**DEPARTAMENTO DE ANTIOQUIA**

**INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA**

**RESOLUCIÓN NÚMERO 259 DE 2021**

**( 26/07/2021 )**

"Por medio del cual se adopta la Política de Administración del Riesgo del Instituto de Cultura y Patrimonio de Antioquia y se deroga la resolución 000081 del 27 de febrero de 2019"

**LA DIRECTORA DEL INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA,**
En uso de sus facultades constitucionales articulo 209 y 269 y legales en especial los Decretos nacionales 943 de 2014 y 612 de 2018, y la conferidas en el Decreto Ordenanzal 494 de 2011, modificado por el 2120 y 2132 de 2011,

**CONSIDERANDO QUE:**

**1.** Para la aprobación de la presente política se contará con la participación y aprobación del comité institucional de coordinación de control interno y el Comité Institucional de Gestión y Desempeño de acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 Diciembre de 2020.

**2.** Mediante Resolución No. 000081 del 27 de febrero de 2019" se adopto la política de administración de riesgos en el Instituto y se derogo la resolución No. 0221 del 13 de septiembre de 2012.

**3.** El Decreto Nacional 943 de 2014, actualizó el Modelo Estándar de Control Interno para el Estado Colombiano (MECI) en el cual se determinan las generalidades y estructura necesaria para establecer, implementar y fortalecer un Sistema de Control Interno en las entidades y organismos obligados a su implementación, de acuerdo con lo dispuesto en el artículo 5° de la Ley 87 de 1993, y en su artículo 5° derogo el Decreto 1599 de 2005.

**4.** Que la misma norma señala que el Modelo se implementará a través del Manual Técnico del Modelo Estándar de Control Interno, el cual hace parte integral del Decreto, y es de obligatorio cumplimiento y aplicación para las entidades del Estado,

además, que el Departamento Administrativo de la Función Pública es la entidad encargada de realizar actualizaciones y modificaciones al Manual Técnico.

**5.** Que el Decreto 1499 de 2017; Articulo 2.2.23.2 definió la actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG en la séptima Dimensión, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5° de la Ley 87 de 199.

**6.** Que el Departamento Administrativo de la Función Pública, pone a disposición la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - Octubre de 2018, disponible en: https://www.funcionpublica.gov.co

**7.** Que el Departamento Administrativo de la Función Pública, publico la Guía de auditoría interna basada en riesgos para entidades públicas - Versión 4 - Julio de 2020, disponible en: https://www.funcionpublica.gov.co

**8.** Que el Departamento Administrativo de la Función Pública como entidad técnica, estratégica y transversal del Gobierno nacional pone a disposición de las entidades la Guía para la gestión por procesos en el marco del modelo integrado de planeación y gestión (Mipg) - Versión 1 - Julio de 2020, disponible en https://www.funcionpublica.gov.co

**9.** Que el Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, pone a disposición de las entidades la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 Diciembre de 2020. https://www.funcionpublica.gov.co

En mérito de lo expuesto,

**RESUELVE:**

**ARTÍCULO PRIMERO: ADOPCION.** Adóptese la Política de Administración del Riesgo para la administración de los riesgos de gestión, corrupción y seguridad digital; teniendo en cuenta los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 5 de Diciembre de 2020. En cuanto a los demás riesgos aplicables a la entidad se considerará lo siguiente:

- Los riesgos relacionados con la seguridad y salud en el trabajo se intervendrán de acuerdo con la matriz de identificación de peligros, la cual está de acuerdo con la metodología GTC 45 VERSION 2012, disponible en el sistema de gestión de la entidad.
- Para la gestión de los riesgos de contratación se tendrá en cuenta los lineamientos, guías y manuales expedidos por Colombia Compra Eficiente para regular la materia.
- Los riesgos de defensa jurídica serán administrados bajo la respectiva política adoptada por el Instituto de Cultura y Patrimonio de Antioquia, junto con la política de

prevención del daño antijurídico donde el Comité de Conciliación anualmente revisará y de ser necesario actualizará las mismas, que deberán ser divulgadas y su evaluación se realizará acorde con los indicadores y la periodicidad allí se defina.

- La gestión de riesgos de desastres (naturales y antrópicos) se desarrollará de acuerdo con lo estipulado en el Decreto 2157 de 2017 "por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la ley 1523 de 2012" o normas que la actualicen o sustituyan.

**ARTÍCULO SEGUNDO: OBJETIVOS**. La Política de Administración de Riesgos tendrá los siguientes objetivos:

- Contribuir a la seguridad razonable frente al cumplimiento de la misión y al logro de los objetivos institucionales, mediante la asignación de roles y responsabilidades de cada uno de los servidores y contratistas de prestación de servicios de la Entidad (Esquema de las Líneas de Defensa) y adopción de lineamientos para el tratamiento, manejo y seguimiento a los riesgos de gestión, corrupción y de seguridad digital, para la administración de riesgos de la entidad.

- Establecer los parámetros de manera sistemática para administrar los riesgos del Instituto de Cultura y Patrimonio de Antioquia, con el fin de promover el mejoramiento continuo, con el fin de establecer acciones, métodos y procedimientos de control y de gestión del riesgo, así como mecanismos para la prevención y evaluación del mismo.

**ARTÍCULO TERCERO**: **ALCANCE.** La Política de Administración de Riesgos es aplicable a todos los procesos, a los planes institucionales, a los programas, a los proyectos y a las acciones ejecutadas por los servidores públicos y contratistas de prestación de servicios del Instituto de Cultura y Patrimonio de Antioquia, durante el ejercicio de sus funciones y obligaciones, respectivamente.

Incluye lineamientos para el tratamiento, manejo y seguimiento a los riesgos de: gestión, corrupción y seguridad digital.

**ARTICULO CUARTO: TERMINOS Y DEFINICIONES:** Se detallan a continuación los términos y definiciones relacionados con la administración de riesgos y con los temas que en esta guía se desarrollen y sean relevantes para que todos los funcionarios entiendan su contenido y aplicación:

- **APETITO AL RIESGO:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **ÁREAS DE IMPACTO**: Consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional

- **CAPACIDAD DE RIESGO:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **CAUSA:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **CAUSA INMEDIATA**: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **CAUSA RAÍZ:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **CONSECUENCIA:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **CONTROL:** Medida que permite reducir o mitigar un riesgo. Los responsables de implementar y monitorear los controles son los líderes de proceso.
- **ESTRATEGIA PARA COMBATIR EL RIESGO** (tratamiento): Decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente y puede ser:

    - **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
    - **Transferir:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
    - **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo. Mo necesariamente es un control adicional.
    - **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
    - **Evitar:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

- **EVENTO:** Riesgo materializado. Los eventos de riesgo son aquellos incidentes que generan o podrían generar pérdidas a la entidad.
- **FACTORES DE RIESGO:** Son las fuentes generadoras de riesgos. Pueden ser: Procesos, Talento Humano, Tecnología, Infraestructura y Eventos externos (Terceros).
- **INDICADORES CLAVE DE RIESGO** (Un indicador de riesgos clave, también conocido como KRI de sus siglas en inglés Key Risk Indicators): Es una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos.
- **IMPACTO**: Las 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. La gestión de riesgos no es estática, se integra

en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana.

- **GESTIÓN DEL RIESGO DE DESASTRES:** Es el proceso social de planeación, ejecución, seguimiento y evaluación de políticas y acciones permanentes para el conocimiento del riesgo y promoción de una mayor conciencia del mismo, impedir o evitar que se genere, reducirlo o controlarlo cuando ya existe para prepararse y manejar las situaciones de desastre, así como para la posterior recuperación, entiéndase: rehabilitación y reconstrucción. Estas acciones tienen el propósito explícito de contribuir a la seguridad, el bienestar y la calidad de vida de las personas y al desarrollo sostenible.
- **MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo, administrado por la Subdirección de Planeación.
- **MODELO DE TRES LÍNEAS DE DEFENSA (3LD)**: Realza el entendimiento del manejo de riesgos y controles mediante la asignación o clarificación de roles y responsabilidades a través de toda la organización.

  • **Línea Estratégica** Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad.
  • **1ª Línea de Defensa**: La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. • La gestión operacional identifica, evalúa, controla y mitiga los riesgos.
  **• 2ª Línea de Defensa:** Asegura que los controles y procesos de gestión del riesgo de la 1ªLínea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. •Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
  • **3ª Línea de Defensa:** ejercida por la Oficina de Control interno.

- **NIVEL DE RIESGO:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo es Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
- **PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO**: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **POLÍTICA DE ADMINISTRACIÓN DEL RIESGO**: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos
- **POLÍTICA DE PREVENCIÓN DEL DAÑO ANTIJURÍDICO**: Solución de los problemas administrativos que generan litigiosidad e implica el uso de recursos públicos para reducir los eventos generadores del daño antijurídico.

