**RESOLUCION**
**N° 344-2022**
**(30 noviembre 2022)**

*"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DEL SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS Y SUS SUBSISTEMAS EN LA ESE HOSPITAL MENTAL RUDESINDO SOTO"*

El gerente de la empresa social del estado salud Hospital Mental Rudesindo Soto, en uso de sus facultades legales y estatutarias, y,

**CONSIDERANDO**

a) Que, conforme a lo previsto en la ley 100 de 1993,numeral 6 del artículo 195 y en su decreto 1876 de 1994,en su artículo 16,las empresas sociales del estado constituyen una categoría especial de entidad pública descentralizada, con personería jurídica, patrimonio propio y autonomía administrativa, creadas por la ley o por las asambleas o consejos, según el caso, sometidas al régimen jurídico previsto en el capítulo III, título II del libro II de la ley 100 de 1993 y sus modificaciones en las leyes 1122 del 2007 y 1438 de 2011.
b) Que, la E.S.E Hospital Mental Rudesindo Soto, fue creada mediante ordenanza de creación N° 060 del 29 de Diciembre de 1995 de conformidad al artículo 195 de la ley 100 de 1993, del nivel departamental de Norte de Santander.
c) Que la Constitución Política en el artículo 209 indica que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.
d) Que el artículo 269 determina la obligación de las Entidades Públicas de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de Control Interno, de conformidad con la normatividad que regula la materia.
e) Que el decreto 1499 de 2017 en su artículo 2.2.23.1. establece que el Sistema de Control Interno previsto en la Ley 87 de 1993 y en la Ley 489 de 1998, se articulará al Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión — MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados. El Control Interno es transversal a la gestión y desempeño de las entidades y se implementa a través del Modelo Estándar de Control Interno — MECI.
f) Que el manual operativo del Sistema de Gestión MIPG establece en la Política de Control Interno como criterio para la implementación de los componentes de control, el asegurar la gestión del riesgo en la entidad estableciendo sus objetivos alineados con la planeación estratégica, dirigidos al cumplimiento de la normatividad vigente; partiendo del análisis del contexto interno, externo de la entidad y el del proceso, se identifican los riesgos para la consecución de sus objetivos en todos los niveles y los analiza como base para determinar cómo deben gestionarse, para lo cual la entidad debe contar con mecanismos efectivos de evaluación de riesgos, con el fin de establecer en nivel de riesgo inherente y residual.

Así mismo, considera la probabilidad de fraude y corrupción (Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado) que pueda afectar el logro de los objetivos, en cumplimiento al artículo 73 de la Ley 1474 de 2011, relacionado con la prevención de los riesgos de corrupción articulado con el Plan Anticorrupción y Atención al Ciudadano aprobado para la vigencia.

g) Que mediante resolución 344 del 30 noviembre 2022, se adopta el Sistema Integrado de Gestión de Riesgos y sus subsistemas de Administración de Riesgos en la ESE Hospital Mental Rudesindo Soto.
h) Que la Norma Técnica Colombiana NTC-ISO 31000 expedida por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) establece los principios y directrices genéricos para la gestión del riesgo en una organización sin importar su naturaleza, industria y sector.
i) Que la Resolución 4559 de 2018 "Por la cual se adopta el modelo de Inspección, Vigilancia y Control para la Superintendencia Nacional de Salud para el ejercicio de la supervisión de los riesgos inherentes al Sistema General de Seguridad Social en Salud", la cual en los

artículos 2, 3 y 4 insta a las entidades vigiladas a la implementación de un Sistema Integrado de gestión de riesgos.

Este Sistema Integrado de Gestión de Riesgos debe estar alineado con los planes estratégicos de la entidad. Se precisa que la Superintendencia Nacional de Salud llevará a cabo seguimiento a los Subsistemas de Administración de los Riesgos priorizados de acuerdo con la Resolución 4559 de 2018, con fines de supervisión.

Los Subsistemas de Administración de Riesgos de forma individual les permite a las entidades identificar, evaluar, medir, controlar y monitorear eficazmente como mínimo los riesgos prioritarios a los que están expuestas en desarrollo de sus operaciones, para mejorar los resultados en salud de la población, la satisfacción de los usuarios, la estabilidad financiera del sistema, fortalecer la confianza de la población en los componentes de salud del SGSSS y prevenir posibles impactos negativos.

Por otro lado, la evaluación de los riesgos de las entidades consiste en identificar y analizar la probabilidad que ocurra un evento y que impacto tiene sobre los objetivos misionales y, de esta forma adoptar estrategias preventivas.

En mérito de lo expuesto,

**RESUELVE:**

**ARTÍCULO PRIMERO. Política para la Administración de los riesgos del Sistema Integrado de Gestión de Riesgos y sus subsistemas en la ESE Hospital Mental Rudesindo Soto.** Adoptar la Política para la Administración de los riesgos del Sistema Integrado de Gestión de Riesgos y sus subsistemas en la ESE Hospital Mental Rudesindo Soto en todos sus componentes.

**ARTICULO SEGUNDO. Objetivo.** Instaurar lineamientos y criterios institucionales que permitan la correcta identificación, análisis, valoración y tratamiento de los riesgos del Sistema Integrado de Gestión de Riesgos y sus subsistemas de Administración de Riesgos en la ESE Salud; minimizando los efectos de los riesgos al interior de la Entidad y asegurar el logro de la misión y los objetivos estratégicos dentro de los procesos, procedimientos y actividades.

**ARTICULO TERCERO. Alcance.** La Política para la Administración de los riesgos del Sistema Integrado de Gestión de Riesgos y sus subsistemas es aplicable a todos los procesos, proyectos y programas de la ESE Hospital Mental Rudesindo Soto y a todas las acciones ejecutadas por los servidores públicos y contratistas durante el ejercicio de sus funciones.

**ARTICULO CUARTO. Metodología para la Administración del Riesgo.** Está fundamenta en la guía para la administración del riesgo y diseño de controles en entidades Públicas (V5 de diciembre de 2020) del Departamento Administrativo de la Función Pública y la Circular Externa 20211700000004-5 y 20211700000005-5 de 2021 de la Superintendencia Nacional de Salud.

Bajo este entendido, la metodología de administración de riesgos se lleva a cabo a través del desarrollo de las siguientes actividades:

**a. Identificación del riesgo**

- Análisis de objetivos estratégicos y de los procesos
- Identificación de los puntos de riesgo
- Identificación de áreas de impacto
- Identificación de áreas de factores de riesgo

Descripción del riesgo

- Clasificación del riesgo

**b. Valoración del riesgo**

- Análisis de riesgos
- Evaluación del riesgo

**c. Nivel de aceptación y tratamiento del riesgo**

**d. Monitoreo y revisión**

**e. Comunicación y consulta**

Para lo cual, se adopta de la Función Pública la matriz Excel Matriz de Riesgos para facilitar el proceso de identificación, valoración y tratamiento de los riesgos.

