

**MANUAL**

**Política de Administración del Riesgo**

**BOGOTÁ, D.C. NOVIEMBRE**

**2022**

TABLA DE CONTENIDO

[POLÍTICA DE ADMINISTRACIÓN DE RIESGO 5](#_Toc116995102)

[1. OBJETIVOS 5](#_Toc116995103)

[2. ALCANCE DE LA POLÍTICA 5](#_Toc116995104)

[3. TÉRMINOS Y DEFINICIONES 6](#_Toc116995105)

[4. ROLES Y RESPONSABILIDADES 9](#_Toc116995106)

[5. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS 11](#_Toc116995107)

[5.1. IDENTIFICACIÓN DEL RIESGO 12](#_Toc116995108)

[5.1.1. Análisis de objetivos estratégicos y de los procesos: 12](#_Toc116995109)

[5.1.2. Identificación de los puntos de riesgo 12](#_Toc116995110)

[5.1.3. Identificación de áreas de factores de riesgos impacto 14](#_Toc116995111)

[5.1.4. Descripción del riesgo 15](#_Toc116995112)

[5.1.5. Clasificación del riesgo 17](#_Toc116995113)

[5.2. VALORACIÓN DE RIESGOS – RIESGO INHERENTE. 18](#_Toc116995114)

[5.2.1. Análisis de Riesgos 18](#_Toc116995115)

[5.2.2. Evaluación de riesgo inherente 20](#_Toc116995116)

[5.3. VALORACIÓN DE CONTROLES 21](#_Toc116995117)

[5.3.1. Definición y clasificación de controles: 21](#_Toc116995118)

[5.3.2. Análisis y evaluación de los controles 22](#_Toc116995119)

[5.4. EVALUACIÓN DE CONTROLES - RIESGO RESIDUAL: 23](#_Toc116995120)

[5.5. TRATAMIENTO DE RIESGOS 25](#_Toc116995121)

[5.5.1. Plan de acción 25](#_Toc116995122)

[5.5.2. Plan de contingencia 25](#_Toc116995123)

[5.6. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 25](#_Toc116995124)

[5.6.1. Identificación de los activos de seguridad de la información 25](#_Toc116995125)

[5.6.2. Identificación riesgos de seguridad de la información 28](#_Toc116995126)

[5.6.3. Identificación de amenazas y vulnerabilidades 29](#_Toc116995127)

[5.6.4. Controles asociados a la seguridad de la información 34](#_Toc116995128)

[6. MONITOREO Y SEGUIMIENTO 34](#_Toc116995129)

[7. AJUSTES Y MODIFICACIONES: 35](#_Toc116995130)

[8. LINEAMIENTOS PARA EL MANEJO DE RIESGOS MATERIALIZADOS 36](#_Toc116995131)

**LISTADO DE TABLAS**

[Tabla 1 Factores de riesgo 14](#_Toc116994907)

[Tabla 2 Errores en la redacción de riesgos 17](#_Toc116994908)

[Tabla 3 Descripción del riesgo de corrupción 17](#_Toc116994909)

[Tabla 4 Clasificación de Riesgos 17](#_Toc116994910)

[Tabla 5 Criterios parar calificar la probabilidad 19](#_Toc116994911)

[Tabla 6 Criterios para definir el nivel de impacto 19](#_Toc116994912)

[Tabla 7 Criterios para determinar impacto de corrupción 20](#_Toc116994913)

[Tabla 8 Matriz de calor (niveles de severidad del riesgo) 21](#_Toc116994914)

[Tabla 9 Riesgo Inherente 21](#_Toc116994915)

[Tabla 10 Criterios para la evaluación de los controles 23](#_Toc116994916)

[Tabla 11 Aplicación de controles para establecer el riesgo residual 24](#_Toc116994917)

[Tabla 12 Clasificación de Activos 26](#_Toc116994918)