- **PROBABILIDAD**: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **PUNTOS DE RIESGO**: Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.
- **RIESGO:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
  Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **RIESGO DE CORRUPCIÒN:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **RIESGO DE SEGURIDAD DE LA INFORMACIÒN:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **RIESGO INHERENTE:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **RIESGO RESIDUAL:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SEVERIDAD:** Nivel de un riesgo, dado por una probabilidad y un impacto. En cada nivel se define el tratamiento y los niveles de responsabilidad.
- **TOLERANCIA DEL RIESGO:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

**ARTÍCULO QUINTO**: **RESPONSABLES Y COMPROMISOS.** Son responsables frente al riesgo en el Instituto de Cultura y Patrimonio de Antioquia, los siguientes, de acuerdo con los compromisos respectivos:

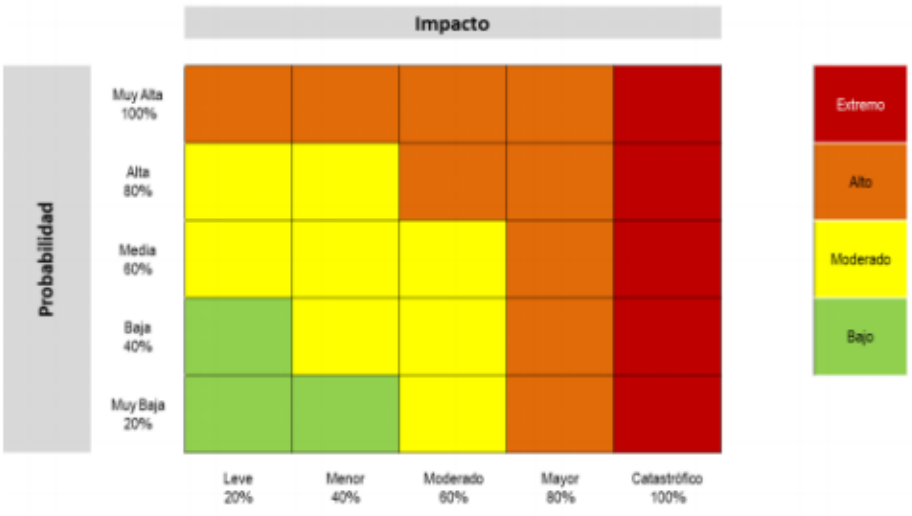
Tabla 1. Responsables y compromisos

| ROL | RESPONSABLES Y COMPROMISOS |
|---|---|
| **LÍNEA ESTRATEGICA** | **Alta Dirección:**<br>• Definirán los lineamientos para la administración del riesgo de la entidad; el equipo directivo determinará el apetito, tolerancia y capacidad de los riesgos, identificará aquellos riesgos que impidan el logro de su propósito fundamental y las metas estratégicas.<br>• Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.<br>• Aprobar el mapa de riesgos de gestión, corrupción y de seguridad digital corrupción, analiza la gestión del riesgo y aplica mejoras.<br><br>**Comité Institucional de Coordinación de Control Interno:**<br>• Aprobar el mapa de riesgos de gestión, corrupción y de seguridad digital corrupción, analiza la gestión del riesgo y recomendar mejoras. |

| | |
|---|---|
| | • A este comité debe subir el análisis de eventos y riesgos críticos<br>• Asegurará de la permeabilización en todos los niveles de la organización pública de la presente política institucional, de tal forma que cada una de las tres líneas de defensa conozcan claramente los niveles de responsabilidad y autoridad que posee frente a la gestión del riesgo.<br>• Evaluará y dará línea sobre la administración de los riesgos en la Entidad.<br>• Evaluará el estado del Sistema de Control Interno y aprobará las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.<br>• Realizará seguimiento a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por la Oficina de Control Interno.<br>• Analizará eventos y riesgos críticos.<br><br>**Comité Institucional de Gestión y Desempeño:**<br>• Aprobará el Mapa de Aprobar el mapa de riesgos de gestión, corrupción y de seguridad digital corrupción, analiza la gestión del riesgo y aplica mejoras.<br>• Atención al Ciudadano y las actualizaciones del mismo.<br>• Analizará gestión del riesgo y aplica mejoras. |
| **LINEA DE DEFENSA 1.** | **Lideres de los procesos, programas y proyectos de la entidad y equipos de trabajo:**<br>• Identificarán y valorarán los riesgos, que pueden afectar los procesos a su cargo y los actualizarán cuando se requiera, bajo la metodología vigente, informando de la novedad a la subdirección de Planeación.<br>• Definirán, diseñarán, aplicarán y realizarán seguimiento a los controles para mitigar los riesgos y propondrán mejoras a la gestión del riesgo en su proceso.<br>• Supervisarán la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectando las deficiencias de los controles y determinando las acciones de mejora a que haya lugar<br>• Reportar a la subdirección de planeación los eventos (riesgos materializados) que podrían generar perdidas a la entidad y el tratamiento correspondiente.<br>• Monitoreo y evaluación permanente a la gestión de riesgos de acuerdo con el nivel de aceptación del riesgo. |
| **LINEA DE DEFENSA 2.** | **Subdirección de Planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos de contratación.**<br>• Asiste y guía la línea estratégica y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.<br>• Difundirá la presente metodología y acompañará, orientará y entrenará a los líderes de procesos en la identificación, análisis y valoración del riesgo.<br>• Consolidará el Mapa de riesgos de Corrupción y lo presentará para revisión y aprobación del Comité Institucional de Gestión y Desempeño. Una vez sea aprobado, lo publicará en la página web de la entidad, como |

| | |
|---|---|
| | anexo al Plan Anticorrupción y de Atención al Ciudadano, a más tardar el 31 de enero de cada vigencia.<br>• Consolidará el Mapa de riesgos institucional y lo presentará para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno. |
| **LINEA DE DEFENSA 3.** | **Oficina de control interno:**<br>• Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.<br>• Revisará la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.<br>• Recomienda mejoras a la política de administración del riesgo.<br>• Alertará a la línea estratégica sobre la probabilidad de riesgo de corrupción en las áreas auditadas.<br>• Asesorará de forma coordinada con la subdirección de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. |

**ARTÍCULO SEXTO**: **NIVEL DE ACEPTACIÓN DEL RIESGO.** Los niveles de aceptación de los riesgos de gestión y seguridad digital variarán según la celda en la que se ubica el riesgo residual en la matriz de calor (niveles de severidad):




La matriz cuenta con 5 filas y 5 columnas, siendo las columnas las alternativas de impacto y las filas las opciones de probabilidad. Los niveles aceptables de riesgos serán los siguientes:

"Por medio del cual se adopta la Política de Administración del Riesgo del Instituto de Cultura y Patrimonio de Antioquia y se deroga la resolución 000081 del 27 de febrero de 2019"

| | Descripción |
|---|---|
| Extremo | Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, la Alta Dirección debe establecer el tratamiento e informar al Comité Institucional de Coordinación de Control Interno. |
| Alto | Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe establecer el tratamiento e informar al Comité Institucional de Gestión y Desempeño. |
| Moderado | Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe hacer seguimiento mediante procedimientos existentes. |
| Bajo | Los riesgos que se ubiquen en esta zona serán aceptados, el líder del proceso debe hacer seguimiento y llevar el registro correspondiente. |

En la siguiente tabla se encuentran las acciones a emprender ante los riesgos materializados:

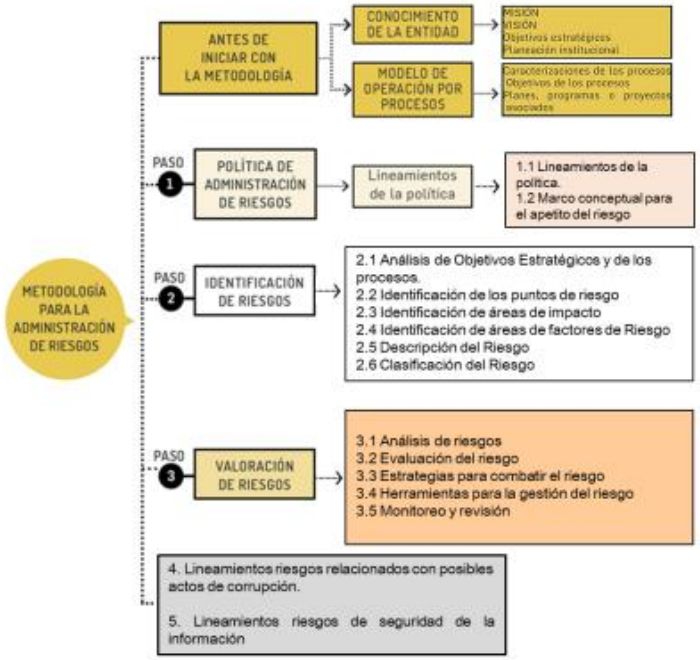
| Responsable | Acción |
|---|---|
| **Líder de Proceso** | Informar a la Subdirección de Planeación sobre el hecho encontrado y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado) realizar la denuncia ante la instancia de control correspondiente. Identificar las acciones correctivas necesarias y documentarlas en el Plan de Mejoramiento, efectuando análisis de causas y determinando acciones preventivas y de mejora. Coordinar con la Subdirección de Planeación la actualización de lo pertinente en los mapas de riesgos de corrupción, del proceso e institucional. |
| **Oficina de Control Interno** | Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado) realizará la denuncia ante la instancia de control correspondiente. Informar a la Dirección y a la Subdirección de Planeación con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar lo pertinente en los mapas de riesgos de corrupción, del proceso e institucional. |
| **Comité de Coordinación de Control Interno** | Analizará las causas de los eventos (riesgos materializados) y definirá cursos de acción. |

En el caso de los riesgos de corrupción, estos no pueden ser aceptados, en cumplimiento de la consigna tolerancia cero a los hechos de corrupción. De igual manera, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor.

