# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HOMERIS
E.S.E. Hospital Mental
Universitario de Risaralda

**VIGENCIA AÑO 2021**

HOMERIS
E.S.E. Hospital Mental
Universitario de Risaralda

Humanizando la Salud Mental

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021


**John Jairo Ramirez Cardona**
Gerente


## EQUIPO DE TRABAJO


**Paula Andrea Vélez Cardona**
Subdirectora Administrativa y Financiera

**Jhon Jairo Naranjo Ramirez**
Profesional Universitario Sistemas

**Jhoan Sebastián Cuervo Burbano**
Profesional Universitario Sistemas

**Beatriz Elena Gomez Castaño**
Profesional Universitario Calidad y Planeación

# Contenido

# 1. Introducción

La gestión de riesgos de seguridad y privacidad de la información se refiere a los procesos que pretenden reducir las pérdidas y brindar protección a esta, al conocer las debilidades que afectan el ciclo de vida del servicio. Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio.

Este plan de tratamiento de riesgos se basa en la normatividad del Departamento Administrativo de la Función Pública (DAFP) "G*uía para la administración del riesgo*" y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) "*Guía de gestión de riesgos*".

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos de información de la E.S.E. Hospital Mental Universitario de Risaralda (HOMERIS), incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos informáticos.

Es importante destacar que este plan se articula con la Línea Estratégica de *Gestión Tecnológica* del Plan de Desarrollo Institucional de HOMERIS, vigencia 2021 – 2024. Más específicamente en el objetivo estratégico de "*Contar con recursos físicos, tecnológicos y de infraestructura que sean acordes a los requerimientos y necesidades de la ESE; y que su gestión sea orientada a la eficiencia, efectividad y seguridad.".*

# 2. Objetivos

## 2.1. Objetivo general

Desarrollar un plan de gestión de seguridad y privacidad que permita identificar y mitigar los riesgos de pérdida de activos de la información, en la E.S.E. Hospital Mental Universitario de Risaralda.

## 2.2. Objetivos específicos

- Identificar las principales amenazas que afectan los activos de la información del Hospital.
- Definir controles que permitan minimizar los riesgos a los que están expuestos los activos de información de HOMERIS.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

## 3. Alcance

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, aplica para todos los funcionarios y contratistas de la E.S.E. Hospital Mental Universitario de Risaralda.

## 4. Marco Normativo

- **Ley 87 de 1993**: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- **Decreto 943 de 2014**: Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
- **Ley 1474 de 2011**: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Decreto 2641 de 2012**: Por el cual se reglamentan el artículo 73, Plan Anticorrupción y de Atención al Ciudadano, y el artículo 76, Oficina de Quejas, Sugerencias y Reclamos de la Ley 1474 de 2011.
- **Ley 872 de 2003**: Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios.
- **Decreto 4110 de 2004**: Por el cual se reglamenta la Ley 872 de 2003 y se adopta la Norma Técnica de Calidad en la Gestión Pública.

# 5. Definiciones

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** Son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** Situación externa que no controla la entidad y que puede afectar su operación.
- **Análisis del riesgo:** Etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** Medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

- **Consecuencia:** Efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo. Está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** Acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo. Está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** Situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** Opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** Etapa de la administración del riesgo donde se

establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

- **Impacto:** Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** Ocurrencia del riesgo identificado.
- **Opciones de manejo:** Posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** Conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.
- **Probabilidad:** Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- **Riesgo:** Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es que se necesita.

## 6. Roles y Responsabilidades frente a la Administración del Riesgo

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

- *Alta Dirección:* Aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- *Proceso de Administración del Sistema Integrado de Gestión:* Genera la metodología para la administración del riesgo de la Entidad. Coordina, lidera, capacita y asesora en su aplicación.
- *Responsables de los procesos:* Identifican, analizan, evalúan y valoran los

riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos esté solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- *Servidores públicos y contratistas:* Ejecutan los controles y acciones definidas para la administración de los riesgos definidos, aportan en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

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

# 7. Política de Administración Del Riesgo

## 7.1. 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.

## 7.2. 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.

## 7.3. 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.
- **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.

[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.

- **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.

## 7.4. 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.

## 7.5. 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.

# 8. Etapas para la Administración del Riesgo

Para la administración del riesgo del riesgo se debe tener en cuenta lo siguiente:

| | |
|---|---|
| Contexto Estratégico | •Determinar los factores externos e internos del riesgo. |
| Identificación | •Determinar las causas, los riesgos, consecuencias y clasificación del riesgo. |
| Análisis | •Calificación y evaluación del riesgo inherente. |
| Valoración | •Identificación y evaluación de controles; incluye la determinación del riesgo residual. |
| Manejo | •Determinar, si es necesario, acciones para el fortalecimiento de los controles. |
| Seguimiento | •Evaluación integral de los riesgos. |

## 8.1. Análisis Contexto Estratégico

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de éstos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo.

