2020

HOMERIS

POLÍTICA DE ADMINSTRACIÓN DEL RIESGO

ESE HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA

INTRODUCCIÓN

La E.S.E. Hospital Mental Universitario de Risaralda, HOMERIS, define su política de administración de riesgos tomando como referente los lineamientos de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital*, emitido por la Función Pública en octubre de 2018.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

En la E.S.E. HOMERIS establecemos los lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de nuestros programas, proyectos, planes, procesos y productos, a través de:

a) La identificación y documentación de los riesgos de gestión, de corrupción y de seguridad digital en los programas, proyectos, planes y procesos.

b) El establecimiento de acciones de control detectivas y preventivas para los riesgos identificados.

c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

TÉRMINOS Y DEFINICIONES[1]

- **Análisis del riesgo:** Proceso llevado a cabo para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Causa:** Todos aquellos factores internos y externos que solos en combinación con otros, pueden producir la materialización de un riesgo.

[1] Definiciones tomadas de la ISO 31000 y de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, de la Función Pública.

- **Consecuencia:** Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Contexto externo:** Ambiente externo en el cual la organización desea lograr sus objetivos.
- **Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos.
- **Control:** Medida que modifica al riesgo.
- **Establecimiento del contexto:** Definición de los parámetros internos y externos que han de ser tenidos en cuenta para gestionar el riesgo y establecer el alcance y los criterios del riesgo.
- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis de riesgos con los criterios de los riesgos. Así se determinará si el riesgo, su magnitud, o ambos en conjunto son tolerables o aceptables.
- **Evento:** Presencia o cambio de un conjunto particular de circunstancias.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **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.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de varios. Se expresa en términos de combinación de la probabilidad y las consecuencias de los mismos.
- **Parte involucrada:** Persona u organización que puede afectar o verse afectada por una decisión o actividad.

- **Probabilidad:** Posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
- **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.
- **Riesgo inherente:** Aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **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.
- **Tratamiento del riesgo:** Proceso para modificar el riesgo.

ALCANCE

La política de riesgos es aplicable a todos los procesos, proyectos, productos de la E.S.E. HOMERIS y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones. Asimismo, la administración del riesgo contemplará:

- Los riesgos de gestión y de corrupción en todos los procesos de la E.S.E.
- Los riesgos del Sistema de Gestión de Seguridad de la Información – Seguridad Digital, en los procesos que hacen parte del alcance del Sistema de Gestión de la Seguridad de la Información.

Esta política de administración del riesgo contribuye al control interno de la entidad, y fomenta la cultura del autocontrol al interior de los procesos.

OBJETIVOS

- Establecer los parámetros necesarios para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos; valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
- Orientar la toma de decisiones.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad, para así aumentar nuestra eficacia y efectividad.
- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la alta dirección de la entidad tener una seguridad razonable en el logro de sus objetivos.

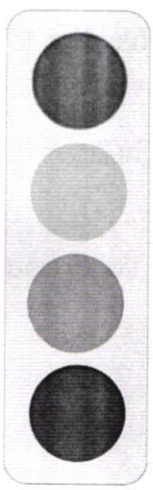
NIVELES DE LA GESTIÓN DEL RIESGO

La gestión del riesgo se realiza en estricto cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG), atendiendo las responsabilidades del mismo mediante la aplicación de las tres líneas de defensa durante las etapas de desarrollo de la gestión institucional. Los niveles de aceptación del riesgo se establecen, así:

- **Zona de riesgo BAJA:** Se ASUME el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado.
- **Zona de riesgo MODERADA:** Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Se hace seguimiento BIMESTRAL y se registra sus avances en el sistema implementado por la entidad para tal efecto.

- **Zona de riesgo ALTA:** Se debe incluir el riesgo en el Mapa de riesgo del Proceso y en el Mapa de Riesgo Institucional. Se establecen acciones de Control Preventivas que permitan MITIGAR la materialización del riesgo. Se monitorea MENSUALMENTE y se registra en el sistema de riesgos implementado por la entidad.
- **Zona de riesgo EXTREMA:** Se incluye el riesgo en el Mapa de riesgo del Proceso y en el Mapa de Riesgo Institucional. Se establece la cancelación de actividades que generan el riesgo, con el fin de EVITAR la materialización del mismo. El seguimiento será MENSUAL y su adecuado control se registra en el sistema implementado por la entidad para el efecto.

En la Figura 1 *(Ver)* se resumen los niveles de riesgo.