**ARTÍCULO SEPTIMO**: **METODOLOGÍA PARA LA GESTIÓN DEL RIESGO**. Atendiendo la metodología propia de Función de la Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 5 de Diciembre de 2020, se requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su

efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos.

Figura 1. Metodología para la administración del riesgo




Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**Paso 1: POLITICA ADMINISTRACIÓN DEL RIESGOS**:

1. **Se tiene en cuenta los lineamientos de la Política:** (¿Qué es?, ¿quién la establece?, ¿qué se debe tener en cuenta?, que debe contener, objetivo, alcance, términos y definiciones, estructura para la gestión del riesgo, nivel de responsabilidad frente al manejo de los riesgos, nivel de aceptación del riesgo, nivel de calificación del impacto y tratamiento de riesgos).

- **¿Qué es la política de administración de riesgos?:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

- **¿Quién establece la política de administración de riesgos?:** La alta dirección con la participación del Comité Institucional de Coordinación de Control Interno.

- **¿Qué se debe tener en cuenta en la política de administración de riesgos?**: Objetivo estratégico de la entidad, niveles de responsabilidad frente al manejo de los riesgos y mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad.

- **¿Qué debe contener la política de administración de riesgos?:**

1. **Objetivo:** Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
2. **Alcance:** La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información. (ver caja de herramientas)
3. **Niveles de aceptación del riesgo:** Decisión informada de tomar un riesgo en particular NTC GTC 137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
4. **Niveles para calificar el impacto:** Riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos.
5. **Tratamiento de riesgos:** Proceso para modificar el riesgo (NTC GTC 137, Numeral 3.8.1). Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.

**1.1. Marco conceptual para el apetito del riesgo:** Dentro de los lineamientos para la política de administración de riesgo se debe considerar el apetito del riesgo**,** a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis la entidad, iniciando con las siguientes definiciones:

- **Nivel de riesgo**: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Gráficamente los anteriores conceptos se relacionan así:

Figura 2. Definiciones de apetito, tolerancia y capacidad de riesgo


Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

**Determinación de la capacidad de riesgo**

Se debe aplicar los valores de probabilidad e impacto contenidos en esta Guía y con base en esto debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina "capacidad de riesgo".

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

**Determinación del apetito de riesgo**

Luego de determinada la capacidad de riesgo por parte de la alta dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.

Este valor se denomina "apetito de riesgo", dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones

de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

**Tolerancia de riesgo**

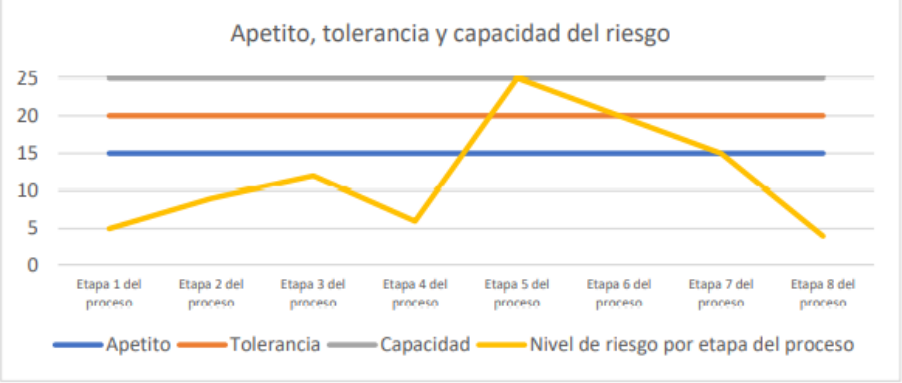
La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

El apetito, tolerancia y capacidad del riesgo será la misma para los riesgos de gestión, corrupción y seguridad digital y se calculó de la siguiente forma:

Figura 3. Apetito, tolerancia y capacidad de riesgo




- El apetito del riesgo corresponde a 15, valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.
- La tolerancia es 20, valor que es superior al apetito de riesgo y menor a la capacidad de riesgo.
- La capacidad del riesgo es 25, teniendo en cuenta qué es el valor máximo al combinar la escala de probabilidad e impacto.

La identificación de riesgos tiene como objetivo establecer cuáles son los riesgos asociados a la operación de la entidad, lo que permitirá determinar cuáles están identificados, controlados y cuáles no. Para ello se debe tener en cuenta el contexto

estratégico en el que opera la Entidad, objetivos estratégicos y de procesos, puntos de riesgo operativo, áreas de impacto y factores de riesgo.
Durante el análisis de los riesgos se establecerá la probabilidad de ocurrencia y sus consecuencias o impacto. Partirá del análisis preliminar (riesgo inherente) y tendrá en cuenta la valoración de los controles, para establecer el movimiento en la matriz de calor y determinar el nivel de riesgo residual; elementos considerados para definir el plan de acción (opción de tratamiento) acorde con las estrategias para combatir el riesgo.

El paso a paso para la identificación y valoración de los riesgos variará teniendo en cuenta las particularidades de los riesgos de gestión, corrupción y seguridad digital.

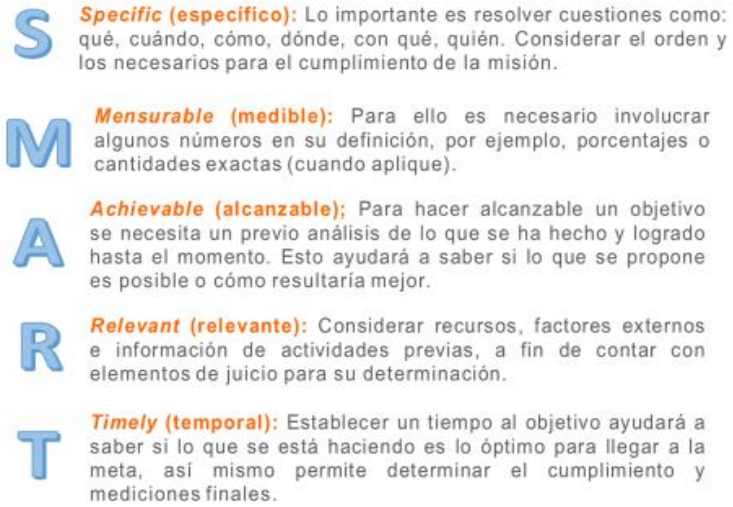
**Pasó 2: IDENTIFICACIÓN DE RIESGOS**:

- Identificar los riesgos que estén o no bajo el control de la organización, 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:

**2.1 Análisis de objetivos estratégicos y de los procesos:** Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y las líneas estratégicas institucionales, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características SMART1, cuya estructura se explica a continuación:

Figura 4. Desglose características SMART

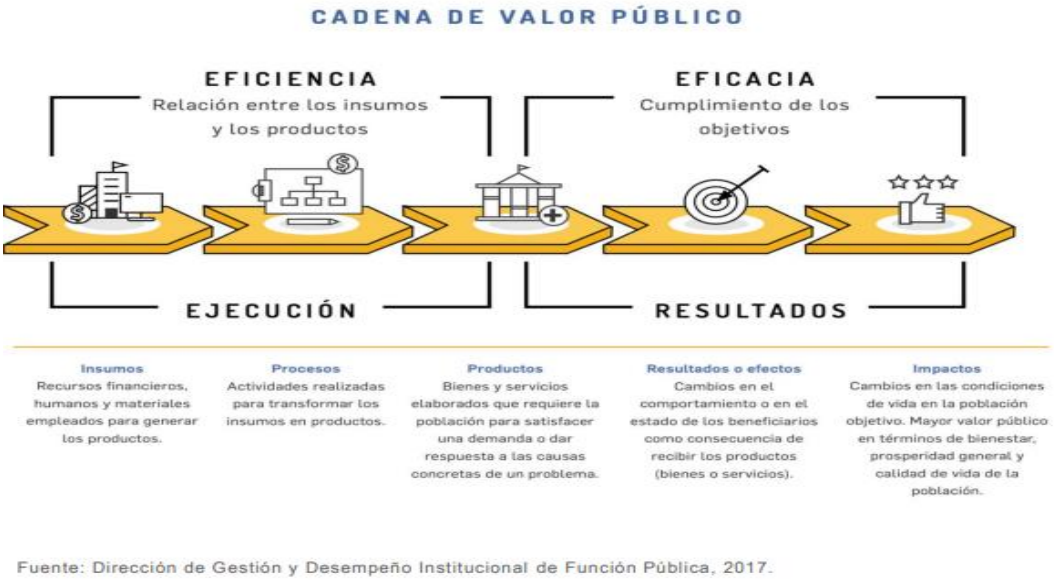



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**2.2 Identificación de los 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.

