



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 1 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

POLÍTICA DE GESTIÓN DEL RIESGO





HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 2 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

CONTENIDO

POLITICA DE RIESGOS EN HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	3
1. OBJETIVO DE LA POLÍTICA.....	3
2. ALCANCE DE LA POLÍTICA.....	3
3. NIVELES DE ACEPTACION DEL RIESGO O TOLERANCIA AL RIESGO.	3
4. TÉRMINOS Y DEFINICIONES	4
5. RESPONSABILIDAD Y COMPROMISOS FRENTE AL RIESGO.....	6
6. TIPOLOGÍA DE RIESGOS EN EL HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	8
7. ESTRUCTURA PARA LA GESTION DEL RIESGO.....	8
7.1 IDENTIFICACIÓN DEL RIESGO.....	8
7.2 ANÁLISIS DEL RIESGO	9
7.2.1 Niveles para calificar la Probabilidad.....	9
7.2.2 Niveles para calificar el impacto.....	9
7.2.3 Determinación de la zona de riesgo inicial o inherente	13
7.3 TRATAMIENTO DEL RIESGO	13
7.4 IMPLEMENTACIÓN DE CONTROLES.....	14
7.4.1 Determinación del riesgo residual.....	16
7.5 MONITOREO DE LA ACTIVIDAD DE CONTROL.....	16
8 SEGUIMIENTO Y MONITOREO.....	17

ELABORACIÓN	REVISIÓN	APROBACIÓN
 César Fernando Zambrano Pineda Profesional de Apoyo para el proceso de Planeación	 Duver Dicson Vargas Rojas Presidente Comité Institucional de Gestión y Desempeño	 Duver Dicson Vargas Rojas Agente Especial Interventor
Fecha: 29/09/2020	Fecha: 30/09/2020	Fecha: 30/09/2020



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 3 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

POLITICA DE RIESGOS EN HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE

El Hospital Regional de II nivel de San Marcos ESE define su política del riesgo atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en Entidades Públicas, expedida en octubre de 2018 por la Dirección de Gestión y Desempeño Institucional del Departamento Administrativo de la Función Pública, como mecanismo para identificar, analizar, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar el logro de los objetivos institucionales.

Como Empresa Social del Estado, la entidad formula y adopta esta política orientada a la preservación de los recursos institucionales que permitan garantizar la continuidad en la prestación de los servicios de salud a la población usuaria, frente a los diferentes riesgos a los que se encuentra expuesta en cumplimiento de su objeto misional.

1. OBJETIVO DE LA POLÍTICA

Adoptar criterios institucionales que orienten al Hospital Regional de II nivel de San Marcos en la correcta identificación, análisis, valoración y administración de todo tipo de riesgos; que, de materializarse pueden afectar el logro de los objetivos institucionales, logrando que el proceso de toma de decisiones sea oportuno y se minimicen los efectos adversos al interior de la Entidad, lo anterior con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de Valor, así como fomentar y fortalecer el enfoque preventivo.

2. ALCANCE DE LA POLÍTICA

La política de riesgos se aplica a todos los procesos y subprocesos de la Entidad y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones y actividades.

3. NIVELES DE ACEPTACION DEL RIESGO O TOLERANCIA AL RIESGO

El Hospital Regional de II nivel de San Marcos, aceptará únicamente los riesgos que, según la medición expuesta por el Departamento Administrativo de la Función Pública en la Guía para la administración del riesgo y el diseño de controles en Entidades Públicas, se encuentren en la zona de riesgo BAJA, para lo anterior no se formularán controles; sin embargo, se realizará monitoreo anual a estos riesgos revalorando el impacto y la probabilidad de ocurrencia; al momento



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 4 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

de observar que alguno de ellos se incrementa, se realizará lo pertinente para darle tratamiento al riesgo.

Respecto a los riesgos de corrupción, **ninguno de estos podrá ser aceptado** por la entidad, para la totalidad de los riesgos identificados e incluidos en el respectivo mapa, se implementarán controles que conlleven a disminuir, evitar o compartir el riesgo.

4. TÉRMINOS Y DEFINICIONES

Activo: En el contexto de seguridad digital, son los elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Administración de Riesgos: Un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.