[Tabla 13 Clasificación de acuerdo con la confidencialidad 27](#_Toc116994919)

[Tabla 14 Clasificación de acuerdo con la integridad 28](#_Toc116994920)

[Tabla 15 Clasificación de acuerdo con la disponibilidad 28](#_Toc116994921)

[Tabla 16 Niveles de clasificación 28](#_Toc116994922)

[Tabla 17 Amenazas más comunes 29](#_Toc116994923)

[Tabla 18 Vulnerabilidades más comunes 31](#_Toc116994924)

[Tabla 19 Ejemplos de vulnerabilidades y amenazas 32](#_Toc116994925)

**LISTADO DE ILUSTRACIONES**

[Ilustración 1 Metodología para la administración del riesgo 11](#_Toc116995969)

[Ilustración 2 Cadena de valor 13](#_Toc116995970)

[Ilustración 3 Tipo de impacto 13](file:///C:\Users\natis\Downloads\DESI-MA-002-V10%20Politica%20Administracion%20del%20Riesgo%20EN%20ACTUALIZACIÓN%20PR.docx#_Toc116995971)

[Ilustración 4 Descripción del riesgo 16](#_Toc116995972)

[Ilustración 5 Ejemplo Descripción del riesgo 16](#_Toc116995973)

[Ilustración 6 Ciclo del proceso y las tipologías de controles 22](#_Toc116995974)

[Ilustración 7 Movimiento en la matriz de calor acorde con el tipo de control 24](#_Toc116995975)

[Ilustración 8 Esquema Pasos para identificar los activos 26](#_Toc116995976)

# POLÍTICA DE ADMINISTRACIÓN DE RIESGO

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial - UAERMV, establece su política de administración del riesgo como expresión del compromiso de la alta dirección en administrar los riesgos de gestión, de corrupción y de seguridad digital, que puedan dificultar la misión y el cumplimento de los objetivos, proyectos y/o procesos institucionales, mediante la implementación y reporte de controles preventivos, defectivos o correctivos con la participación de los colaboradores para fortalecer la cultura de la prevención de eventos, acciones u omisiones.

# OBJETIVOS

* **Analizar el contexto interno y externo:** Identificar oportunamente el contexto interno y externos de la entidad a través de sus procesospara la identificación de posibles riesgos.
* **Identificar, analizar y gestionar los riesgos:** Fomentar en la Entidad una cultura de pensamiento basado en riesgo, como herramienta para incrementar la eficacia en el logro de los resultados institucionales.
* **Promover el reporte oportuno:** Fortalecer los seguimientos, análisis y validación en la efectividad de controles y la implementación de acciones, que permitan detectar de forma oportuna situaciones de riesgos potenciales.
* **Prevenir la materialización de los riesgos:** Involucrar y comprometer a todos los colaboradores de la Unidad en la búsqueda de acciones efectivas encaminadas a prevenir y administrar los riesgos de forma oportuna.
* **Fortalecer la generación de buenas prácticas:** Promover en los colaboradores de la Unidad la identificación de buenas prácticas atreves de acciones que permitan potencializar el cumplimiento de los objetivos de institucionales y fortalecer los controles existentes.

# ALCANCE DE LA POLÍTICA

La política de riesgos es aplicable a todos los procesos y proyectos de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. Esta debe ser conocida, aplicada y apropiada por todos los colaboradores de la entidad, dado que abarca los principios básicos y metodológicos para la administración y gestión de riesgos a nivel de procesos, aprobados para las entidades públicas y adaptados en lo pertinente a las funciones de la Entidad.

Las políticas y las acciones definidas para el manejo de los riesgos son de carácter obligatorio para todos los colaboradores, en las diferentes dependencias de la Entidad.

Los mapas de riesgos por proceso deberán ser aprobados por los Responsables Directivos. Además, el Comité Institucional de Gestión y Desempeño, podrá incluir los riesgos potenciales que no hayan sido incluidos en el mapa de riesgos.