Figura 5. Cadena de valor




Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017.

**2.3 Identificación de áreas de impacto:** El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

**2.4 Identificación de áreas de factores de riesgo**: Son las fuentes generadoras de riesgos.

En la Tabla 2 encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

"Por medio del cual se adopta la Política de Administración del Riesgo del Instituto de Cultura y Patrimonio de Antioquia y se deroga la resolución 000081 del 27 de febrero de 2019"

Tabla 2. Factores de riesgo

| Factor | Definición | | Descripción |
|---|---|---|---|
| Procesos | Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización. |  | Falta de procedimientos |
| | |  | Errores de grabación, autorización |
| | |  | Errores en cálculos para pagos internos y externos |
| | |  | Falta de capacitación, temas relacionados con el personal |
| Talento humano | Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción. |  | Hurto activos |
| | |  | Posibles comportamientos no éticos de los empleados |
| | |  | Fraude interno (corrupción, soborno) |
| Tecnología | Eventos relacionados con la infraestructura tecnológica de la entidad. |  | Daño de equipos |
| | |  | Caída de aplicaciones |
| | |  | Caída de redes |
| | |  | Errores en programas |
| Infraestructura | Eventos relacionados con la infraestructura física de la entidad. |  | Derrumbes |
| | |  | Incendios |
| | |  | Inundaciones |
| | |  | Daños a activos fijos |
| Evento externo | Situaciones externas que afectan la entidad. |  | Suplantación de identidad |
| | |  | Asalto a la oficina |
| | |  | Atentados, vandalismo, orden público |

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

**NOTA:** Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.

**2.5 Descripción del riesgo:** La 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:

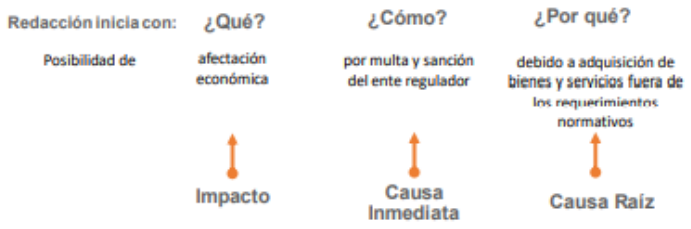
Figura 6. Estructura propuesta para la redacción del riesgo


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

Desglosando la estructura propuesta tenemos:

- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, so n la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede n existir más de una causa o subcausas que pueden ser analizadas.

Figura 7. 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.

**2.6 Clasificación del riesgo:** Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 3. Clasificación de riesgos

| | |
|---|---|
| **Ejecución y administración de procesos** | Pérdidas derivadas de errores en la ejecución y administración de procesos. |
| **Fraude externo** | Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad). |
| **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. |
| **Fallas tecnológicas** | Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos. |
| **Relaciones laborales** | Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación. |
| **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. |
| **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. |

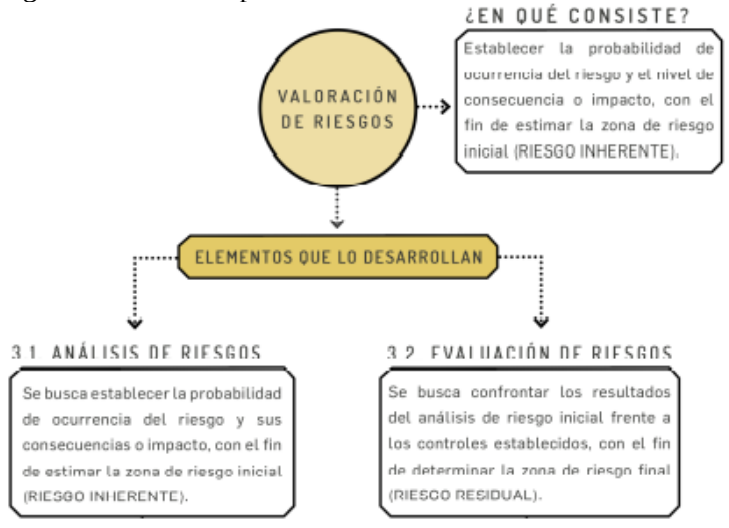
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública. 2020.

Figura 8. Relación ente factores de riesgo y clasificación del riesgo


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

**Paso 3: VALORACIÓN DE RIESGOS:** Se tiene en cuenta:

Figura 9. Estructura para el desarrollo de la valoración del riesgo




Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

**3.1 Análisis de riesgos:** En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

**3.1.1 Determinar la probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubica dos en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla 4 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>*Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.<br>Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas. | Diaria | Muy alta |

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

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla 5 se establecen los criterios para definir el nivel de probabilidad.

Tabla 5 Criterios 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Nota: Dependiendo del tamaño y complejidad de los procesos de la entidad, la tabla 5 podrá ser ajustada o adaptada a las necesidades de cada entidad.

**3.1.2 Determinar el impacto:** Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado. Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis. En la tabla 5 se establecen los criterios para definir el nivel de impacto.

Tabla 5 Criterios 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**Nota:** Dependiendo del tamaño y complejidad de los procesos en la entidad, la tabla 5 podrá ser ajustada o adaptada a sus necesidades.

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.

Ejemplo (continuación):

- **Proceso:** Gestión de recursos
- **Objetivo:** Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
- **Riesgo identificado:** Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
- **N. º de veces que se ejecuta la actividad:** La actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.
- **Cálculo afectación económica:** De llegar a materializarse, tendría una afectación económica de 500 SMLMV. Aplicando las tablas de probabilidad e impacto tenemos:

| | 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% |

La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es **media**.

| | 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 |

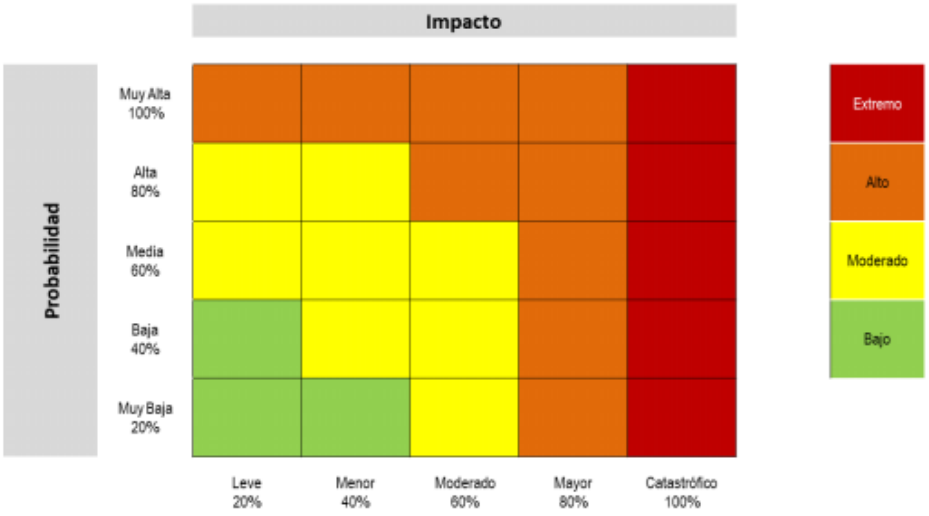
La afectación económica se calcula en 500SMLMV, el impacto del riesgo es **mayor**.

**Probabilidad inherente=** media 60%, **Impacto inherente:** mayor 80%

**3.2 Evaluación de riesgos:** A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

**3.2.1 Análisis preliminar (riesgo inherente):** Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver tabla 6).

Tabla 6. Matriz de calor (niveles de severidad del riesgo)

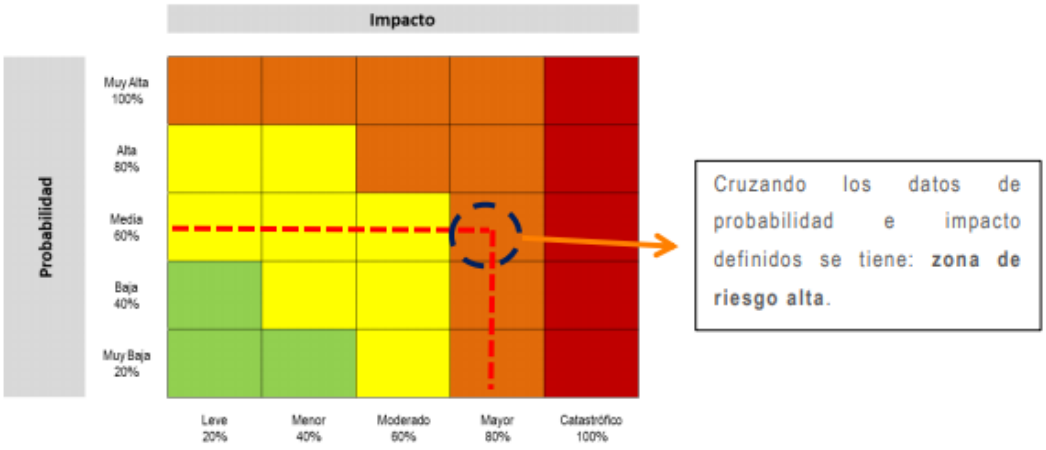



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Ejemplo (continuación):

- **Proceso:** Gestión de recursos
- **Objetivo:** Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.
- **Riesgo identificado:** Posibilidad de afectación 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:** moderada 60%
- **Impacto Inherente:** mayor 80%

Aplicando la matriz de calor tenemos:




**3.2.2 Valoración de controles:** En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. 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.