Nivel del riesgo	¿Qué hacemos?	¿Cada cuánto hacemos seguimiento?	¿Registro en Mapas de Riesgos?
Zona de riesgo BAJA	Asumimos el riesgo	N/A	☒
Zona de riesgo MODERADA	Reducimos la probabilidad de que ocurra el riesgo	Bimestralmente	☒
Zona de riesgo ALTA	Mitigamos la materialización del riesgo	Mensualmente	☑
Zona de riesgo EXTREMA	Evitamos la materialización del riesgo	Mensualmente	☑

Figura 1. Niveles de riesgo

Para el caso de los riesgos de **gestión y de seguridad de la información** se consideran ACEPTABLES aquellos ubicados en nivel de riesgo bajo.

En cuanto a los **riesgos de corrupción**, se establecen los siguientes niveles de aceptación:

Zona de riesgo BAJA

- Ningún riesgo de corrupción podrá ser aceptado.
- Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.

Zona de riesgo MODERADA

- Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo.
- Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.

Zona de riesgo ALTA

- Se adoptan medidas para:
    - **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
    - **TRANSFERIR O COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto del mismo.
- Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.

Zona de riesgo EXTREMA

- Se adoptan medidas para:
    - **EVITAR** las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
- Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos

En la Figura 2 *(Ver)* se resumen los niveles para los riesgos de corrupción.

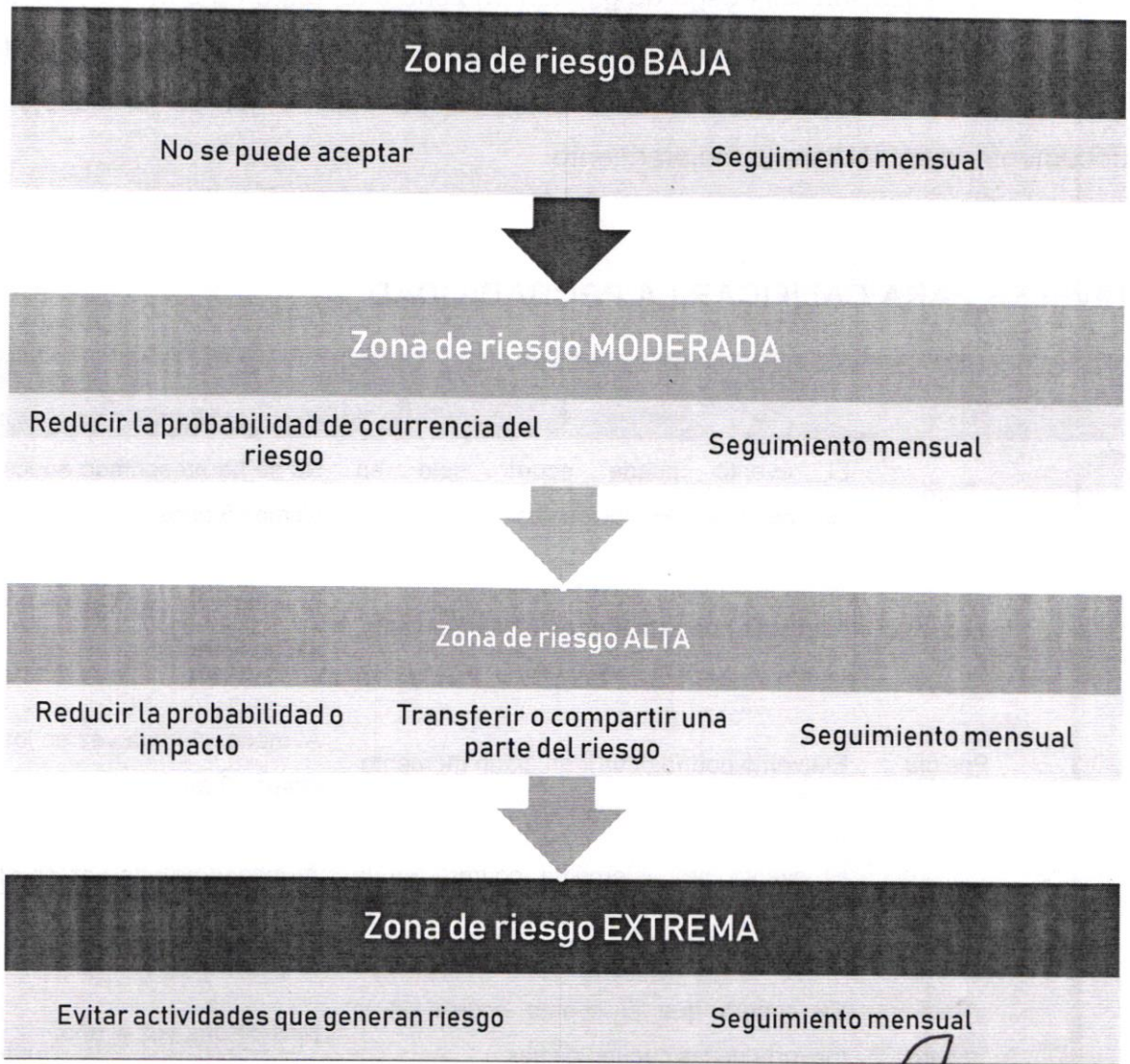


Figura 2. Niveles para los riesgos de corrupción

De igual manera la entidad establece las acciones a seguir por el líder de proceso ante la materialización del **riesgo de corrupción**, así: **1)** Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado; **2)** Realizar la denuncia ante la instancia de control correspondiente (cuando se requiera); **3)** Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento; y **4)** Actualizar el mapa de riesgos.