Por lo tanto, el diseño de esta primera etapa se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar

riesgos que afecten el cumplimiento de los objetivos institucionales. Se centra en determinar las amenazas y debilidades de la entidad, siendo ésta la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS de este.

### 8.1.1 Desarrollo práctico - Contexto Estratégico

- Cada responsable de proceso del Sistema Integrado de Gestión deberá identificar a los funcionarios, que, por su competencia, pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso. Serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad.
- Se establecerán los factores internos y externos que afectan el proceso, para esto, se debe diligenciar el formato Matriz DOFA para identificación de riesgos.

Con esta información, se identificarán las posibles debilidades como:

- La administración, la estructura organizacional, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que existen para su realización.
- Las capacidades, entendidas en términos de recursos y de conocimiento (humanos, de capital, tiempo, personas, infraestructura, procesos, sistemas y tecnologías).
- Los sistemas de información y comunicación, flujos de información formales e informales y toma de decisiones.
- Las normas, directrices y modelos adoptados por la organización.

- La forma y el alcance de las relaciones contractuales.

## 8.2. Identificación de riesgos

Permite conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo las causas y los efectos de su ocurrencia. Adicionalmente, en esta etapa se realiza la clasificación del riesgo.

En este paso, se identifican los riesgos institucionales y por procesos que la organización debe gestionar. Esta identificación se realiza con base en el Contexto Estratégico.

### 8.2.1. Componentes de la identificación del riesgo

#### *8.2.1.1. Causas del riesgo*

Son las causas uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice. Esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

- *Lluvia de ideas:* Usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz.
- *Diagrama Causa-efecto:* Es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo mediante el análisis de los factores generadores del riesgo.

#### *8.2.1.2. Consecuencias*

Son los efectos que se generan o pueden generarse con la materialización del riesgo, sobre los objetivos de los procesos y de la entidad. Generalmente se dan sobre las personas o los bienes materiales o inmateriales, con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

#### *8.2.1.3. Clasificación de los riesgos*

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

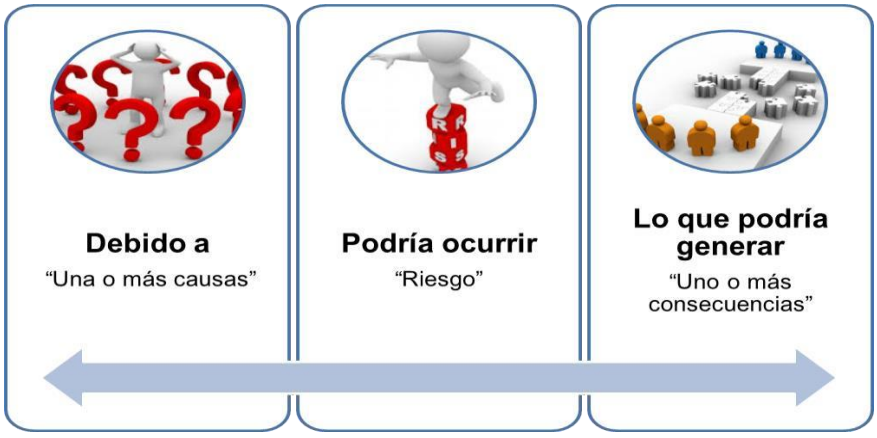
Los riesgos pueden clasificarse así:

| Clases de riesgo | Definición |
|---|---|
| Estratégico | Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia. |
| Operativo | Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias. |
| Financieros | Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes. |
| Cumplimiento | Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad. |

| | |
|---|---|
| Tecnológico | Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión. |
| Imagen | Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad. |

### 8.2.2. Estructura adecuada de la identificación del riesgo

La identificación del riesgo no se puede realizar de manera fragmentada. Debe existir una relación total entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización. Para evitar confusiones y definir articuladamente todos los componentes de la identificación del riesgo se establece un método apropiado que consiste en el uso del metalenguaje del riesgo para una identificación estructurada en tres partes:




## 8.3. Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de éste y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados: probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