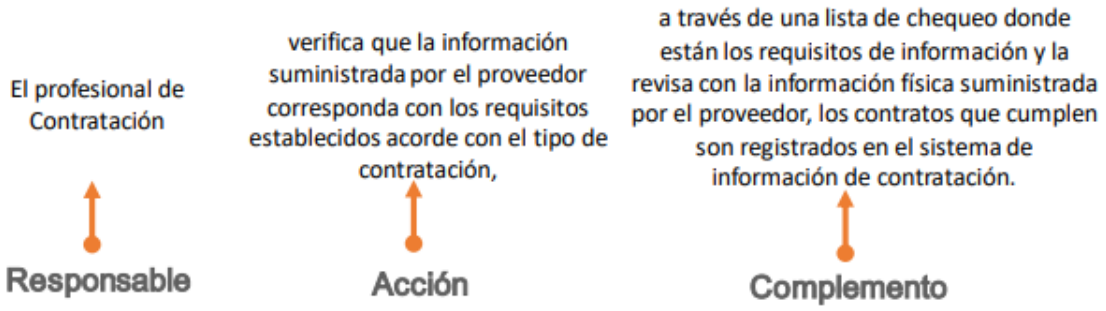
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

**3.2.2.1 Estructura para la descripción del control**: Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **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.

En la figura 10 se establece un ejemplo bajo esta estructura.

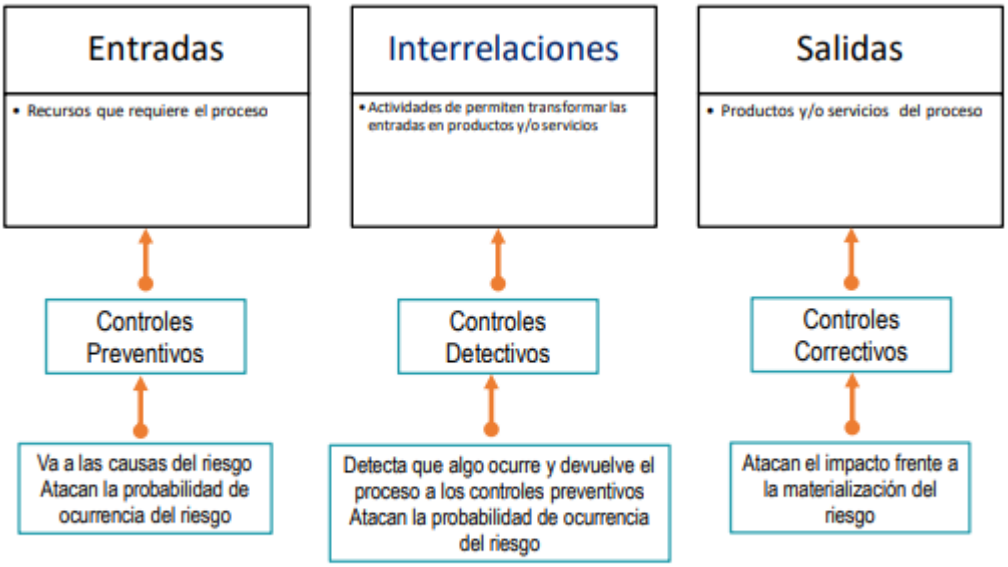
Figura 10. Ejemplo aplicado bajo la estructura propuesta para la redacción del control




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

**3.2.2.2 Tipología de controles y los procesos**: A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 11 se consideran 3 fases globales del ciclo de un proceso así:

Figura 11. Ciclo del proceso y las tipologías de controles




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

**Tipologías de controles:**

- **Control preventivo**: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** Controles que son ejecutados por personas.

- **Control automático:** Son ejecutados por un sistema.

**3.2.2.3 Análisis y evaluación de los controles – Atributos:** A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 se puede observar la descripción y peso asociados a cada uno así:

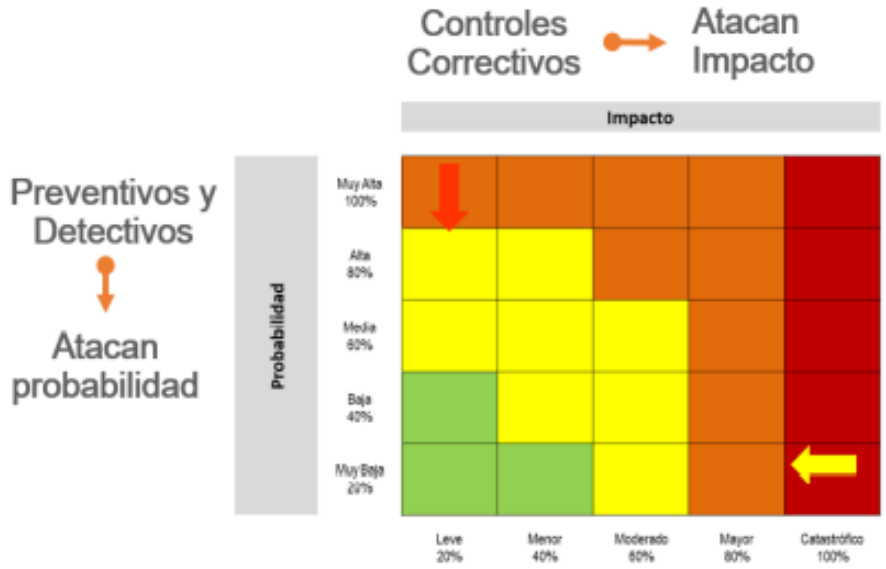
Tabla 7. Atributos de para el diseño del control

| Características | | | 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. Se pueden generar reprocesos. | 15% |
| | | Correctivo | Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación. | 10% |
| | Implementación | Automático | Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la | 25% |

| Características | | | Descripción | Peso |
|---|---|---|---|---|
| | | | intervención de personas para su realización. | |
| | | 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 realiza la actividad que conlleva el riesgo. | - |
| | | Aleatoria | El control se aplica aleatoriamente a la actividad que conlleva 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Tabla 8. Movimiento en la matriz de calor acorde con el tipo de control




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

Ejemplo (continuación):

- **Proceso:** gestión de recursos
- **Objetivo:** adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
- **Riesgo identificado:** posibilidad de afectación 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**: moderada 60%
- **Impacto Inherente:** mayor 80%
- **Zona de riesgo:** alta
- **Controles identificados**:

**Control 1**: El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

**Control 2**: El jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

En la tabla 9 se observa la aplicación de la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos.

Tabla 9. Aplicación tabla atributos a ejemplo propuesto

| Controles y sus características | | | | Peso |
|---|---|---|---|---|
| **Control 1** El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación. | Tipo | Preventivo | X | 25% |
| | | Detectivo | | |
| | | Correctivo | | |
| | Implementación | Automático | | |
| | | Manual | X | 15% |
| | Documentación | Documentado | X | - |
| | | Sin documentar | | - |
| | Frecuencia | Continua | X | - |
| | | Aleatoria | | - |
| | Evidencia | Con registro | X | - |
| | | Sin registro | | - |
| **Total valoración control 1** | | | | **40%** |
| **Control 2** El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar | Tipo | Preventivo | | |
| | | Detectivo | X | 15% |
| | | Correctivo | | |
| | Implementación | Automático | | |
| | | Manual | X | 15% |
| | Documentación | Documentado | X | - |
| | | Sin documentar | | - |
| | Frecuencia | Continua | X | |
| | | Aleatoria | | - |
| inconsistencias, devuelve el proceso al profesional de contratos asignado. | Evidencia | Con registro | X | - |
| | | Sin registro | | - |
| **Total valoración control 2** | | | | **30%** |

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

**3.2.3 Nivel de riesgo (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.

Para mayor claridad, en la tabla 10 se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Tabla 10. 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%** | | | |