**ARTICULO QUINTO. Estructura para la gestión del riesgo.** La ESE Hospital Mental Rudesindo Soto de acuerdo a resolución 344 del 30 noviembre 2022, gestionará todos los riesgos a los que esté expuesto dentro de su operación, y su gestión dependerá de la discrecionalidad y organización de acuerdo a su rol y responsabilidades en el marco de las Líneas de Defensa.

Es de notar que los siguientes riesgos están priorizados con sus respectivos subsistemas:

Riesgo en Salud
Riesgo Operacional
Riesgo Actuarial
Riesgo de Crédito
Riesgo de Liquidez
Riesgo de mercado de capitales
Riesgo de grupo
Riesgo de Lavado de Activos y Financiación del Terrorismo- SARLAFT.

**ARTICULO SEXTO. Seguimiento.** La Oficina de Planeación en compañía de la Oficina de Control Interno realizará trimestral y cuatrimestral el seguimiento a la Política de Administración del Riesgo implementada en la Entidad de acuerdo a su nivel de responsabilidad definidos en las líneas de defensa a fin de determinar su nivel de apropiación y materialidad establecido en la ley y la jurisprudencia, de tal manera establecer la formulación de planes de mejoramiento, si hubiere lugar.

**ARTICULO SEPTIMO. Incumplimiento de la Política.** El incumplimiento de la política se clasificará en dos formas: Por acción o por omisión. De la materialización de ellas se derivarán las medidas de carácter administrativas o disciplinarias necesarias que garanticen la normalización de la situación o subsanen el evento sucedido o eliminen la causa raíz del problema identificado.

**ARTICULO OCTAVO. Vigencia y Derogatoria.** La presente Resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

**COMUNÍQUESE Y CÚMPLASE**

Dada en Cúcuta, a los treinta (30) días de noviembre 2022


**JESUS EMILIO RINCON VERA**
**GERENTE**

Elaboro: Grupo calidad – planeación
Reviso: Oficina jurídica.
Aprobó: Gerente.

# POLITICA PARA LA ADMINISTRACIÓN DEL RIESGO

## OBJETIVO

Establecer los lineamientos y criterios Institucionales que permitan la correcta identificación, análisis, valoración y tratamiento de los riesgos del Sistema Integrado de Gestión de Riesgos y sus subsistemas; minimizando los efectos de los riesgos al interior de la ESE y asegurarel logro de la misión y los objetivos institucionales dentro de los procesos, procedimientos y actividades.

## ALCANCE

La Política para la Administración de los riesgos del Sistema Integrado de Gestión de Riesgos y sus subsistemas es aplicable a todos los procesos, proyectos y programas de la ESE y a todas las acciones ejecutadas por los servidores públicos y contratistas durante el ejercicio de sus funciones.

## TERMINOS Y DEFINICIONES

- **Actitud hacia el riesgo:** Enfoque de la ESE con respecto a los riesgos, esto incluye una evaluación que implica decisiones como retener, tomar o alejarse del riesgo.
- **Activo:** En el contexto de seguridad digital son 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.
- **Análisis del riesgo:** Es el conjunto de acciones, recursos y métodos para comprender la naturaleza del riesgo. Este proceso soporta la evaluación del riesgo y las decisiones relacionadas con el tratamiento del riesgo.
- **Áreas de impacto:** Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo.
- **Consecuencia:** Es el resultado de un evento que afecta los objetivos de la ESE, esta consecuencia puede ser expresada de manera cualitativa o cuantitativamente.
- **Contexto externo:** Son las condiciones, tendencias o circunstancias externas con las cuales se busca para alcanzar el logro de los objetivos, estas condiciones son de tipo cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo de la ESE . Estas condiciones pueden ser de orden nacional o internacional.
- **Contexto interno:** Son condiciones de tipo interno con los cuales se consiguen los objetivos institucionales, son políticas, estrategias y los estructurales, éstos últimos van desde la línea de organización jerárquica, la distribución y responsabilidad funcional, la capacidad operativa, entendida como el talento humano, los recursos tecnológicos y económicos, los métodos de trabajo.
- **Control:** Es la medida que modifica el riesgo. Los controles pueden ser procesos, políticas prácticas u otras acciones dentro del sistema de administración del riesgo.
- **Establecimiento del contexto:** Es el conjunto de parámetros internos y externos que se deben tener en cuenta en la gestión del riesgo. Este contexto es el punto de partida para la evaluación yel establecimiento de políticas de gestión del riesgo.
- **Evaluación del riesgo:** Es el proceso utilizado para determinar las prioridades del sistema de administración del riesgo y la decisión de tratamiento acerca del riesgo, esto comparando el nivelde un determinado riesgo con respecto a los criterios del riesgo, determinando de esta forma, si el riesgo, la magnitud de este o ambos se pueden considerarse aceptables o tolerables.
- **Evento:** Incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Un evento puede ser una o más ocurrencias y ser atribuido a una o más causas.
- **Fuente del riesgo:** Es un elemento tangible o intangible que por sí mismo o en combinación tiene el potencial intrínseco de originar un riesgo.
- **Gestión del Riesgo:** Se refiere a la arquitectura, entendida esta como los principios y metodología para la gestión eficaz del riesgo, es decir, son un conjunto de actividades coordinadas para dirigir y controlar la ESE con respecto al riesgo.

- **Identificación del riesgo:** Es la parte de la valoración del riesgo que encuentra, reconoce y describe el riesgo. Es un mecanismo de control, que permite conocer los eventos potenciales que ponen en riesgo el logro de la misión. El alcance incluye la identificación de las fuentes del riesgo, los eventos, las causas y consecuencias.
- **Impacto:** Son las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Nivel de riesgo:** Es la magnitud de un riesgo o una combinación de riesgos. Esta magnitud seda en función de las consecuencias que se derivan del riesgo y la probabilidad de ocurrencia.
- **Política para la gestión del riesgo:** Es la declaración y lineamientos generales de la Alta Dirección con respecto a la gestión del riesgo.
- **Proceso para la gestión del riesgo:** Se entiende como la aplicación sistemática de las políticas,los procedimientos y las prácticas de gestión a las actividades de gestión del riesgo.
- **Probabilidad:** Es la oportunidad que algo suceda, esta puede ser medida con criterios de frecuencia.
- **Puntos de riesgo:** Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.
- **Riesgo:** Efecto de incertidumbre sobre los objetivos estratégicos de la ESE, debido a eventos potenciales.
- **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 que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de seguridad 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. Incluyeaspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo inherente:** Es 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 medidas de tratamiento del riesgo.
- **Tratamiento del riesgo:** Es el proceso para modificar el riesgo. Las decisiones sobre esta modificación implican evitar o tomar el riesgo, retirar la fuente del riesgo, cambiar la probabilidad de ocurrencia del riesgo, cambiar las consecuencias del riesgo, compartir o transferir el riesgo con uno o varios de los actores que tienen incidencia o se afectan con el riesgo y retener el riesgo a través de una decisión informada.
- **Valoración del riesgo:** Se define como el producto de verificar los resultados de la evaluación del riesgo con los controles identificados, estableciendo prioridades para su manejo y para la fijación de políticas. Comprende el proceso total de identificación, análisis y evaluación del riesgo.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## NIVELES DE RESPONSABILIDAD SOBRE LA GESTIÓN DEL RIESGOS

