Impacto (consecuencias) cualitativo
Catastrófico	5	Afectación ≥ X% de la población. Afectación ≥ X % del presupuesto anual de la entidad. Afectación muy grave del medio ambiental requiere de ≥ X meses de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad integridad de la información debido al interés particular de los empleados y terceros.

Subsistema de Riesgos de Defensa Jurídica

El subsistema de riesgos de defensa jurídica implementado en la ESE HUS se rige bajo la Guía paso a paso para la elaboración de una política del daño antijuridico de la Agencia Nacional de la Defensa Jurídica del Estado – ANDJE.

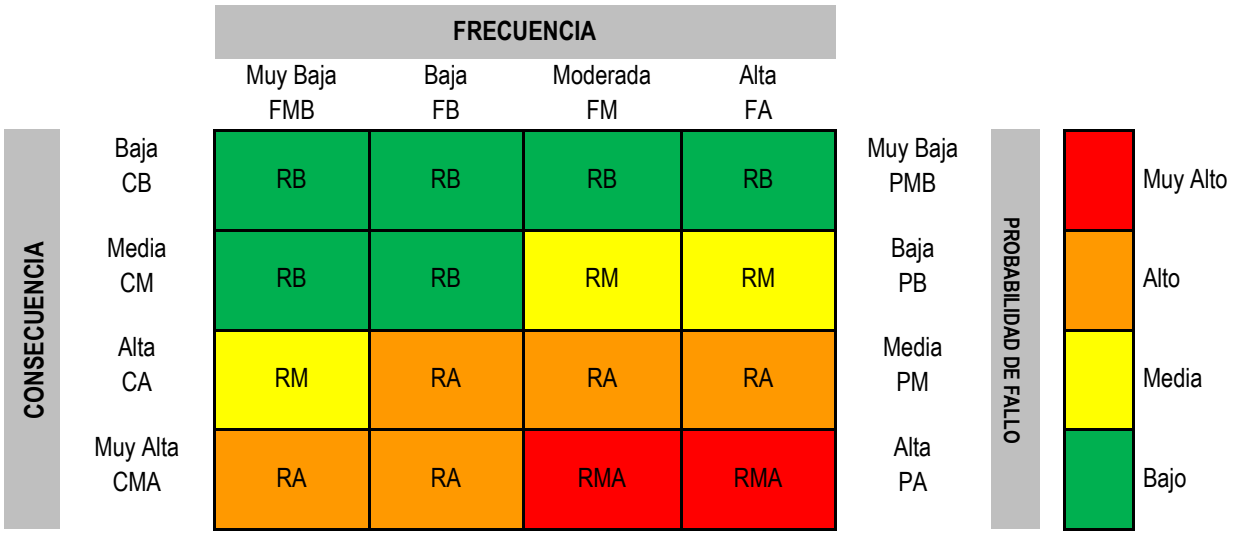
Los riesgos serán identificados en el COMITÉ DE CONCILIACIONES, en cual está a cargo de realizar la evaluación, seguimiento, control y plan de acción de este subsistema de riesgo.

Una vez se ha identificado la actividad litigiosa o los riesgos, la entidad debe priorizar la causa general sobre la cual va a seguir el proceso de formulación de la política de prevención del daño antijurídico. La ANDJE sugiere que en la decisión de priorización se tenga en cuenta la frecuencia y el valor con que se presenta la causa general.

Subsistema de Riesgos de Braquiterapia

El subsistema de riesgos de braquiterapia implementado en la ESE HUS se rige bajo la Aplicación del Método de la Matriz de Riesgos a la Radioterapia del Organismo Internacional de Energía.

La magnitud que caracteriza finalmente la secuencia accidental es el riesgo (R), que es función de las tres variables independientes, la frecuencia del suceso iniciador, la probabilidad de fallo de las barreras y la gravedad de las consecuencias. En el método de la matriz de riesgo, la variables no se cuantifican, sino que se clasifican en niveles. Se establecieron cuatro niveles para cada una de las variables. Las variables de frecuencia y probabilidad de fallo de barreras tienen niveles alto (A), medio (M), bajo (B), muy bajo (MB), mientras que la variable consecuencias tiene niveles muy alto (MA), alto (A), medio (M) y bajo (B). los criterios para asignar estos niveles los decide un grupo multidisciplinar de expertos, formado por Físico médicos, Médicos radioterapéuticas y personal administrativo especializado en el área de Radioterapia, la participación de diversos especialistas da una mayor objetividad al proceso.



TRATAMIENTO DEL RIESGO

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Asumir el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de Corrupción, Opacidad y Fraude podrá ser aceptado).

- **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 y/o acciones ciclo PHVA (Planear, Hacer, Verificar y Actuar).

- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

- **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Los riesgos de Corrupción, Opacidad y Fraude se pueden compartir, pero no se puede transferir su responsabilidad.

PERIODICIDAD

La E.S.E. Hospital Universitario de Santander identifica y valida los riesgos en cada vigencia, atendiendo la metodología vigente y define el plan de acción institucional, asegurando la articulación de éstos con los compromisos de cada proceso.