# TÉRMINOS Y DEFINICIONES

* **Activo** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
* **Administración del riesgo:** “Un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación”[[1]](#footnote-2)
* **Amenaza:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
* **Análisis del Riesgo:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
* **Apetito de 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.
* **Autocontrol:** Es la capacidad que tiene cada servidor público, independientemente de su nivel jerárquico dentro de la institución, para evaluar su trabajo, detectar desviaciones, efectuar correctivos, mejorar y solicitar ayuda cuando lo considere necesario, de tal manera que la ejecución de los procesos, actividades y tareas bajo su responsabilidad garanticen el ejercicio de una función administrativa transparente y eficaz.
* **Causas:** 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.
* **Consecuencias:** 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.
* **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
* **Control:** Medida que permite reducir o mitigar un riesgo.
* **Corrupción:** Abuso de poder o de confianza para el beneficio particular en detrimento del interés colectivo, en el que se incurre al ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios a cambio de acciones, decisiones u omisiones
* **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
* **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
* **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
* **Gestión de 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.
* **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la organización la materialización del riesgo; se refiere a la magnitud de sus efectos.
* **Integridad:** propiedad de exactitud y completitud.
* **Mapa de riesgos:** Es la herramienta metodológica que permite hacer un inventario de los riesgos de manera ordenada y sistemática. Permite definirlos, describirlos, indicar sus posibles consecuencias, así como indicar la probabilidad, el impacto inherente facilitando el registro de las acciones a seguir.
* **Monitoreo:** Análisis continuo del estado de las actividades de un proceso durante su ejecución. Es un proceso interno coordinado con los responsables de la acción.
* **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 poder ser 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
* **Probabilidad:** se entiende como 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.
* **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
* **Regalo**: Todo pago, gratuidad, gratificación, regalo o beneficio, pecuniario o no, ofrecido, prometido, dado o recibido, sin ninguna compensación material o inmaterial directa o indirecta
* **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 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.
* **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.[[2]](#footnote-3)
* **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
* **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Condiciones que pueden debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
* **Seguimiento**: Observación minuciosa del desarrollo de un proceso, revisa continuamente la evolución del rendimiento respecto de lo previsto, mediante el análisis de datos e indicadores establecidos con fines de seguimiento y evaluación. Para efectos de la presente política, el seguimiento es una actividad propia de la primera y tercera línea de defensa.
* **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.
* **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

# ROLES Y RESPONSABILIDADES

La gestión del riesgo se desarrolla en estricto cumplimiento de la dimensión de Control Interno del Modelo Integrado de Planeación y Gestión, atendiendo la responsabilidad de este mediante la aplicación de las líneas de defensa durante las etapas de desarrollo de la gestión institucional, así:

**LÍNEA ESTRATEGICA:**

Está conformada por el Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno y tienen a cargo las siguientes responsabilidades:

* Definir y evaluar la Política de Administración del Riesgo. La evaluación debe considerar su aplicación, seguimiento, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo y riesgos emergentes.
* Revisar, y hacer seguimientos de las políticas de control, los resultados de las evaluaciones y a la auditoría interna para toda la entidad.
* Evaluar la forma como funciona el Esquema de Líneas de Defensa
* Revisar el cumplimiento de los objetivos institucionales y de procesos, con sus respectivos indicadores e identificar los posibles riesgos, en caso de que no se estén cumpliendo.
* Revisar los informes presentados por lo menos cada cuatrimestre de los eventos de riesgos de corrupción que se han materializado en la entidad, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas.
* Revisar las acciones de contingencia establecidas para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
* Asegurar los recursos necesarios para ayudar a los responsables de gestionar y tratar los riesgos.
* Determinar los valores de probabilidad e impacto de acuerdo con la Guía de riesgos de la Departamento Administrativo de la función publica