Amenazas: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis de Riesgos: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Apetito del Riesgo: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

Control: Acciones encaminadas a reducir la probabilidad de ocurrencia o el impacto que pueda generar la materialización del riesgo.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 5 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Establecimiento del Contexto: Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo de este, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Gestión del Riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Identificación del Riesgo: Se realiza determinando las causas, fuentes del riesgo y los eventos con base en el análisis de contexto para la entidad y del proceso, que pueden afectar el logro de los objetivos. Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos y los objetivos institucionales.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de Riesgos: Documento con la gestión resultante de la gestión del riesgo.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Política de Administración del Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO31000 Numeral 2.4). La gestión o Administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

Probabilidad: Medida para estimar la posibilidad de que ocurra un evento. Puede ser medida con criterios de frecuencia o factibilidad.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 6 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

Riesgo de Corrupción: Posibilidad de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. El riesgo en su tendencia más común es valorado como una amenaza, en este sentido, los esfuerzos institucionales se dirigen a reducirlo, evitarlo, transferirlo o mitigarlo; sin embargo, el riesgo puede ser analizado como una oportunidad, lo cual implica que su gestión sea dirigida a maximizar los resultados que éstos generan.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo Residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

Tolerancia al Riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.

Tratamiento del Riesgo: Es la respuesta establecida para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

5. RESPONSABILIDAD Y COMPROMISOS FRENTE AL RIESGO

LÍNEA DE DEFENSA	RESPONSABILIDAD
Línea Estratégica: Alta dirección y Comité Institucional de	<ul style="list-style-type: none">– Establecer la Política de Administración del Riesgo– Establecer las políticas de operación encaminadas a controlar los riesgos que pueden llegar a incidir en el cumplimiento de los objetivos institucionales– Hacer seguimiento a la adopción, implementación y aplicación de controles– Analizar las evaluaciones de la gestión del riesgo, elaboradas por la segunda



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 7 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

Coordinación de Control Interno	<p>línea de defensa</p> <ul style="list-style-type: none"> – Retroalimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles.
Primera Línea: Subgerentes y Líderes de proceso y subprocesos	<ul style="list-style-type: none"> – Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales – Definir y diseñar los controles a los riesgos – A partir de la política de gestión del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecer los mapas de riesgos – Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Implementar procesos para identificar, disuadir y detectar fraudes; y revisar la exposición de la entidad al fraude con el auditor interno de la entidad o quien haga sus veces – Efectuar seguimiento a los riesgos y controles de su proceso – Informar periódicamente a la alta dirección sobre el desempeño de las actividades de gestión de riesgos de la entidad
Segunda Línea: Servidores responsables de monitoreo y evaluación de controles y gestión del Riesgo – Jefe Oficina de Planeación o quien haga sus veces	<ul style="list-style-type: none"> – Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada – Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude – Asegurar que los riesgos son monitoreados en relación con la política de gestión de riesgos establecida para la entidad – Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento – Consolidar los mapas de riesgos – Establecer un líder de la gestión de riesgos para coordinar las actividades en esta materia – Elaborar informes consolidados para las diversas partes interesadas – Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar – Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas – Suministrar información a la alta dirección sobre el monitoreo llevado a cabo a los indicadores de gestión, determinando si el logro de los objetivos está dentro de las tolerancias de riesgo establecidas
Tercera Línea: Oficina de Control Interno	<ul style="list-style-type: none"> – Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa – Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de control interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. – Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías – Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad – Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas – Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos – Evaluar si los controles están presentes (en políticas y procedimientos) y funcionan, apoyando el control de los riesgos y el logro de los objetivos establecidos en la planeación institucional



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 8 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

6. TIPOLOGÍA DE RIESGOS EN EL HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se han identificado los siguientes tipos de riesgos en los cuales podría incurrir la institución y que se incluirán en los mapas de riesgos de gestión, de seguridad digital y de corrupción:

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgos de Corrupción: Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

7.1 IDENTIFICACIÓN DEL RIESGO

Como primera medida es necesario realizar la identificación del riesgo para lo cual se implementa la matriz de definición, en esta también se incluyen las causas que



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 9 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

generan el riesgo y las consecuencias de su materialización; esta identificación se lleva a cabo dando respuesta a los siguientes interrogantes: ¿Qué puede suceder?, ¿Cómo puede suceder?, ¿Cuándo puede suceder? y, ¿Qué consecuencias tendría su materialización?, la respuesta a las anteriores preguntas deberá ser incluida en la descripción del riesgo.