En cuanto al seguimiento a la administración del riesgo, y a las acciones de control, el responsable de cada subsistema de riesgo, trimestralmente efectúa el control y seguimiento de los riesgos que le corresponda, en donde:

- Analiza los resultados del seguimiento de las acciones realizados por la primera línea de defensa.
- Comunica las desviaciones según el nivel de aceptación del riesgo a la Oficina de Desarrollo Institucional y las acciones a seguir.
- Revisa la actualización del mapa de riesgo cuando se modifique las acciones o la ubicación del riesgo.

HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

La E.S.E. Hospital Universitario de Santander determina que el Módulo de Riesgos del Sistema de Gestión de la Información ALMERA es la herramienta para identificar, medir, controlar y monitorear los Subsistemas de Riesgos de: Procesos Operacional; Estratégicos; Seguridad digital, Seguridad de la información y protección de datos; Subsistema de Administración del Riesgo de Lavado de Activos, de la Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva – SARLAFT/PADM; Seguridad y Salud en el Trabajo; Defensa Jurídica; Gestión del Riesgo Clínico – GRC; Estándares y Ejes del Sistema Único de Acreditación – SUA; Impactos Ambientales; Emergencias y Desastres; Gestión Documental; y Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude – SICOF; por tanto, toda información asociada con los riesgos es provista por dicha herramienta, para lo cual la Oficina Asesora de Desarrollo Institucional identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información y dispone un manual de uso para el servicio de todos los procesos.

El subsistema de riesgo de braquiterapia será identificado, medido, controlado y monitoreado manualmente en el formato dispuesto para ello.

MATERIALIZACION DEL RIESGO

En caso de materialización de un riesgo identificado en algún subsistema que esta implementado en la ESE HUS los funcionarios y/o ejecutores de proceso deben aplicar las siguientes acciones de respuesta a riesgos:

SUBSISTEMA DE RIESGO	RESPONSABLE	ACCIÓN
Subsistema de Administración del Riesgo de Corrupción, la Opacidad y el Fraude – SICOF	Líder de proceso	• Informar al Jefe Oficina Asesora de Desarrollo Institucional y a la Oficina Asesora de Control Interno sobre el hecho encontrado. • Reportar el incidente en la herramienta Reporte de Materialización de Riesgo en ALMERA. • Una vez surtido el conducto regular establecido y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. • Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Actualizar el mapa de riesgos
	Oficina Asesora Desarrollo Institucional	• Informar al Comité Institucional de Coordinación de Control Interno del incidente o riesgo materializado. • Realizar acompañamiento al líder del proceso en el reporte y establecimientos de acciones correctivas. • Realizar seguimiento al plan de mejoramiento suscrito. • Realizar seguimiento a la actualización del mapa de riesgo.
	Oficina Asesora de Control Interno	En caso de conocer la materialización del Riesgo debe: • Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. • Una vez surtido el conducto regular establecido y dependiendo del alcance (normatividad asociada al hecho de Corrupción, Opacidad y Fraude 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, para revisar el mapa de riesgos.

SUBSISTEMA DE RIESGO	RESPONSABLE	ACCIÓN
Demás subsistemas de riesgo	Líder del proceso	• Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento. • Reportar el incidente en la herramienta Reporte de Materialización de Riesgo en ALMERA. • Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. • Analizar y actualizar el mapa de riesgos. • Informar al responsable del subsistema de riesgo involucrado sobre el hallazgo y las acciones tomadas.
	Líder del subsistema de riesgo	• Informar al Comité Institucional de Coordinación de Control Interno del incidente o riesgo materializado. • Realizar acompañamiento al líder del proceso en el reporte y establecimientos de acciones correctivas. • Realizar seguimiento al plan de mejoramiento suscrito. • Realizar seguimiento a la actualización del mapa de riesgo.
	Oficina Asesora de Control Interno	En caso de conocer la materialización del Riesgo debe: • Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

Para realizar el reporte de incidentes y materialización del riesgo, se debe realizar la siguiente ruta en la plataforma ALMERA.

1. Dirigirse a la pestaña de Plan Individual
2. Seleccionar la carpeta Mi Plan de Trabajo
3. Seleccionar Encuestas, dentro de este ítem nuevamente seleccionar Encuesta
4. Seleccionar “Reporte Materialización de Riesgo”
5. Diligenciar toda la información solicitada para generar un reporte completo, como se evidencia enseguida:

Fecha reporte *(Año – Mes – Día)*
Fecha de evento *(Año – Mes – Día)*
Área o proceso de ocurrencia *(Describir el área o proceso al que se le materializo el riesgo)*

Área o proceso que reporta *(Describir el área o proceso que reporta el evento)*
Descripción del riesgo
Describa las fallas que pudieron haber ocurrido
Observaciones
Reportado por
Cargo
Teléfono
Correo electrónico
Adjuntar archivo o evidencia

6. Guarde la información diligenciada y envíela