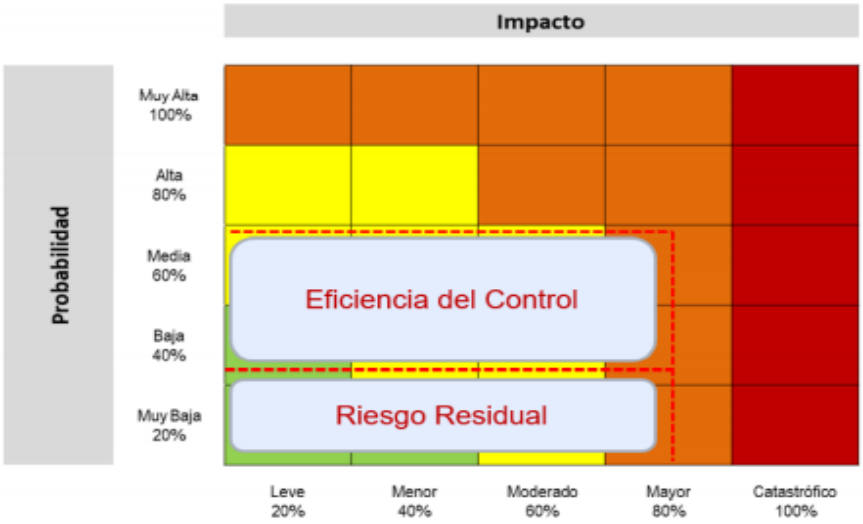
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Ejemplo (continuación):

- **Proceso:** gestión de recursos
- **Objetivo:** adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
- **Riesgo identificado:** 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 residual:** baja 26.8%
- **Impacto Residual**: mayor 80%
- **Zona de riesgo residual:** alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo. En la tabla 11 se observa el movimiento en la matriz de calor.

Tabla 11. Movimiento en la matriz de calor con el ejemplo propuesto




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

Nota: 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.

A continuación, se podrá observar el formato propuesto para el mapa de riesgos, este incluye la matriz de calor correspondiente.

**Parte 1 identificación del riesgo:**

Tabla 12. Ejemplo mapa de riesgos acorde con el ejemplo propuesto

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Proceso:** | Gestión de recursos | | | | | | | | | | |
| **Objetivo:** | Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación | | | | | | | | | | |
| **Alcance:** | Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas | | | | | | | | | | |
| **Referencia** | **Impacto** | **Causa inmediata** | **Causa raíz** | **Descripción del riesgo** | **Clasificación riesgo** | **Frecuencia** | **Probabilidad inherente** | **%** | **Impacto inherente** | **%** | **Zona de riesgo inherente** |
| 1 | Afectación económica | Multa y sanción del organismo de control | Incumplimiento de los requisitos para contratación | Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos. | Ejecución y administración de procesos | 120 | Moderada | 60% | Mayor | 80% | Alta |

"Por medio del cual se adopta la Política de Administración del Riesgo del Instituto de Cultura y Patrimonio de Antioquia y se deroga la resolución 000081 del 27 de febrero de 2019"

**Parte 2 Valoración del riesgo:**

| No. control | Descripción del control | Afectación | | Atributos | | | | | | Probabilidad residual (2 controles) | Probabilidad residual final | % | Impacto residual final | % | Zona de riesgo final | Tratamiento |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Probabilidad | Impacto | Tipo | Implementación | Calificación | Documentación | Frecuencia | Evidencia | | | | | | | |
| 1 | El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación. | X | | Preventivo | Manual | 40% | Documentado | Continua | Registro material | 36% | Baja | 25,2% | Mayor | 80% | Alta | Reducir |

| No. control | Descripción del control | Afectación | | Atributos | | | | | | Probabilidad residual (2 controles) | Probabilidad residual final | % | Impacto residual final | % | Zona de riesgo final | Tratamiento |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Probabilidad | Impacto | Tipo | Implementación | Calificación | Documentación | Frecuencia | Evidencia | | | | | | | |
| 2 | El jefe de del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado. | X | | Detectivo | Manual | 30% | Documentado | Continua | Con registro | 25,2% | | | | | | |

**Parte 3 Planes de acción (para la opción de tratamiento reducir):**

| Plan de acción | Responsable | Fecha de implementación | Fecha de seguimiento | Seguimiento | Estado |
|---|---|---|---|---|---|
| Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso. | Oficina de TIC | 30/11/2021 | 30/06/2021 | Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo. | En curso |

**3.3 Estrategias para combatir el riesgo:** Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, 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.

En la figura 12 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Figura 12. Estrategias para combatir el riesgo


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

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

**3.4 Herramientas para la gestión del riesgo:** Como producto de la aplicación de la metodología se contará con los mapas de riesgo.

Además de esta herramienta, se tienen las siguientes:

**3.4.1 Gestión de eventos:** Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

**Desempeño del control**= # eventos / frecuencia del riesgo (# veces que se hace la actividad)

**3.4.2 Indicadores clave de riesgo**: Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

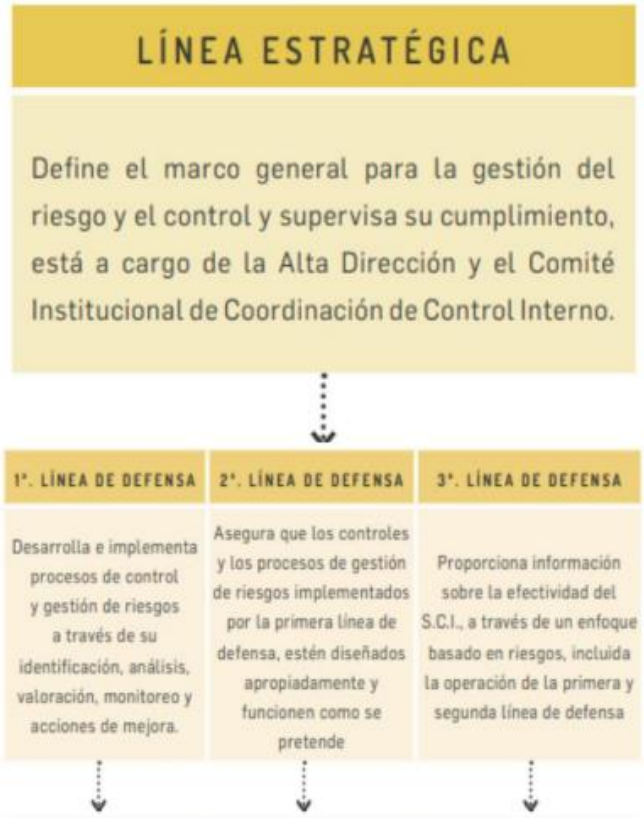
Tabla 13. Ejemplos indicadores clave de riesgo

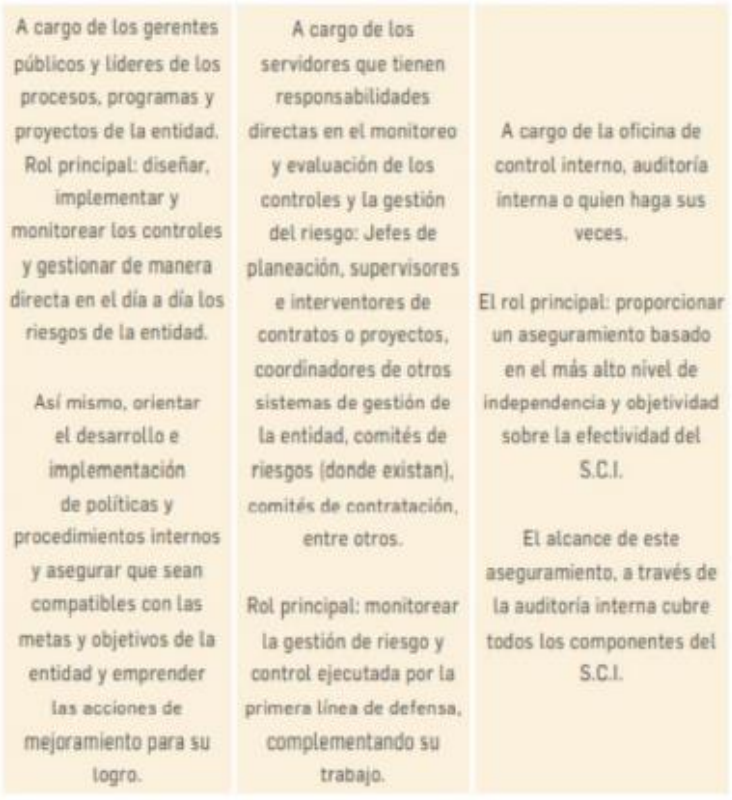
| PROCESO ASOCIADO | INDICADOR | MÉTRICA |
|---|---|---|
| TIC | Tiempo de interrupción de aplicativos críticos en el mes | Número de horas de interrupción de aplicativos críticos al mes |
| FINANCIERA | Reportes emitidos al regulador fuera del tiempo establecido | Número de reportes mensuales remitidos fuera de términos |
| ATENCIÓN AL USUARIO | Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados | % solicitudes mensuales fuera de términos<br>% solicitudes reiteradas por tema |
| ADMINISTRATIVO Y FINANCIERA | Errores en transacciones y su impacto en la gestión presupuestal | Volumen de transacciones al mes sobre la capacidad disponible |
| TALENTO HUMANO | Rotación de personal | % de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses |

**3.5 Monitoreo y revisión:** El modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad

de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

Tabla 14. Esquema de líneas de defensa





| | | |
|---|---|---|
| A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad. Rol principal: diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.<br><br>Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro. | A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.<br><br>Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo. | A cargo de la oficina de control interno, auditoría interna o quien haga sus veces.<br><br>El rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.<br><br>El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I. |

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

**Paso 4: LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN:**

Continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Por lo anterior es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento. Para mayor facilidad, a continuación, se transcriben algunos de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018, que reiterando sigue vigente.