### 8.3.1. Calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse; mientras que la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto, se debe tener en cuenta las siguientes tablas:

| Escala para calificar la probabilidad del riesgo | | | |
|---|---|---|---|
| **Valor** | **Nivel** | **Concepto** | **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 1 vez en los últimos 5 años. |
| 3 | Moderado | El evento podría ocurrir en algún momento. | Al menos de 1 vez en los últimos 2 años. |
| 4 | Probable | El evento probablemente ocurrirá en la mayoría de las circunstancias. | Al menos de 1 vez en el último año. |
| 5 | Casi certeza | Se espera que el evento ocurra en la mayoría de las circunstancias. | Más de 1 vez al año. |

| Valor | Tipos de efecto o impacto | Escala para calificar el impacto del riesgo | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Estratégico | Operativo | Financiero | Cumplimiento | Tecnología | Imagen |
| 1 | **Insignificante** | Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución | Afecta el cumplimiento de algunas actividades | Genera ajustes a una actividad concreta | La pérdida financiera no afecta la operación normal de la institución | Genera un requerimiento | Afecta a una persona o una actividad del proceso | Afecta a un grupo de servidores del proceso |
| 2 | **Menor** | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución | Afecta el cumplimiento de las metas del proceso | Genera ajustes en los procedimientos | La pérdida financiera afecta algunos servicios administrativos de la institución | Genera investigación es disciplinarias, y/o fiscales y/o penales | Afecta el proceso | Afecta a los servidores del proceso |
| 3 | **Moderado** | Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución | Afecta el cumplimiento de las metas de un grupo de procesos | Genera ajustes o cambios en los procesos | La pérdida financiera afecta considerablemente la prestación del servicio | Genera interrupciones en la prestación del bien o servicio | Afecta varios procesos de la institución | Afecta a todos los servidores de la institución |
| 4 | **Mayor** | Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución | Afecta el cumplimiento de las metas de la institución | Genera intermitencia en el servicio | La pérdida financiera afecta considerablemente el presupuesto de la institución | Genera sanciones | Afecta a toda la entidad | Afecta el sector |
| 5 | **Catastrófico** | Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución | Afecta el cumplimiento de las metas del sector y del gobierno | Genera paro total de la institución | Afecta al presupuesto de otras entidades o a de la del departamento | Genera cierre definitivo de la institución | Afecta al Departamento | Afecta al Departamento, Gobierno, Todos los usuarios de la institución |

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen). De acuerdo con la clase del riesgo y la magnitud del impacto, se debe determinar el nivel en el que se encuentra.

### 8.3.2. Evaluación del riesgo

Permite comparar los resultados de la calificación con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

| Probabilidad | Impacto | | | | |
|---|---|---|---|---|---|
| | Insignificante | Menor | Moderado | Mayor | Catastrófico |
| Raro | B | B | B | M | M |
| Improbable | B | M | M | A | A |
| Moderado | B | M | A | A | E |
| Probable | M | A | A | E | E |
| Casi certeza | M | A | E | E | E |

| Color | Zona de riesgo |
|---|---|
| B | Zona de riesgo baja |
| M | Zona de riesgo moderada |
| A | Zona de riesgo alta |
| E | Zona de riesgo extrema |

Con la evaluación del riesgo, previa a la formulación de controles, se obtiene la ubicación del riesgo en la matriz de evaluación. Esto se denomina **evaluación del riesgo inherente.**

### 8.3.3. Desarrollo práctico - Análisis

Formato de Análisis de riesgos, el cual hace parte del proceso de Administración del Sistema Integrado de Gestión, donde debe relacionarse la siguiente información:

- **Riesgo:** Relacionar el riesgo redactado en el formato Identificación de riesgos.
- **Calificación de probabilidad:** De acuerdo con la información cuantitativa y cualitativa.
- **Calificación de impacto:** de acuerdo con la información cuantitativa y cualitativa
- **Clasificación del riesgo:** Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- **Evaluación:** Surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto;

## 8.4. Valoración de los riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y valoración del riesgo.

### 8.4.1. Identificación de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo. Éstos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

#### *8.4.1.1. Valoración de los controles*

La evaluación de los controles existentes implica:

a) Describirlos (estableciendo si son preventivos o correctivos).
   - **Preventivos:** Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
   - **Correctivos:** Aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia.

b) Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.

c) Es importante que la valoración de los controles incluya un análisis de tipo cuantitativo, que permita saber con exactitud cuántas posiciones dentro de la Matriz de Calificación, Evaluación y Respuesta a los Riesgos es posible desplazarse, a fin de bajar el nivel de riesgo al que se está expuesto.