La definición de la Política de Administración del Riesgo está a cargo del Representante Legal de la Entidad; a fin de garantizar una adecuada gestión del riesgo, se requiere el compromiso de todo el personal para cumplir con cada una de las instancias que participan en la definición y ejecución de las acciones, métodos, y procedimientos de control de riesgos.

Cabe resaltar que la primera línea- los líderes de proceso, o a quienes corresponde, deben:

- Identificar y valorar los riesgos que puedan afectar el logro de los Objetivos Institucionales.
- Definir y diseñar los controles a los riesgos.
- Cumplir con los planes de acción establecidos para cada uno de los riesgos materializados,establecido en el Plan de Tratamiento de Riesgos.

A continuación, se detalla cada nivel de responsabilidad frente al riesgo desde la línea de defensa:

***Tabla 1.*** *Niveles de responsabilidad sobre la gestión del riesgo.*

| LINEA DE DEFENSA | RESPONSABLE | OBJETIVO | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|---|
| Estratégica | Representante Legal de la Entidad | Define el marco general para la gestión y control del riesgo y supervisa su cumplimiento. | Revisar los cambios en el Direccionamiento Estratégico y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados.<br>❖ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.<br>❖ Hacer seguimiento a la implementación de cada una de las Etapas de la Gestión del Riesgos y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.<br>❖ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.<br>❖ Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgoinherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo con las políticas de toleranciaestablecidas y aprobadas.<br>Revisar los informespresentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo losriesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.<br>❖ Revisar los planes de acción establecidos para cada uno delos riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.<br>❖ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgoso modificar los que ya se tienen identificados en cada uno de susprocesos, para la actualizaciónde la matriz de riesgos de su proceso. |

| LINEA DE DEFENSA | RESPONSABLE | OBJETIVO | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|---|
| Primera Línea | Gerente<br><br>Líderes de proceso | Gestionar los riesgos que puedan afectar el cumplimiento de los objetivos Institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos. | ❖ Revisión como parte de susprocedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.<br><br>❖ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.<br><br>❖ Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.<br><br>Revisar y reportar a planeación, los eventos de riesgos que sehan materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgosmaterializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadoresasociados a dichos objetivos.<br>❖ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, conel fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento alos objetivos.<br>❖ Revisar y hacer seguimiento al cumplimiento de las actividadesy planes de acción acordados con la Línea Estratégica, Segunda y Tercer Línea de Defensa con relación a la Gestión de Riesgos. |

| | | | |
|---|---|---|---|
| Segunda Línea | Asesor de Planeación yMercadeo<br><br>Supervisores e interventores decontratos o proyectos<br><br>Líderes de los Sistemas de Gestión | Asiste y guía a la Línea estratégica y a la 1ra Línea de Defensa en la Gestión adecuada de los Riesgosque pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción a través del establecimiento<br><br>de directrices y apoyo en el proceso de identificar, analizar y evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapasde la gestión de riesgos. | ❖ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgoso modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de lasmatrices de riesgos.<br><br>❖ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, quehan servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.<br><br>❖ Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.<br><br>❖ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.<br><br>❖ Hacer seguimiento a que las actividades de controlestablecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en losprocedimientos.<br><br>Revisar los planes de acción establecidos para cada uno de los riesgos materializados, conel fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva amaterializar el riesgo y lograr el cumplimiento a los objetivos. |

| LINEA DE DEFENSA | RESPONSABLE | OBJETIVO | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|---|
| Tercera Línea | Oficina de Control Interno oAuditoría Interna | Provee aseguramiento independiente y objetivo sobre la efectividad del Sistema de Gestión de Riesgos, validando que la Línea Estratégica, la 1ra Línea y 2da Línea de defensa cumplan con sus responsabilidades en laGestión de Riesgos para ellogro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. | ❖ Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgoso modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.<br><br>❖ Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, quehan servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.<br><br>Revisar que se hayan identificado los riesgossignificativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.<br><br>❖ Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones yseguimiento para elfortalecimiento de los mismos.<br><br>❖ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.<br><br>❖ Hacer seguimiento a que las actividades de controlestablecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditoríasrealizadas, se realicen demanera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o<br>❖ materialización de riesgos. |

***Fuente:*** *Manual Operativo MIPG-2019- DAFP*

Además de las líneas de defensa y las responsabilidades designadas en la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" del DAFP, es necesario indicar las responsabilidades designadas al responsable de Seguridad Digital, de acuerdo al Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas, establecido por el MinTIC.

**Tabla 2.** *Nivel de responsabilidad frente al riesgo de seguridad digital.*

| RESPONSABLE | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|
| Profesional Universitario deSistemas de la Información | ❖ Definir el procedimiento para la Identificación y Valoración de Activos.<br>❖ Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación yTratamiento).<br>❖ 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.<br>❖ Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.<br>❖ Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos deseguridad digital. |

***Fuente:*** *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.*

## ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

### 5.1.SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS

La ESE de acuerdo a la Resolución 1632 del 2021, gestionará todos los riesgos a los que esté expuesto dentro de su operación, y su gestión dependerá de la discrecionalidad y organización de acuerdo a su rol y responsabilidades en el marco de las Líneas de Defensa.

Es de notar que los siguientes riesgos están priorizados con sus respectivos subsistemas:

- Riesgo en Salud
- Riesgo Operacional
- Riesgo Actuarial
- Riesgo de Crédito
- Riesgo de Liquidez
- Riesgo Contable
- Riesgo de Lavado de Activos y Financiación del Terrorismo- SARLAFT
- Riesgo de corrupción, la opacidad y el fraude – SICOF.

## 5 METODOLOGIA PARA LA IDENTIFICACION, VALORACION Y CONTROL DE LOS RIESGOS

Está fundamenta en la guía para la administración del riesgo y diseño de controles en entidades Públicas (V5 de diciembre de 2020) del Departamento Administrativo de la Función Pública y la Circular Externa 20211700000004-5 y 20211700000005-5 de 2021 de la Superintendencia Nacional de Salud.