Al momento de identificar riesgos de corrupción, es importante anotar que estos tienen que cumplir con cuatro características: 1) Que haya acción u omisión, 2) Que se observe uso del poder, 3) Que se presente desviación de la gestión de lo público y 4) Que las anteriores 3 condiciones tengan como fin un beneficio privado o particular.

7.2 ANÁLISIS DEL RIESGO

Con el fin de estimar la zona de riesgo inicial o inherente, se debe establecer la probabilidad de ocurrencia del riesgo y su impacto, para lo cual se tienen en cuenta las siguientes directrices:

7.2.1 Niveles para calificar la Probabilidad

Como probabilidad se entiende la posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia (teniendo en cuenta el histórico de la entidad) o factibilidad (teniendo en cuenta que tan propensa es su materialización), la probabilidad se debe determinar a partir de la siguiente escala:

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

7.2.2 Niveles para calificar el impacto

Por Impacto se entienden las consecuencias que para la institución podría acarrear la materialización del riesgo; la medición del impacto varía según el tipo de riesgo, sea este de gestión, de corrupción o de seguridad digital; se debe medir a partir de las siguientes especificaciones.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 10 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

7.2.2.1 Riesgos de Gestión:

Niveles para calificar el Impacto	Impacto Cuantitativo	Impacto Cualitativo
CATASTRÓFICO	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 50\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 50\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 50\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 50\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 20\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 20\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 20\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 20\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 5\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 10\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 5\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 5\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	<ul style="list-style-type: none"> - Impacto que afecte la ejecución 	<ul style="list-style-type: none"> - Interrupción de las operaciones de la



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 11 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

	<p>presupuestal en un valor $\leq 1\%$</p> <ul style="list-style-type: none"> - Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 5\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\leq 1\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\leq 1\%$ del presupuesto general de la entidad. 	<p>Entidad por algunas horas.</p> <ul style="list-style-type: none"> - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\leq 0,5\%$ - Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 1\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\leq 0,5\%$ - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\leq 0,5\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> - No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

7.2.2.2 Riesgos de Seguridad Digital:

NIVEL	VALOR DE IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		Impacto Cuantitativo	Impacto Cualitativo
CATASTRÓFICO	5	<p>Afectación $\geq 50\%$ de la población</p> <p>Afectación $\geq 15\%$ del presupuesto anual</p> <p>Afectación medioambiental muy grave que requiere ≥ 10 años de recuperación</p>	<p>Afectación muy grave de la integridad de la información debido al interés particular de empleados y terceros.</p> <p>Afectación muy grave de la disponibilidad de la información debido al interés particular de empleados y terceros.</p> <p>Afectación muy grave de la confidencialidad de la disponibilidad de la información debido al interés particular de empleados y terceros.</p>
MAYOR	4	<p>Afectación $\geq 20\%$ de la población</p> <p>Afectación $\geq 10\%$ del presupuesto anual</p> <p>Afectación medioambiental importante que requiere ≥ 5 meses de recuperación</p>	<p>Afectación grave de la integridad de la información debido al interés particular de empleados y terceros.</p> <p>Afectación grave de la disponibilidad de la información debido al interés particular de empleados y terceros.</p> <p>Afectación grave de la confidencialidad de la disponibilidad de la información debido al interés particular de</p>



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 12 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

			empleados y terceros.
MODERADO	3	Afectación $\geq 10\%$ de la población Afectación $\geq 5\%$ del presupuesto anual Afectación medioambiental leve que requiere ≥ 3 semanas de recuperación	Afectación moderada de la integridad de la información debido al interés particular de empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de empleados y terceros. Afectación moderada de la confidencialidad de la disponibilidad de la información debido al interés particular de empleados y terceros.
MENOR	2	Afectación $\geq 5\%$ de la población Afectación $\geq 2\%$ del presupuesto anual Afectación medioambiental leve que requiere ≥ 2 días de recuperación	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad
INSIGNIFICANTE	1	Afectación $\geq 1\%$ de la población Afectación $\geq 1\%$ del presupuesto anual No hay afectación medioambiental	Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad

7.2.2.3 Riesgos de Corrupción: Para medir el impacto en los riesgos de corrupción debe darse respuesta a 18 interrogantes, el nivel de impacto resultará de la cantidad de respuestas afirmativas a estas preguntas:

No.	Pregunta: Si el riesgo de corrupción se materializa podría...	Respuesta	
		Sí	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 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 o servicios o los 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	¿Generar pérdida de credibilidad del sector?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		