**Definición de riesgo de corrupción:**

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con u na X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

Tabla 15. Matriz de definición del riesgo de corrupción

| MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN | | | | |
|---|---|---|---|---|
| **Descripción del riesgo** | **Acción u omisión** | **Uso del poder** | **Desviar la gestión de lo público** | **Beneficio privado** |
| Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato. | X | X | X | X |

Fuente: Secretaría de Transparencia de la Presidencia de la República.

**Generalidades acerca de los riesgos de corrupción:**

- **Entidades encargadas de gestionar el riesgo:** lo deben adelantar las entidades del orden nacional, departamental y municipal.
- Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.
- **Consolidación**: La oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de

administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

- La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.

- En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

- Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.

- Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- **Ajustes y modificaciones**: Se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- **Monitoreo:** En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

- **Seguimiento:** El jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de

corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

**Acciones a seguir en caso de materialización de riesgos de corrupción**

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo

**Paso 5. Lineamientos riesgos de seguridad de la información**

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) 3, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

**5.1 Identificación de los activos de seguridad de la información:** Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

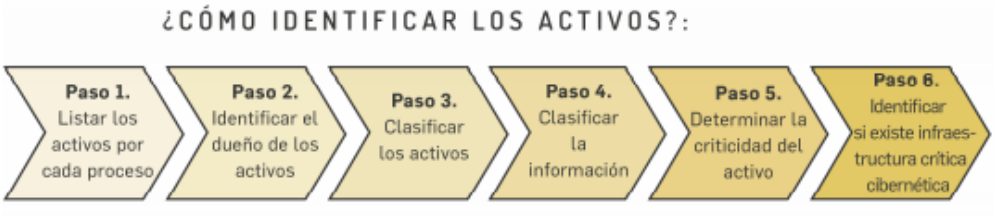
"Por medio del cual se adopta la Política de Administración del Riesgo del Instituto de Cultura y Patrimonio de Antioquia y se deroga la resolución 000081 del 27 de febrero de 2019"

Tabla 15. Conceptualización activos de información

| ¿Qué son los activos? | ¿Por qué identificar los activos? |
|---|---|
| Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:<br>-Aplicaciones de la organización | Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). |
| -Servicios web<br>-Redes<br>-Información física o digital<br>-Tecnologías de información TI<br>-Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital | La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital. |

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

Figura 13. Pasos para la identificación de activos




Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

**Nota:** para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas" que hace parte de los anexos de la presente guía.

Tabla 16. Ejemplo identificación activos del proceso

| Proceso | Activo | Descripción | Dueño del activo | Tipo del activo | Ley 1712 de 2014 | Ley 1581 de 2012 | Criticidad respecto a su confidencialidad | Criticidad respecto a completitud o integridad | Criticidad respecto a su disponibilidad | Nivel de criticidad |
|---|---|---|---|---|---|---|---|---|---|---|
| Gestión financiera | Base de datos de nómina | Base de datos con información de nómina de la entidad | Jefe de oficina financiera | Información | Información reservada | No contiene datos personales | ALTA | ALTA | ALTA | ALTA |
| Gestión financiera | Aplicativo de nómina | Servidor web que contiene el *front office* de la entidad | Jefe de oficina financiera | Software | N/A | N/A | BAJA | MEDIA | BAJA | MEDIA |
| Gestión financiera | Cuentas de cobro | Formatos de cobro diligenciados | Jefe de oficina financiera | Información | Información pública | No contiene datos personales | BAJA | BAJA | BAJA | BAJA |

**5.2. Identificación del riesgo**: se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de 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. Para este efecto , es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla 5. Tabla de amenazas comunes
Tabla 6. Tabla de amenazas dirigida por el hombre
Tabla 7. Tabla de vulnerabilidades comunes

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.

Tabla 17. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

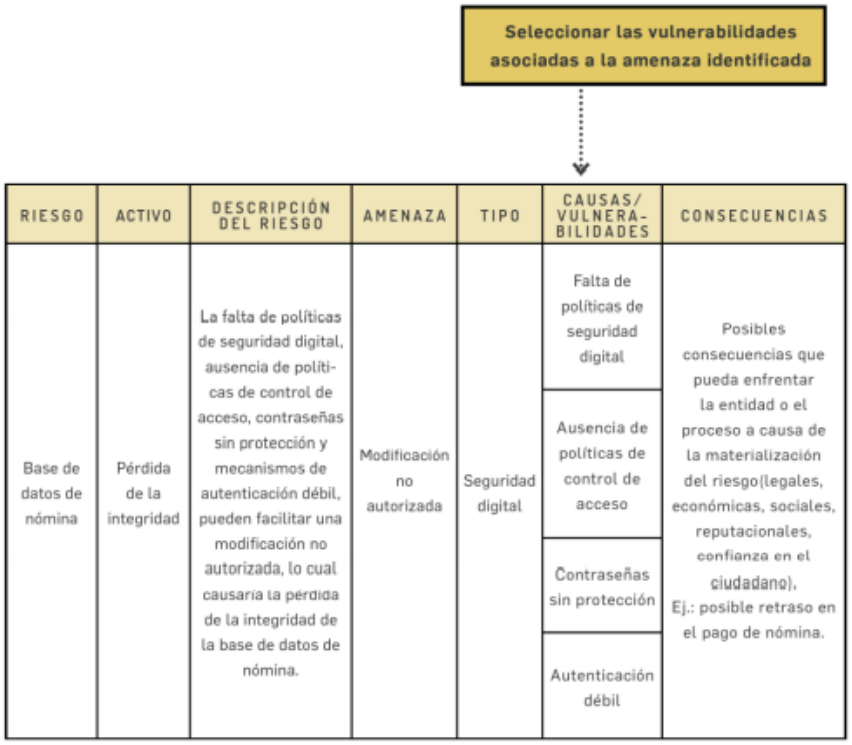
| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| Hardware | Almacenamiento de medios sin protección | Hurto de medios o documentos |
| Software | Ausencia de parches de seguridad | Abuso de los derechos |
| Red | Líneas de comunicación sin protección | Escucha encubierta |
| Información | Falta de controles de acceso físico | Hurto de información |

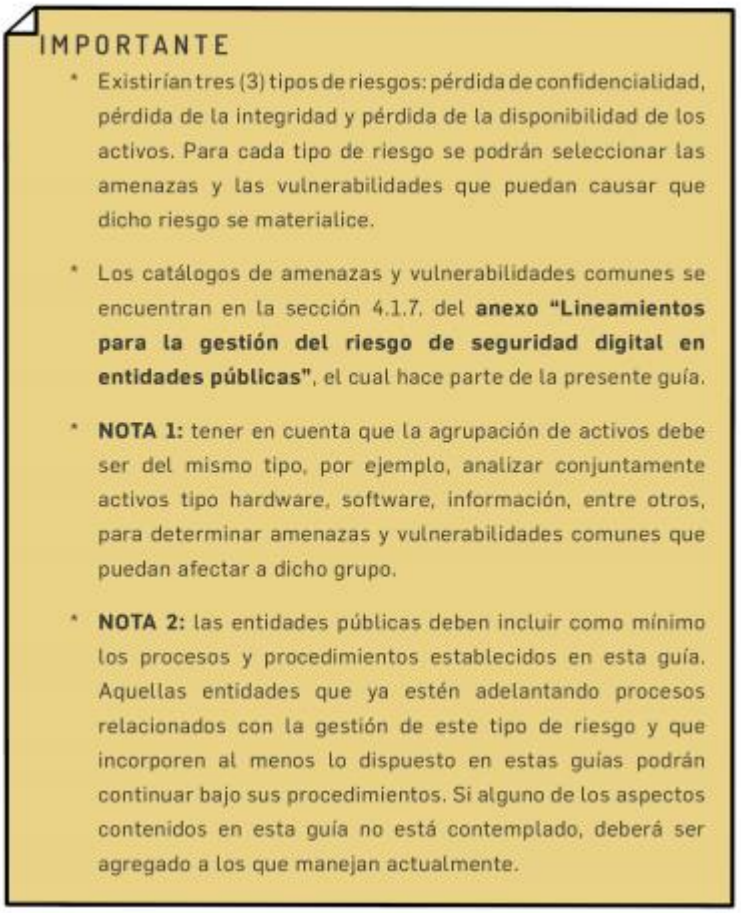
| Tipo de activo | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| Personal | Falta de capacitación en las herramientas | Error en el uso |
| Organización | Ausencia de políticas de seguridad | Abuso de los derechos |

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

En la figura 14 se observa un ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina.