Bajo este entendido, la metodología de administración de riesgos se lleva a cabo a través del desarrollo de las siguientes actividades:

a. **Identificación del riesgo**
   - ❖ Análisis de objetivos estratégicos y de los procesos
   - ❖ Identificación de los puntos de riesgo
   - ❖ Identificación de áreas de impacto
   - ❖ Identificación de áreas de factores de riesgo
   - ❖ Descripción del riesgo
   - ❖ Clasificación del riesgo

b. **Valoración del riesgo**
   - Análisis de riesgos
   - Evaluación del riesgo

c. **Nivel de aceptación y tratamiento del riesgo**
d. **Monitoreo y revisión**
e. **Comunicación y consulta**

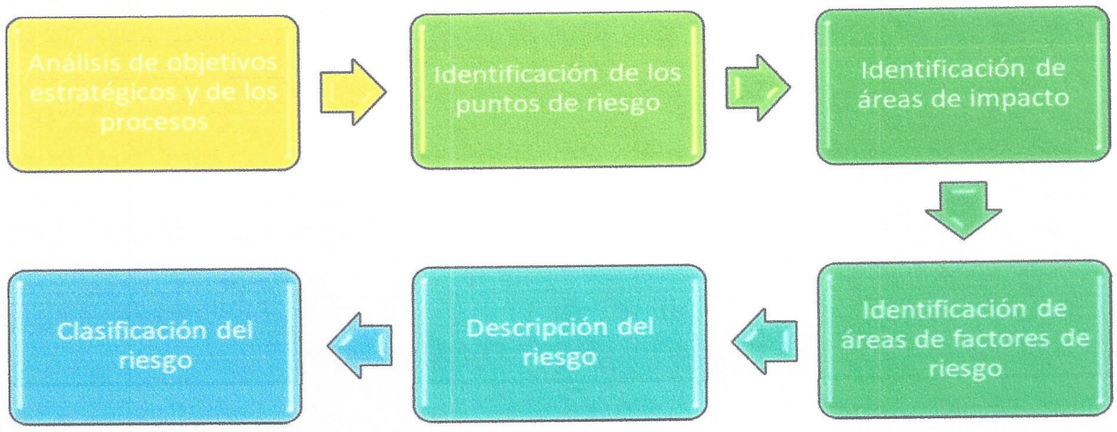
Para lo cual, se adopta de la Función Pública Matriz Excel de Riesgos para facilitar el proceso de identificación, valoración y tratamiento de los riesgos.

## 5.3. IDENTIFICACION DE RIESGOS

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la ESE, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Se aplican las siguientes fases:

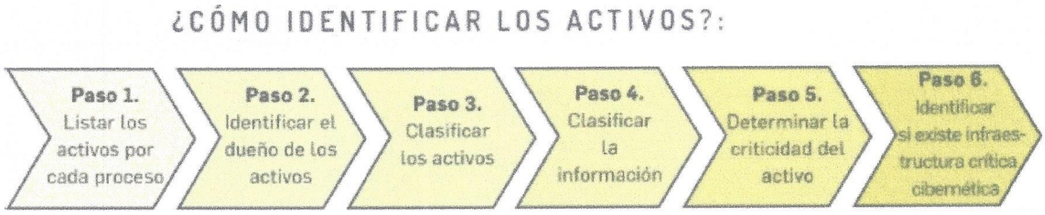
**Figura 1.** *Fases identificación de riesgos*




***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

Para los riesgos de Seguridad de la Información, como primer paso para la identificación de riesgos es necesario identificar los activos de información del proceso, a través de los siguientes pasos:

**Figura 2.** *Pasos identificación de activos de seguridad digital*




***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP-Pág. 80*

**Tabla 3.** *Identificación activos del proceso*

| Proceso | Activos | Descripción | Dueño del activo | Tipo del activo | Ley 1712/2014 | Ley 1581/2012 | Criticidad respecto a su confidencialidad | Criticidad respecto a su integridad | Criticidad respecto a su disponibilidad | Nivel de criticidad |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP-Pág. 81*

**Tabla 4.** *Tipología de Activos*

| TIPO DE ACTIVO | DESCRIPCIÓN |
|---|---|
| Información | Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| Software | Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades. |
| Hardware | Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información. |
| Servicios | Servicio brindado por parte de la entidad para el apoyo de las actividades de losprocesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software). |
| Intangibles | Aquellos activos inmateriales que otorgan a la entidad una ventaja competitivarelevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros. |

| | |
|---|---|
| Componentes de red | Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, |
| Personas | Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades. |
| Instalaciones | Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa. |

***Fuente:*** *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.*

**Figura 3.** *Criterios de evaluación de criticidad*

| CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD |
|---|---|---|
| INFORMACIÓN PUBLICA RESERVADA | ALTA (A) | ALTA (1) |
| INFORMACIÓN PUBLICA CLASIFICADA | MEDIA (M) | MEDIA (2) |
| INFORMACIÓN PÚBLICA | BAJA (B) | BAJA (3) |
| NO CLASIFICADA | NO CLASIFICADA | NO CLASIFICADA |

Tabla 1: Criterios de Clasificación

| | |
|---|---|
| ALTA | Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta. |
| MEDIA | Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio. |
| BAJA | Activos de información en los cuales la clasificación de la información en todos sus niveles es baja. |

Tabla 2: Niveles de Clasificación

| | |
|---|---|
| INFORMACION PUBLICA RESERVADA | Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. |
| INFORMACION PUBCLCA CLASIFICADA | Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma.<br><br>Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. |
| INFORMACION PÚBLICA | Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. |
| NO CLASIFICADA | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA. |

**Tabla3. Esquema de clasificación por confidencialidad**

| | |
|---|---|
| A (ALTA) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad. |
| M (MEDIA) | Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad. |
| B (BAJA) | Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos. |
| NO CLASIFICADA | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA. |

**Tabla4. Esquema de clasificación por Integridad**

| | |
|---|---|
| 1 (ALTA) | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos. |
| 2 (MEDIA) | La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad. |
| 3 (BAJA) | La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. |
| NO CLASIFICADA | Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA. |

**Tabla5. Esquema de clasificación por Disponibilidad**

***Fuente:*** *Guía para la Gestión y Clasificación de Activos de Información. MinTIC-pág.7,16-18*

Es de resaltar, que solamente se podrá identificar los siguientes tres (3) riesgos inherentes de seguridadde la información:

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

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.

A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar lostres (3) riesgos previamente mencionados:

Deliberadas (D), Fortuito (F) o Ambientales (A).