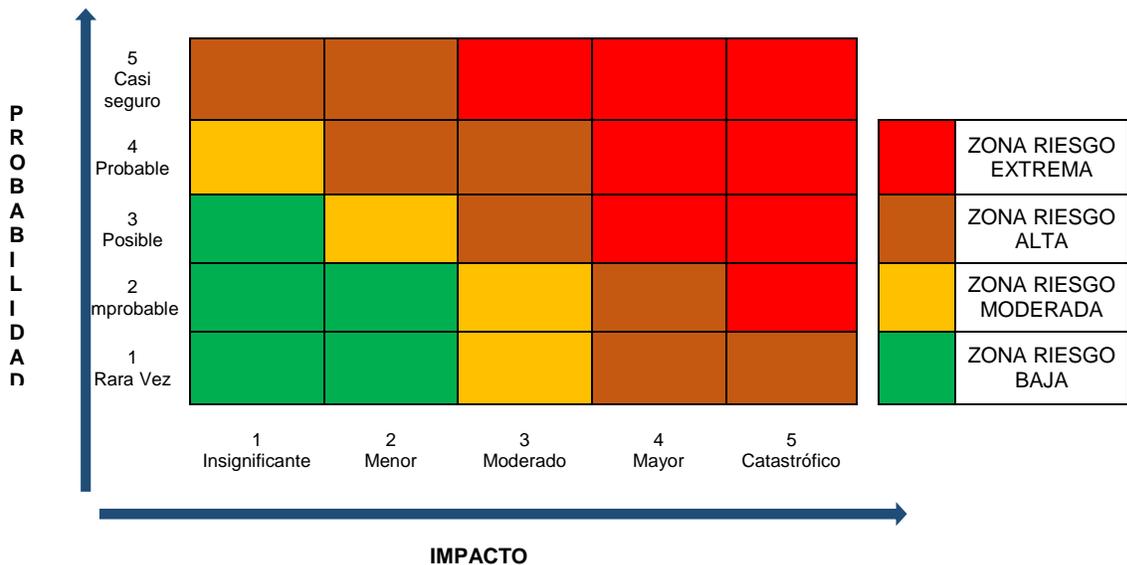
HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 13 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

18	¿Afectar la imagen nacional?		
TOTAL			
Clasificación del Riesgo: Moderado _____ Mayor _____ Catastrófico _____			

Calificación de Riesgo de Corrupción Impacto	
Respuestas Afirmativas	Descripción
1 – 5	Moderado
6 – 11	Mayor
12 – 18	Catastrófico

7.2.3 Determinación de la zona de riesgo inicial o inherente

Acogiendo la Matriz de riesgo sugerida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de octubre de 2018, la medición de los riesgos de proceso y subproceso se hace a través de la tabla de probabilidad e impacto como se mencionó anteriormente, para ello se utiliza el mapa de calor (ver gráfico). Se toma la calificación de probabilidad (resultante de la tabla Matriz de Priorización de probabilidad), se ubica la calificación de la probabilidad en la fila y la del impacto en la columna correspondientes, estableciendo el punto de intersección de las dos, que corresponderá al nivel de riesgo.



7.3 TRATAMIENTO DEL RIESGO

La finalidad del tratamiento del riesgo es lograr que la zona de riesgo residual disminuya respecto a la zona de riesgo inherente, para lograr esto, los dueños de los procesos deberán tener en cuenta la importancia del riesgo, lo cual incluye el



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 14 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. De cualquier forma, en todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo. **Ningún riesgo de corrupción podrá ser aceptado.**

Para el tratamiento de los riesgos en el Hospital Regional de II nivel de San Marcos ESE, se tendrán en cuenta los siguientes criterios:

Aceptar el Riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Esto es posible únicamente para los riesgos ubicados en la zona de riesgo baja en el mapa de calor.

Dentro de las alternativas de tratamiento para los riesgos iniciales o inherentes que queden ubicados en las zonas de riesgo moderada, alta o extrema se tendrá:

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.

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.

7.4 IMPLEMENTACIÓN DE CONTROLES

El tratamiento del riesgo se realiza mediante la implementación de controles con la finalidad de realizar un monitoreo constante a estos; teniendo en cuenta lo mencionado anteriormente, los controles deben estar encaminados a reducir, evitar o compartir el riesgo, lo cual se logra implementando acciones que gestionen las causas y/o que disminuyan las consecuencias.