**PRIMERA LÍNEA DE DEFENSA**

Está conformada por los colaboradores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Tienen a cargo las siguientes responsabilidades:

* Conocer y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus procesos.
* Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.
* Identificar, analizar y valorar los riesgos que pueden afectar los proyectos, planes y procesos a su cargo
* Actualizar, aprobar y proponer mejoras al mapa de riesgos, frente a sus controles, acciones y planes de contingencia, cuando se requiera.
* Definir, ejecutar, y hacer seguimiento a los controles para mitigar los riesgos identificados.
* Alinear los riesgos identificados con las metas, objetivos y proyectos, según aplique.
* Realizar la identificación de activos de información, físicos y humanos en su proceso y valorar la criticidad del activo de información.
* Reportar a la Oficina Asesora de Planeación (segunda línea) los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
* Reportar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados.

**SEGUNDA LÍNEA:**

Está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. Se incluye el jefe de planeación, coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, secretaría general como líder de contratación, financiera, TIC, sistemas de gestión, entre otros. Tienen a cargo las siguientes responsabilidades:

* Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgos, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
* Consolidar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité CIGD.
* Acompañar, orientar y entrenar a los procesos en la identificación, análisis y valoración del riesgo.
* Monitorear los controles y acciones establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y generar recomendaciones para que sean apropiados y funcionen correctamente
* Presentar al Comité CIGD los resultados del monitoreo de los mapas de riesgos de los procesos

**TERCERA LÍNEA**

Está conformada por la Oficina de Control Interno y tienen a cargo las siguientes responsabilidades:

* Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.
* Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.
* Evaluar las actividades adelantadas por la segunda línea de defensa frente a la gestión del riesgo (oficina de planeación, direcciones o gerencias de riesgo), específicamente frente al análisis de contexto y de identificación del riesgo y de ser necesario asesorarlas, a fin de incorporar las mejoras correspondientes (Rol Evaluación de la Gestión del Riesgo)
* Informar los hallazgos y proporcionar recomendaciones de forma independiente.
* Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.
* Recomendar mejoras a la política de administración del riesgo.

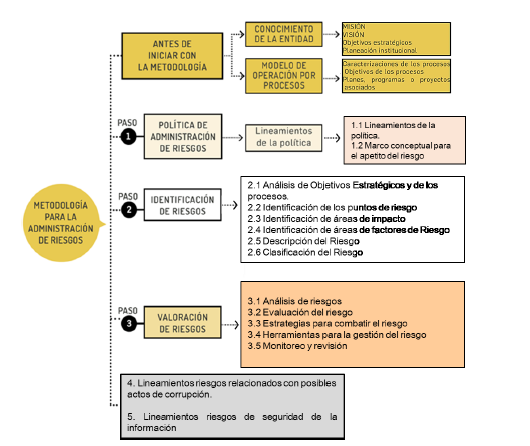
# METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

Con el fin de ejercer una correcta administración del riesgo, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial - UAERMV en cumplimiento de la normatividad, adoptó la guía establecida por el Departamento Administrativo de la Función Pública DAFP.

Como producto de la aplicación de la metodología descrita es este documento, quedará como registro los mapas de riesgo por proceso, los cuales se consolidan en una única herramienta denominada “mapa de riesgos institucional”. La Oficina Asesora de Planeación actualiza el mapa de riesgos institucional por lo menos dos veces al año, quedando disponible para consulta en la página web de la entidad.

A continuación, se presentan los elementos adoptados por la UAERMV para la adecuada administración de los riesgos.

Ilustración 1 Metodología para la administración del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas

Versión 5 diciembre 2020. DAFP. Pág. 20.

## IDENTIFICACIÓN DEL RIESGO

El propósito de este paso es identificar los riesgos que están dentro o fuera del control de la Unidad.