**Tabla 4.** *Tabla de amenazas comunes*

| TIPO | AMENAZA | ORIGEN |
|---|---|---|
| Daño físico | ❖ Fuego<br>❖ Agua | D, F, A |
| Eventos naturales | ❖ Fenómenos climáticos<br>❖ Fenómenos sísmicos | A |
| Perdida de los servicios esenciales | ❖ Fallas en el sistema de suministro de agua<br>❖ Fallas en el suministro de aire acondicionado | D, F, A |
| Perturbación debida a la radiación | ❖ Radiación electromagnética<br>❖ Radiación térmica | D, F, A |
| Compromiso de la información | ❖ Interceptación de servicios de señales de interferenciacomprometida<br>❖ Espionaje remoto | D |
| Fallas técnicas | ❖ Fallas del equipo<br>❖ Mal funcionamiento del equipo<br>❖ Saturación del sistema de información<br>❖ Mal funcionamiento del software<br>❖ Incumplimiento en el mantenimiento del sistema de información | D, F |
| Acciones no autorizadas | ❖ Uso no autorizado del equipo<br>❖ Copia fraudulenta del software | D, F |
| Compromiso de las funciones | ❖ Error en el uso o abuso de derechos<br>❖ Falsificación de derechos | D, F<br>D |

***Fuente:*** *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.*

**Amenazas dirigidas por el hombre:** empleados con o sin intención, proveedores y piratas informáticos,entre otros.

**Tabla 5.** *Tabla de amenazas comunes*

| FUENTE DE AMANAZA | MOTIVACIÓN | ACCIONES AMENAZANTES |
|---|---|---|
| Pirata informático, intruso ilegal | ❖ Reto<br>❖ Ego | ❖ Piratería<br>❖ Ingeniería social |
| Criminal de la computación | ❖ Destrucción de lainformación<br>❖ Divulgación ilegal de la información | ❖ Crimen porcomputador<br>❖ Acto fraudulento |
| Terrorismo | ❖ Chantaje<br>❖ Destrucción | ❖ Ataques contra el sistema DDoS<br>❖ Penetración en el sistema |
| Espionaje industrial (inteligencia, empresas,gobiernos extranjeros, otros intereses) | ❖ Ventaja competitivaEspionaje económico | ❖ Ventaja de defensa<br>❖ Hurto de información |
| Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos) | ❖ Curiosidad<br>❖ Ganancia monetaria | ❖ Chantaje<br>❖ Asalto a unempleado |

***Fuente:*** *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas. MinTIC-pág. 13,14*

**Tabla 6.** *Tabla de vulnerabilidades comunes según el tipo de activo*

| TIPO DE ACTIVO | VULNERABILIDADES |
|---|---|
| Información | ❖ Ausencia de procedimientos y/o de políticas en general (esto aplica para muchasactividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)<br>❖ Falta de controles de acceso físico |
| Software | ❖ Ausencia o insuficiencia de pruebas de software<br>❖ Ausencia de terminación de sesión<br>❖ Ausencia de registros de auditoría<br>❖ Asignación errada de los derechos de acceso<br>❖ Interfaz de usuario compleja<br>❖ Ausencia de documentación<br>❖ Fechas incorrectas<br>❖ Ausencia de mecanismos de identificación y autenticación de usuarios<br>❖ Contraseñas sin protección<br>❖ Software nuevo o inmaduro |
| Hardware | ❖ Mantenimiento insuficiente<br>❖ Ausencia de esquemas de reemplazo periódico<br>❖ Sensibilidad a la radiación electromagnética |

| TIPO DE ACTIVO | VULNERABILIDADES |
|---|---|
| | ❖ Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)<br>❖ Almacenamiento sin protección<br>❖ Falta de cuidado en la disposición final<br>❖ Copia no controlada |
| Servicios | ❖ Ausencia de procedimiento de registro/retiro de usuarios<br>❖ Ausencia de acuerdos de nivel de servicio (ANS o SLA) |
| Componentesde red | ❖ Ausencia de pruebas de envío o recepción de mensajes<br>❖ Líneas de comunicación sin protección<br>❖ Conexión deficiente de cableado<br>❖ Tráfico sensible sin protección<br>❖ Punto único de falla |
| Personas | ❖ Ausencia del personal<br>❖ Entrenamiento insuficiente<br>❖ Falta de conciencia en seguridad<br>❖ Ausencia de políticas de uso aceptable<br>❖ Trabajo no supervisado de personal externo o de limpieza |
| Instalaciones | ❖ Uso inadecuado de los controles de acceso a las instalaciones de la entidad<br>❖ Áreas susceptibles a inundación<br>❖ Red eléctrica inestable<br>❖ Ausencia de protección en puertas o ventanas<br>❖ Ausencia de proceso para supervisión de derechos de acceso<br>❖ Ausencia de control de los activos que se encuentran fuera de las instalaciones<br>❖ Ausencia de mecanismos de monitoreo para brechas en la seguridad |

***Fuente:*** *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.*
*MinTIC-pág. 21 y 22*

**NOTA:** La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad.

Una vulnerabilidad que no tiene una amenaza **puede** no requerir la implementación de un control.

### 5.3.1. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGOS

**Tabla 7.** *Identificación de áreas de factores de riesgos*

| FACTOR | DEFINICIÓN | DESCRIPCIÓN |
|---|---|---|
| Procesos | Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización. | ❖ Falta de procedimientos<br>❖ Errores de grabación, autorización<br>❖ Errores en cálculos para pagos internosy externos<br>❖ Falta de capacitación, temas relacionados con el personal. |

| | | |
|---|---|---|
| Talento Humano | Incluye seguridad y salud en eltrabajo.<br><br>Se analiza posible dolo e intenciónfrente a la corrupción. | ❖ Hurto activos<br>❖ Posibles comportamientos no éticos delos empleados<br>❖ Fraude interno (corrupción, soborno) |
| Tecnología | Eventos relacionados con la infraestructura tecnológica de la entidad. | ❖ Daño de equipos<br>❖ Caída de aplicaciones<br>❖ Caída de redes<br>❖ Errores en programas |
| Infraestructura | Eventos relacionados con la infraestructura física de la entidad. | ❖ Derrumbes<br>❖ Incendios<br>❖ Inundaciones<br>❖ Daños a activos fijos |
| Evento Externo | Situaciones externas que afectan laentidad. | ❖ Suplantación de identidad<br>❖ Asalto a la oficina<br>❖ Atentados, vandalismo, orden público |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

### 5.3.2. DESCRIPCIÓN DEL RIESGO.

Debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.