Para realizar una correcta formulación del control se deben seguir los siguientes pasos:

1. Definir el responsable de llevar a cabo la actividad de control



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 15 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

2. Establecer la periodicidad para su ejecución

3. Indicar cuál es el propósito del control

4. Mencionar como se realiza la actividad de control

5. Indicar que pasa con las observaciones o desviaciones resultantes

6. Dejar evidencia de la ejecución del control

Posterior a la formulación del control, este debe ser evaluado para determinar su solidez, se realiza respecto a seis criterios como se muestra a continuación:

CRITERIO DE EVALUACION	OPCION DE RESPUESTA	PESO
1.1 RESPONSABLE	ASIGNADO	15
	NO ASIGNADO	0
1.2 SEGREGACION Y AUTORIDAD DEL RESPONSABLE	ADECUADO	15
	INADECUADO	0
2. PERIODICIDAD	OPORTUNA	15
	NO OPORTUNA	0
3. PROPOSITO	PREVENIR	15
	DETECTAR	10
	NO ES UN CONTROL	0
4. COMO SE REALIZA LA ACTIVIDAD DE CONTROL	CONFIABLE	15
	NO CONFIABLE	0
5. QUE PASA CON LAS OBSERVACIONES O DESVIACIONES	SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE	15
	NO SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE	0
6. EVIDENCIA DE LA EJECUCIÓN DEL CONTROL	COMPLETA	10
	INCOMPLETA	5
	NO EXISTE	0



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 16 de 17
POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

Los resultados de la evaluación del control se obtienen según la siguiente escala:

SOLIDEZ DEL CONTROL	
RANGO DE CALIFICACION	RESULTADO
FUERTE	96 - 100
MODERADO	86 - 95
DÉBIL	0 - 85

Únicamente se tendrán en cuenta los controles con solidez fuerte o moderada, si la solidez es débil deberá reevaluarse el control y reformularse hasta tanto se logre una solidez mayor.

7.4.1 Determinación del riesgo residual

Con base en la solidez del control determinada conforme al numeral anterior, se procede a establecer la zona de riesgo residual para lo cual se tendrá en cuenta el riesgo inicial ubicado en el mapa de calor y conforme a este se desplazarán las filas (en sentido inferior) y las columnas (hacia la izquierda) de acuerdo a la siguiente tabla:

RIESGO RESIDUAL				
SOLIDEZ DEL CONTROL	AYUDA A DISMINUIR LA PROBABILIDAD	AYUDA A DISMINUIR EL IMPACTO	# DE FILAS QUE SE DESPLAZA EN EL EJE PROBABILIDAD	# DE COLUMNAS QUE SE DESPLAZA EN EL EJE IMPACTO
FUERTE	DIRECTAMENTE	DIRECTAMENTE	2	2
FUERTE	DIRECTAMENTE	INDIRECTAMENTE	2	1
FUERTE	DIRECTAMENTE	NO DISMINUYE	2	0
FUERTE	NO DISMINUYE	DIRECTAMENTE	0	2
MODERADO	DIRECTAMENTE	DIRECTAMENTE	1	1
MODERADO	DIRECTAMENTE	INDIRECTAMENTE	1	0
MODERADO	DIRECTAMENTE	NO DISMINUYE	1	0
MODERADO	NO DISMINUYE	DIRECTAMENTE	0	1

7.5 MONITOREO DE LA ACTIVIDAD DE CONTROL

El responsable del monitoreo a la actividad de control será el líder de proceso o coordinador del Servicio u Oficina, quien además determinará la periodicidad teniendo en cuenta las acciones asociadas al control y deberá dejar registro del

	HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 17 de 17
	POLÍTICA DE GESTIÓN DEL RIESGO	Fecha vigencia 30/09/2020	Código POL-GER-08	

seguimiento realizado en el cual se incluirá la medición del indicador correspondiente.

8 SEGUIMIENTO Y MONITOREO

El monitoreo se realizará mediante mesas de trabajo que se desarrollarán de manera cuatrimestral durante la vigencia y estará bajo la responsabilidad de los líderes de los procesos y su equipo de trabajo, dejando como evidencia la respectiva acta. El seguimiento a los mapas de riesgos institucionales será realizado de manera semestral por el jefe de la Oficina de Control Interno dejando como evidencia el informe.