En las siguientes tablas se muestran la forma de ponderar, de manera objetiva, la efectividad de los controles:

| Parámetros | Criterios | Tipo de Control | | Puntajes |
|---|---|---|---|---|
| | | Probabilidad | Impacto | |
| | Posee una herramienta | | | 15 |

| | | | | |
|---|---|---|---|---|
| Herramientas para ejercer el control | para ejercer el control | | | |
| | Existen manuales, instructivos o procedimientos para el manejo de la herramienta | | | 15 |
| | El tiempo que lleva la herramienta ha demostrado ser efectiva | | | 30 |
| Seguimiento al control | Están definidos los responsables de la ejecución del control y del seguimiento | | | 15 |
| | La frecuencia de la ejecución del control y seguimiento es adecuada | | | 25 |
| **Total** | | | | 100 |

| **Rangos de Calificación de los Controles** | **Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de calificación, evaluación, evaluación y respuesta a los riesgos** | |
|---|---|---|
| | **Cuadrantes a disminuir en la Probabilidad** | **Cuadrantes a disminuir en el impacto** |
| Entre 0 – 50 | 0 | 0 |
| Entre 51 – 75 | 1 | 1 |
| Entre 76 - 100 | 2 | 2 |

### 8.4.2. Riesgo residual y definición de opciones de manejo

Previo a la definición del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

La evaluación de los controles (documentación, aplicación y efectividad) definirá la ubicación del riesgo en la matriz de evaluación; este paso se denomina "*Evaluación del riesgo residual*". Los riesgos pueden desplazarse de la siguiente manera según la calificación de los controles y la definición de la escala que afecta cada riesgo.

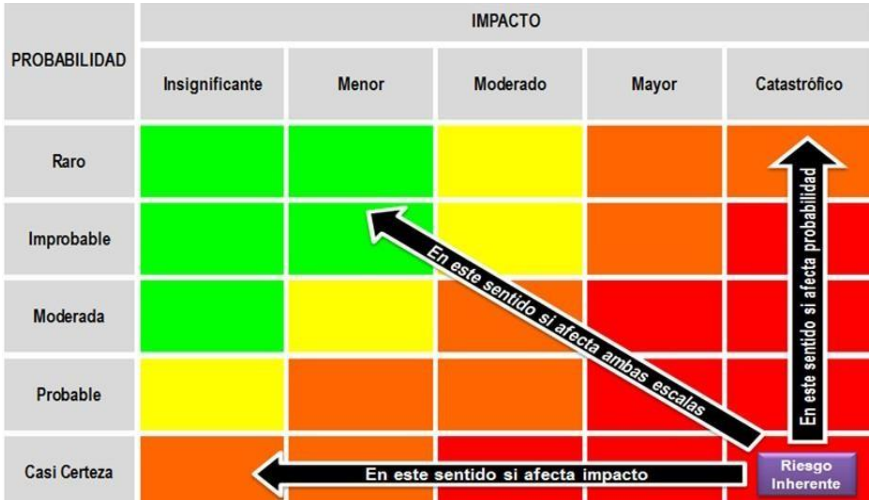



**Figura 1.** Afectación de escalas según la probabilidad y/o el impacto

Cuando se ha determinado el riesgo residual se debe asociar la opción de manejo mediante la cual se dará tratamiento al riesgo residual. Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

| Color | Zona de riesgo | Opciones de manejo |
|---|---|---|
| B | Zona de riesgo baja | Asumir el riesgo |
| M | Zona de riesgo moderada | Asumir el riesgo<br>Reducir el riesgo |
| A | Zona de riesgo alta | Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir el riesgo |
| E | Zona de riesgo extrema | Reducir el riesgo<br>Evitar el riesgo<br>Compartir o transferir el riesgo |

- **Asumir el riesgo:** Aceptar la pérdida residual probable y elaborar los planes de contingencia para su manejo.
- **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).
- **Evitar el riesgo:** Tomar las medidas encaminadas a prevenir su materialización.
- **Compartir o transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o mediante otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Ej.: seguros, sitios alternos, contratos de riesgos compartidos, etc.

### 8.4.3. Desarrollo práctico – Valoración

En el formato *Identificación y evaluación de controles*, se deben identificar y documentar los controles asociados al riesgo y calificar de acuerdo con las preguntas descritas en el formato; finalmente, se debe hacer la sumatoria de los resultados de calificación por control.

Posterior a la identificación y evaluación de los controles, se debe diligenciar el formato *Valoración del riesgo*; en este formato se debe registrar la valoración final del riesgo de acuerdo con la calificación de cada control.

## 8.5. Manejo de riesgos

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

### 8.5.1. Desarrollo práctico -Manejo-

La información correspondiente al plan de manejo se debe registrar en el formato Manejo del riesgo.

En el Anexo 1 - Matriz de Riesgos (*Ver*), se presenta el formato mencionado, con los riesgos identificados en HOMERIS.