Se propone una estructura que facilita su redacción y claridad que inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos: impacto, causa inmediata y causa raíz, como se ilustra a continuación:

**Figura 4.** *Ejemplo redacción del riesgo*

Figura 11 Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo


Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

**5.3.2.1. Premisas para una adecuada redacción del riesgo**

- ❖ No describir como riesgos omisiones ni desviaciones del control.
- ❖ No describir causas como riesgos
- ❖ No describir riesgos como la negación de un control.
- ❖ No existen riesgos transversales, lo que pueden existir son causas transversales.

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

Ahora bien, para la redacción en la descripción de los riesgos de seguridad digital es necesario relacionar las causas/vulnerabilidades y consecuencias.

Para los riesgos de corrupción, se debe de responder las siguientes preguntas claves para la identificación del riesgo, tipificando su acción u omisión, uso del poder, desviar la gestión de lo público, beneficio privado.

- ❖ ¿Qué puede suceder?
- ❖ ¿Cómo puede suceder?
- ❖ ¿Cuándo puede suceder?
- ❖ ¿Qué consecuencias tendría su materialización?

### 5.3.3. CLASIFICACIÓN DEL RIESGO

**Tabla 8.** *Criterios de clasificación del riesgo*

| CLASIFICACIÓN | DESCRIPCIÓN | INTERRELACIÓN CON EL FACTOR DE RIESGO |
|---|---|---|
| Ejecución y administración deprocesos | Pérdidas derivadas de errores en la ejecución y administración de procesos. | Procesos |
| Fraude externo | Pérdida derivada de actos de fraudepor personas ajenas a la organización (no participa personal de la entidad). | Evento externo |
| Fraude interno | Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros | Talento Humano |

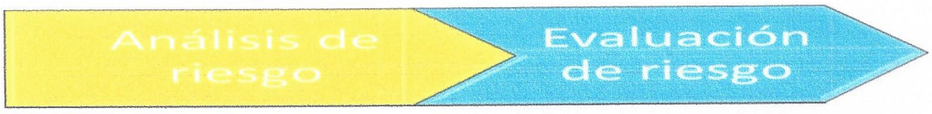
| CLASIFICACIÓN | DESCRIPCIÓN | INTERRELACIÓN CON EL FACTOR DE RIESGO |
|---|---|---|
| Fallas tecnológicas | Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos. | Tecnología |
| Relaciones laborales | Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago dedemandas por daños personales o de discriminación. | Puede asociarse a varios factores |
| Usuarios, productos y Prácticas | Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos. | Puede asociarse a varios factores |
| Daños a activos fijos/eventos externos | Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público. | ❖ Infraestructura<br>❖ Evento externo |
| Corrupción | Posibilidad de que, por acción uomisión, se use el poder para desviar la gestión de lo público hacia unbeneficio privado. | Procesos |
| Seguridad de la Información | 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. | Tecnología |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

### 5.4. VALORACIÓN DEL RIESGO

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, conel fin de estimar la zona del riesgo inicial (RIESGO INHERENTE), para ello se desarrollará dos elementos:

**Figura 5.** *Elementos de valoración de riesgos*




***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

### 5.4.1. ANÁLISIS DE RIESGO

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuenciaso impacto.

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a laexposición 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.

Por lo tanto, para calificar el riesgo se utilizará los siguientes criterios:

#### 5.4.1.1. Determinar la probabilidad.

**Tabla 9.** *Actividades relacionadas con la gestión en entidades públicas*

| ACTIVIDAD | FRECUENCIA DE LA ACTIVIDAD | PROBABILIDAD FRENTE AL RIESGO |
|---|---|---|
| Planeación estratégica | 1 vez al año | Muy baja |
| Actividades de talento humano,jurídica, administrativa | Mensual | Media |
| Contabilidad, cartera | Semanal | Alta |
| *Tecnología (incluye disponibilidad de aplicativos), tesorería.<br><br>*Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.<br><br>Ej.: Aplicativo FURAG está disponibledurante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas. | Diaria | Muy alta |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP- pág. 38*

**Figura 6.** *Criterio para definir el nivel de probabilidad*

| | Frecuencia de la Actividad | Probabilidad |
|---|---|---|
| Muy Baja | La actividad que conlleva el riesgo se ejecuta como máximos 2 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% |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP-pág.39*

**5.4.1.2. Determinar el impacto**

**Criterio para definir el nivel de impacto- Riesgos de gestión yseguridad digital**

Los criterios que definen el nivel de impacto, relacionan los impactos económicos y reputacionales como las variables principales.

**Figura 7.** *Criterio para definir el nivel de impacto*

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

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP-pág40*

**IMPORTANTE:** Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

**5.4.1.2.1. Criterio para definir el nivel de impacto- Riesgo de corrupción**

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupciónse analizarán únicamente los niveles de zona de riesgo moderado, mayor, y catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor.

Ahora bien, para establecer estos niveles de impacto se deberá aplicar las siguientes preguntas frente al riesgo identificado:

**Tabla 10.** *Criterios para calificar el impacto en riesgos de corrupción*

| No. | PREGUNTA<br>Si el riesgo de corrupción 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 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 | ¿Dar lugar a procesos penales? | | |
| 15 | ¿Generar pérdida de credibilidad del sector? | | |
| 16 | ¿Ocasionar lesiones físicas o pérdida de vidas humanas? | | |
| 17 | ¿Afectar la imagen regional? | | |
| 18 | ¿Afectar la imagen nacional? | | |
| 19 | ¿Generar daño ambiental? | | |
| ❖ Responder afirmativamente de UNA (1) A CINCO (5) preguntas(s) genera un impacto **Moderado.**<br>❖ Responder afirmativamente de SEIS (6) a ONCE (11) preguntas genera un impacto **Mayor.**<br>❖ Responder afirmativamente de DOCE (12) a DIECINUEVE (19) preguntas genera unimpacto **Catastrófico.** | | | |
| MODERADO 60% | Genera medianas consecuencias sobre la entidad | | |
| MAYOR 80% | Genera altas consecuencias para la entidad | | |
| CATASTROFICO 100% | Genera consecuencias desastrosas para la entidad | | |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP-pág72*