Figura 14. Formato de descripción del riesgo de seguridad de la información






**5.3. Valoración del riesgo:** Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

En este sentido, se debe considerar para este análisis la tabla 4 definida en el aparte 3.1.1, la cual se retoma a continuación:

| | 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% |

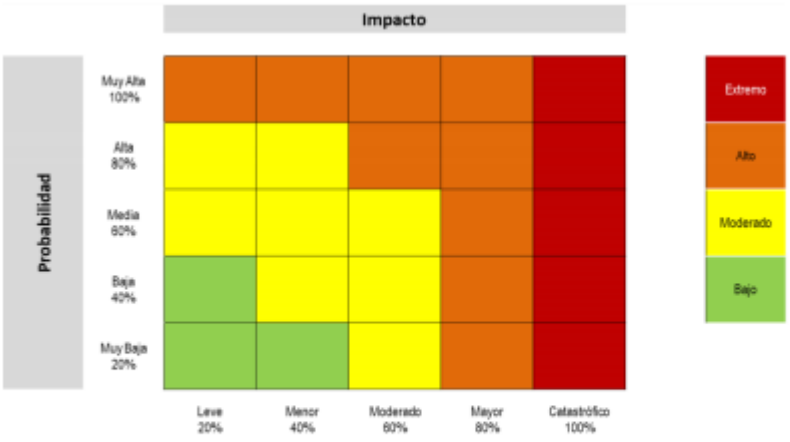
La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 de la presente guía, entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

En este sentido, se debe considerar para este análisis la tabla 5 definida en el aparte 3.1.2, que se retoma a continuación:

| | 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 |

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello,

Se aplica la matriz de calor establecida en el numeral 3.2.1 de la presente guía, que se retoma a continuación:




En la figura 24 se observa un ejemplo aplicando la etapa de valoración del riesgo sobre un activo como es la base de datos de nómina.

Figura 15. Valoración del riesgo en seguridad de la información

**IMPORTANTE**

Cada entidad deberá adaptar los criterios a su realidad.
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

| RIESGO | ACTIVO | AMENAZA | VULNERABILIDAD | PROBABILIDAD | IMPACTO | ZONA DE RIESGO |
|---|---|---|---|---|---|---|
| Pérdida de la Confidencialidad | Base de datos de nómina | Modificación no autorizada | Ausencia de políticas de control de acceso | 4-Probable | 4- Mayor | Extrema |
| | | | Contraseñas sin protección | | | |
| | | | Ausencia de mecanismos de identificación y autenticación de usuarios | | | |
| | | | Ausencia de bloqueo de sesión | | | |

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

| |
|---|
| Extremo |
| Alto |
| Moderado |
| Bajo |

**IMPORTANTE:**
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

### 5.4 Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla 18 Controles para riesgos de seguridad de la información

| **Procedimientos operacionales y responsabilidades** | **Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información** |
|---|---|
| **Procedimientos de operación documentados** | Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten. |
| **Gestión de cambios** | Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. |
| **Gestión de capacidad** | Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura. |
| **Separación de los ambientes de desarrollo, pruebas y operación** | Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. |
| **Protección contra códigos maliciosos** | Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. |
| **Controles contra códigos maliciosos** | Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos. |
| **Copias de respaldo** | Objetivo: proteger la información contra la perdida de datos. |
| **Respaldo de información** | Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. |

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

Figura 16 Formato mapa riesgos seguridad de la información

| N. | RIESGO | ACTIVO | TIPO | AMENAZAS | TIPO | PROBABILIDAD | IMPACTO | RIESGO RESIDUAL | OPCIÓN TRATAMIENTO | ACTIVIDAD DE CONTROL | SOPORTE | RESPONSABLE | TIEMPO | INDICADOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | **Pérdida de la integridad** | Base de datos de nómina | Seguridad digital | Modificación no autorizada | Ausencia de políticas de control de acceso | **Probable** | **Menor** | **Moderado** | Reducir | A.9.1.1 Política de control de acceso | Política creada y comunicada | Oficina TI | Tercer trimestre de 2018 | **EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100<br>**EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas) |
| | | | | | Contraseñas sin protección | | | | Reducir | A.9.4.3 Sistema de gestión de contraseñas | Procedimientos para la gestión y protección de contraseñas | Oficina TI | Tercer trimestre de 2018 | |
| | | | | | Ausencia de mecanismos de identificación y autenticación de usuarios | | | | Reducir | A 9.4.2 Procedimiento de ingreso seguro | Procedimiento para ingreso seguro | Oficina TI | Tercer trimestre de 2018 | |
| | | | | | *Ausencia de bloqueo | | | | Reducir | A.11.2.8 Equipos de usuario desatendidos | Configuraciones para bloqueo automático de sesión | Oficina TI | Tercer trimestre de 2018 | |

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

**ARTÍCULO OCTAVO. MONITOREO Y EVALUACIÓN.** Anualmente los líderes de proceso con sus respectivos equipos de trabajo identifican y/o validan los riesgos de gestión, corrupción y seguridad digital asociados al logro de los objetivos de los procesos institucionales. Para ello, documentarán lo propio en las hojas de trabajo institucionales y podrán contar con el acompañamiento de la Subdirección de Planeación.

Los riesgos de gestión, corrupción y seguridad digital que se encuentren en zona de riesgo BAJO, que soporten documentación de sus controles en procedimientos, se evidencie la implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser considerados para su eliminación.

A continuación, se encuentra una tabla de resumen con la frecuencia y responsable de cada reporte:

| RESPONSABLE | FRECUENCIA | REPORTE |
|---|---|---|
| **COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO** | Anual | Pronunciamiento sobre el perfil de riesgo inherente y residual de la entidad. |
| | Semestral | Análisis de los riesgos institucionales. |
| | Trimestral | Seguimiento sobre los riesgos ubicados en la zona de riesgo extremo. |
| **LÍDERES DE PROCESO** | Acorde al nivel de Riesgo Residual:<br>• MODERADO: Trimestral<br>• ALTO: Bimensual<br>• EXTREMO: Mensual | Seguimiento sobre los riesgos en el formato estandarizado de reporte y/o en la plataforma SICPA. |
| **SUBDIRECCIÓN DE PLANEACIÓN** | Semestral | Estado del arte de implementación de la política institucional de administración del riesgo, socializado mediante resolución. |
| | Trimestral | • Seguimiento a los mapas de riesgo<br>• Eventos de riesgos que se han materializados en la entidad |
| **JEFE OFICINA DE CONTROL INTERNO** | Cuatrimestral | Seguimiento a la gestión de riesgos de corrupción |
| | De conformidad con el Plan Anual de Auditoria | Seguimiento a los riesgos consolidados en los mapas de riesgos |

**ARTÍCULO NOVENO. ESTRATEGIAS DE COMUNICACIÓN TRANSVERSALES.** Los mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad serán acordes al Plan de Comunicaciones Institucional. Con el fin de construir una relación de confianza entre la Entidad y la ciudadanía que derive en el fortalecimiento institucional, se vincularán en las distintas etapas de la gestión del riesgo para:

- Identificar puntos críticos sobre los procesos que permitan mejorar la presentación del servicio y satisfacer las necesidades de los ciudadanos.
- Realizar una valoración sobre la probabilidad e impacto de los riesgos para determinar el nivel de riesgo al que está expuesta la entidad.
- Diseñar y ejecutar controles que atiendan la(s) causa(s) que generan los riesgos.
- Realizar seguimiento a los controles.

"Por medio del cual se adopta la Política de Administración del Riesgo del Instituto de Cultura y Patrimonio de Antioquia y se deroga la resolución 000081 del 27 de febrero de 2019"

- Facilitar la generación de alertas tempranas y oportuna toma de decisiones.

**ARTÍCULO DECIMO. VIGENCIA.** El presente acto administrativo rige a partir de la fecha de su expedición y deroga la Resolución No. 000081 del 27 de febrero de 2021.

**COMUNÍQUESE Y CÚMPLASE**

Dada en Medellín, a los

**MARCELA ISABEL TRUJILLO QUINTERO**
Directora

| | | | | | |
|---|---|---|---|---|---|
| Proyectó: | Sandra Díaz R<br>Sandra Milena Díaz Ríos<br>Contratista de apoyo MIPG | Revisó: | William A. García T.<br>Profesional Universitario – Líder Jurídica y Contratación<br><br>Tatiana Marina Correa Sánchez<br>Subdirección de Planeación<br><br>Juan David Mejía Mejía<br>Subdirección de Patrimonio y Fomento artístico y cultural | Aprobó: | Alejandro Quintero Coral<br>Subdirector Administrativo y Financiero<br><br>Presidente del Comité Institucional de Gestión y Desempeño |