Ante la materialización del riesgo de gestión en zona alta, extrema o moderada, se procede de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), y documentarlo en el Plan de mejoramiento.

NIVELES PARA CALIFICAR LA PROBABILIDAD

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos de una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 1. Niveles de probabilidad

NIVELES PARA CALIFICAR EL IMPACTO

Impacto	Descriptor	Descripción Cuantitativa	Descripción Cualitativa
1	Insignificante	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5%del presupuesto general de la entidad.	- 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.
2	Menor	- Impacto que afecte la ejecución presupuestal en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1%del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - 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.

3	Moderado	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- 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.
4	Mayor	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- 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.
5	Catastrófico	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- 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.

Tabla 2. Niveles de impacto

TRATAMIENTO DE RIESGOS

Las respuestas a los riesgos pueden ser varias: las que evitan, las que reducen, las que los comparten o transfieren, y también las que aceptan *(Ver Figura 3)*:

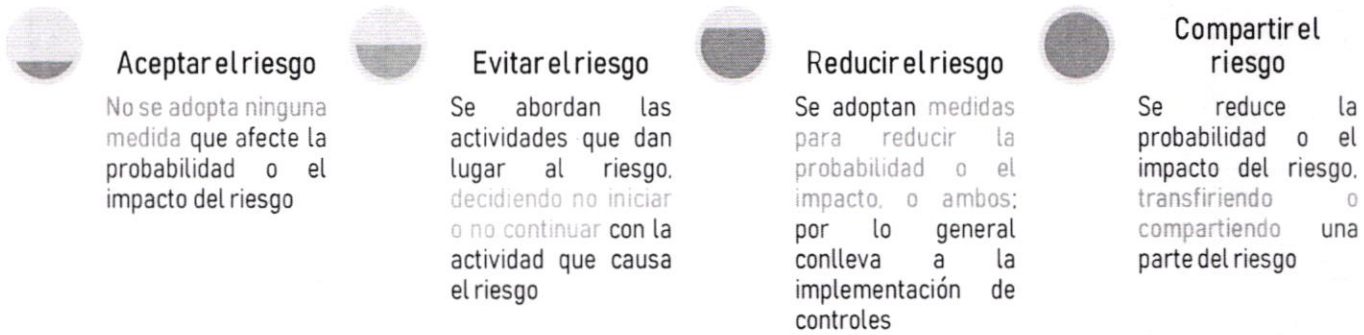


Figura 3. Tratamiento del riesgo

NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión (MIPG) en la dimensión siete (7), "Control Interno", desarrolla a través de la Línea Estratégica y las tres (3) Líneas de Defensa de responsabilidad de la gestión del riesgo y control, así:

Línea Estratégica: Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento. Está a cargo de la Gerencia, Subdirección Administrativa y Financiera, y Subdirección Científica.

1ra Línea de Defensa: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Se encuentra a cargo de los líderes de cada uno de los procesos, la Subdirección Científica, la Subdirección Administrativa y Financiera, con el apoyo de sus colaboradores, y los integrantes del equipo operativo.

2da Línea de Defensa: Asegura que los controles y los procesos de gestión de riesgos, implementados por la primera línea de defensa, estén diseñados

apropiadamente y funcionen como se pretende. El responsable del área de Planeación tiene la responsabilidad de monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, acompaña a los procesos en la administración de riesgos, y elabora su consolidación en los mapas de riesgos de Gestión, Corrupción y Seguridad Digital, así como su publicación en la página web. Para los riesgos de Seguridad de la Información - Seguridad Digital se debe tener el acompañamiento del profesional del área de sistemas.

3ra Línea de Defensa: Proporciona información sobre la efectividad del Sistema de Control Interno (S.C.I.), a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. El Asesor de Control Interno realiza el seguimiento y la medición de los avances de las acciones de respuesta y evaluación de la efectividad de las políticas.

ZACARÍAS MOSQUERA LARA
Gerente

Proyectó: Alejandra Cardona Aristizábal – Jefe de Planeación (En misión) Alejandra Cardona A.
Asesoró: Yaneth Perdomo Cataño – Asesora de Control Interno