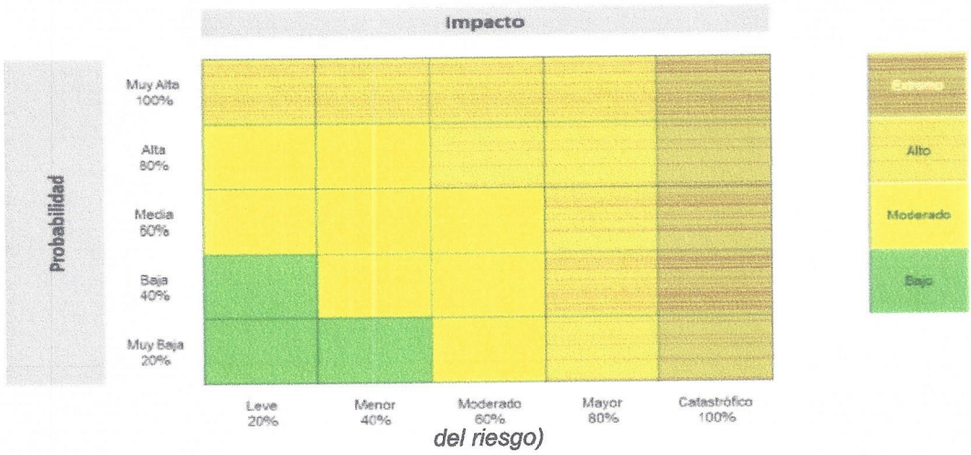
### 5.4.2. EVALUACIÓN DE RIESGO

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

#### 5.4.2.1. Análisis preliminar (riesgo inherente):

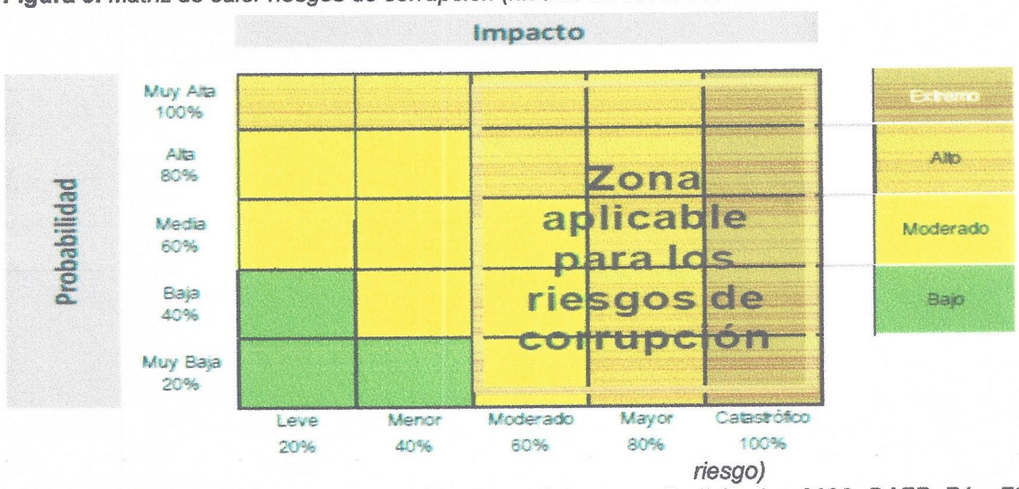
Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, de acuerdo a la Matriz de calor que se relaciona a continuación:

**Figura 8.** *Matriz de calor (niveles de severidad del riesgo)*




***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020 DAFP- Pág. 42*

**Figura 9.** *Matriz de calor riesgos de corrupción (niveles de severidad del riesgo)*




***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP- Pág. 73*

#### 5.4.2.2. Valoración de controles

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los

líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

- La metodología para valoración de los controles de riesgos de gestión, así como de seguridad dela información, es aplicable a la gestión del riesgo de corrupción.

#### *5.4.2.2.1.* Estructura para la descripción del control

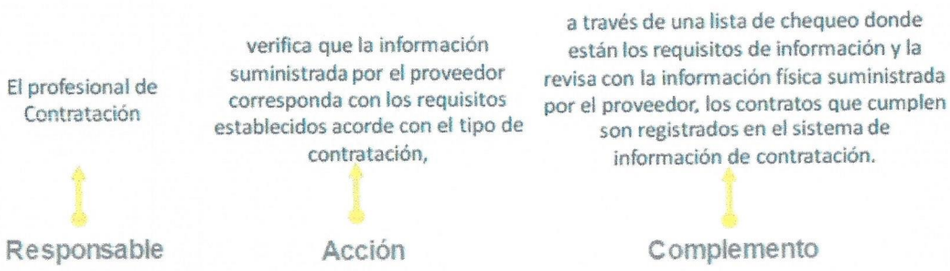
**Tabla 11.** *Componentes para la descripción de controles*

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

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

**Figura 10.** *Ejemplo redacción de control*

Figura 15 Ejemplo aplicado bajo la estructura propuesta para la redacción del control




***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP*

**5.4.2.2.2. Tipología de controles y los procesos**

**Tabla 12.** *Tipología controles*

| TIPOLOGIA | DESCRIPCION | MOVIMIENTO EN LA MATRIZ DE CALOR |
|---|---|---|
| Control preventivo | Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, sebusca establecer lascondiciones que aseguren el resultado final esperado. | Atacan probabilidad |
| Control detectivo | Control accionado durante la ejecución del proceso.<br><br>Estos controles detectan el riesgo, pero generan reprocesos. | Ataca probabilidad |
| Control correctivo | Control accionado en la salida del proceso y después de que se materializa el riesgo.<br><br>Estos controles tienen costos implícitos. | Atacan impacto |
| Control manual | Controles que son ejecutados por personas. | Ataca probabilidad |
| Control automático | Son ejecutados por unsistema. | Ataca probabilidad |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP- pág. 47*

***5.4.2.2.3.*** **Análisis y evaluación de los controles – Atributos:**

**Tabla 13.** *Criterios evaluación de los controles*

| CARACTERISTICAS | | | DESCRIPCIÓN | PESO |
|---|---|---|---|---|
| Atributos de eficiencia | Tipo | Preventivo | Va hacia las causas del riesgo, aseguran el resultado final esperado. | 25% |
| | | Detectivo | Detecta que algo ocurre y devuelve el proceso a los controles preventivos.<br><br>Se pueden generar reprocesos. | 15% |
| | | Correctivo | Control accionado en la salida del proceso y después de que sematerializa el riesgo.<br>Estos controles tienen costos implícitos | 10% |

| CARACTERISTICAS | | | DESCRIPCIÓN | PESO |
|---|---|---|---|---|
| | Implementación | Automático | Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización. | 25% |
| | | Manual | Controles que son ejecutados por una persona, tiene implícito el error humano. | 15% |
| Atributos informativos | Documentación | Documentado | Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso. | - |
| | | Sin documentar | Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso. | - |
| | Frecuencia | Continua | El control se aplica siempre que se real iza la actividad que con lleva el riesgo. | - |
| | | Aleatoria | El control se aplica aleatoriamente a la actividad que con lleva el riesgo. | - |
| | Evidencia | Con registro | El control deja un registro permite evidencia la ejecución del control. | - |
| | | Sin registro | El control no deja registro de la ejecución del control. | - |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP- Págs. 45 y46*

#### 5.4.2.2.4. NIVEL RIESGO RESIDUAL

El riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, como se ilustra a continuación:

**Figura 11.** *Aplicación de controles para establecer el riesgo residual*

| Riesgo | Datos relacionados con la probabilidad e impacto inherentes | | Datos valoración de controles | | Cálculos requeridos |
|---|---|---|---|---|---|
| Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos. | Probabilidad inherente | 60% | Valoración control 1 preventivo | 40% | 60%* 40% = 24%<br>60% - 24% = 36% |
| | Valor probabilidad para aplicar 2° control | 36% | Valoración control 2 detectivo | 30% | 36%* 30% = 10,8%<br>36% - 10,8% = 25,2% |
| | Probabilidad Residual | 25,2 % | | | |
| | Impacto Inherente | 80% | | | |
| | No se tienen controles para aplicar al impacto | N/A | N/A | N/A | N/A |
| | Impacto Residual | 80% | | | |

***Fuente:*** *Guía para la administración del riesgo vs. 5- diciembre 2020- DAFP- Págs. 49*

**IMPORTANTE:** En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

### 5.5. ESTRATEGIAS PARA COMBATIR EL RIESGO

Corresponde a la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede seraceptar, reducir o evitar.

Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de

procesos nuevos, se procede a partir del riesgo inherente.

- **La aceptación del riesgo:** puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y,por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- **Evitar el riesgo:** cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

- **Reducir el riesgo:** El nivel de riesgo debería ser administrado mediante el establecimiento de controles (mitigar), de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad o transferir parte del riesgo a través de seguros y tercerización.

Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de unacuerdo contractual.

**Tabla 14.** *Nivel de aceptación y tratamiento del riesgo*

| COLOR | ZONA DE RIESGO | TRATAMIENTO DEL RIESGO | PERIODICIDAD PARA EL SEGUIMIENTO |
|---|---|---|---|
| | **ZONA RIESGO EXTREMA** | Reducir el riesgo, evitar, compartir o transferir. | Trimestral |
| | **ZONA RIESGO ALTA** | Reducir el riesgo, evitar, compartir o transferir. | Trimestral |
| | **ZONA RIESGO MODERADA** | Asumir el riesgo, reducir el riesgo. | Semestral |
| | **ZONA RIESGO BAJA** | Asumir el riesgo. | Anual |

***Fuente:*** *Elaboración propia*

**Importante:** Los niveles de aceptación del riesgo:

- Puede ocurrir sin tratamiento de riesgo
- Los riesgos aceptados están sujetos a monitoreo
- Los riesgos de corrupción son inaceptables, siempre deben conducir a un tratamiento.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de unplan de acción que especifique:

- Responsable
- Fecha implementación
- Fecha seguimiento
- Estado

### 5.6. MONITOREO Y REVISIÓN A LA GESTIÓN DEL RIEGO

El monitoreo y revisión de la gestión de riesgos, se realizará de la siguiente manera:

- Actualización de todos los mapas por proceso, en el primer trimestre de cada año por el Sistema de Gestión de la Calidad- MIPG, teniendo en cuenta los resultados de seguimiento y la efectividad de los controles. De igual manera, cuando se presente cambios en el entorno incluidos cambios de la legislación.

**Nota:**
Los mapas de riesgo por proceso MISIONALES, su actualización se realizará en compañía de la segunda línea de defensa a cargo del líder del Sistema Obligatorio de Garantías de la Calidad en Salud- SOGCS y/o PAMEC.

La gestión del riesgo de seguridad del paciente se desarrollará según lo establecidoen el Programa de Seguridad del Paciente.

- El abordaje de los riesgos y oportunidades para el Sistema de Gestión Ambiental y el Sistema de Seguridad y Salud en el Trabajo se desarrollará bajo los lineamientos

establecidos en la Norma Técnica Colombiana NTC ISO 14001:2015 e NTC ISO 45001:2018

- Primero, segundo y tercer seguimiento, y evaluación a la gestión del riesgo en el segundo,tercer y cuarto trimestre del año por el Sistema de Gestión de la Calidad- MIPG.
- Los riesgos de corrupción se realizará seguimiento en abril, agosto y diciembre según cronograma establecido para el Plan Anticorrupción y de Atención al Ciudadano.

**Nota:** En caso de que se detecte que un riesgo se materialice, se considera que los controles no fueron efectivos y, por lo tanto, los líderes de los procesos deben reevaluar el riesgo e implementar nuevos controles.

## 2. CRITERIOS OPERACIONALES

- Para la gestión y evaluación del riesgo por proceso se utilizará la herramienta Excel controlada por el Sistema de Gestión de la Calidad en cada uno de los procesos, contemplada en el aplicativo de calidad.
- Con base en los resultados obtenidos en el seguimiento la periodicidad del seguimiento puede ser modificada.
- La Oficina Asesora de Planeación consolida el Mapa de riesgos Institucional con los riesgos contemplados Alto, Extremo y de Corrupción, lo presenta ante el Comité Coordinador de Control Interno y lo publica.
- Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente el documento del Mapa de Riesgos y si es del caso ajustarlo.
- Según el resultado de la administración del riesgo, el líder del proceso solicitará ajuste a los riesgos o controles y elaborará acciones de mejoramiento o correctivas, cada vez que sea necesario.
- Se debe asegurar la permeabilizaciónen todos los niveles de la entidad de la Política de Administración de Riesgos, de tal forma que se conozca claramente los niveles de responsabilidad y autoridad.
- Los líderes de proceso deben asegurarse de implementar la Política de Administración de Riesgos, mitigar los riesgos y reportar oportunamente a la Oficina Asesora de Planeación losavances y dificultades.
- La Oficina de Planeación difundirá la Política de Administración de Riesgos y brindará asesoría a los líderes de proceso en la aplicación de la metodología.
- Tanto la Política de Administración de Riesgos como el mapa de riesgos institucional deberá estar publicado en el sitio web de la entidad, así como, en el aplicativo de calidad.
- Los mapas de riesgos por proceso deberán publicarse en el aplicativo de calidad.
- Para evaluar la Eficacia de los controles establecidos en el mapa de riesgos institucional, se realiza seguimiento a la ejecución de dichos controles visitando los procesos de acuerdo a lo contemplado en la Tabla 14. Nivel de aceptación y tratamiento del riesgo, el cual se reportará a la oficina de control interno el seguimiento y el informe de riesgos, como evidencia se deja el mapa de riesgos institucional, actas de reunión y el informe y también esevaluado por la Auditoria Interna que realiza el proceso de Control Administrativo.
- El informe de la Evaluación a la Gestión del Riesgo, se realizará en el cuarto trimestre del año por la Oficina de Planeación con la Oficina de Control Interno, para su posterior publicación en el sitio web de la entidad.