***¿Qué se debe tener en cuenta para identificar los riesgos?***

* Entender el proceso considerando su objetivo, propósito y alcance
* Revisar los factores de riesgo detectados en la etapa del análisis del contexto estratégico.
* Identificar “qué puede fallar” para cada actividad clave del proceso.
* Identificar el inventario de activos de información

Para la revisión del contexto se analizan las condiciones internas y externas (del entorno) de la Unidad y de los procesos, que pueden generar eventos o situaciones que afecten negativamente el cumplimiento de la misión y objetivos de la UAERMV.

**Análisis Interno**: El análisis interno se realiza identificando debilidades y fortalezas en la organización que puedan interferir con el logro de los objetivos institucionales. Están relacionadas con la estructura orgánica, cultura organizacional, el modelo de operación por procesos, el cumplimiento de los planes y programas, los sistemas de información, los procesos y procedimientos, los recursos humanos y económicos con los que cuenta la entidad.

**Análisis Externo**: Aquí se identifican circunstancias externas a la entidad que pueden intervenir en el cumplimiento de los objetivos. Las cuales pueden ser de carácter social, cultural, económico, ambiental, cambio tecnológico, político-legal, internacional, nacional o regional según sea el análisis.

Es importante tener presente que el objetivo de esta etapa es reunir toda la información que permita tener una mirada global sobre los factores de riesgo que rodean a la entidad y al proceso que se está analizando.

El contexto estratégico es la base para la identificación del riesgo, dado que su análisis suministra la información sobre sus causas.

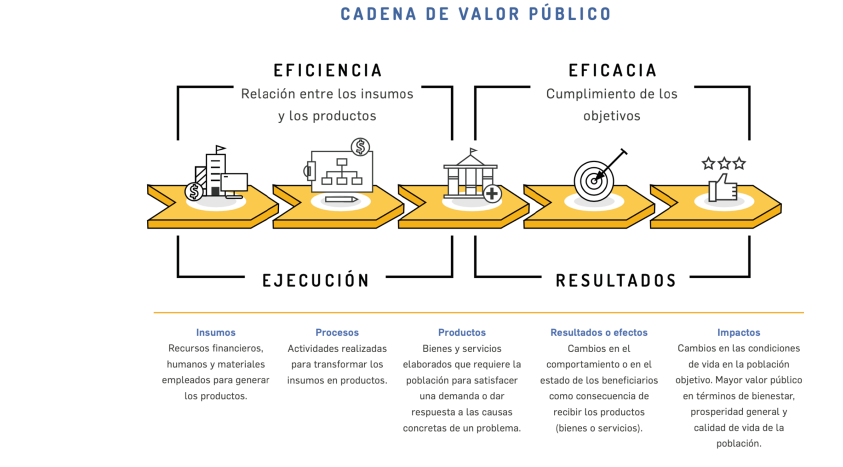
## Análisis de objetivos estratégicos y de los procesos:

Los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso. Los objetivos deben incluir el qué, cómo, para qué, cuándo y cuánto. Así mismo, deben estar alineados con la misión y la visión institucionales.

## Identificación de los puntos de riesgo

Son actividades dentro del proceso qué evidencian o presentan indicios de que pueden ocurrir eventos de riesgo operacional y deben ser controlados para asegurar que el proceso logre sus metas.

Ilustración 2 Cadena de valor



**Fuente:** Guía para la administración del riesgo y el diseño de controles en entidades públicasVersión 5 diciembre 2020. DAFP. Pág. 30.

Identificación de áreas de impacto

Ilustración 3 Tipo de impacto

El área de impacto es la consecuencia: económica o reputacional a la cual se ve expuesta la Unidad en caso de materializarse un riesgo.

## Identificación de áreas de factores de riesgos impacto

Son las fuentes generadoras de riesgos

Tabla 1 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 |
| D:\cmunoz\Documents\Downloads\contrato.png | Errores de grabación, autorización |
| D:\cmunoz\Documents\Downloads\sitio-web (1).png | Errores en cálculos para pagos internos y externos |
| D:\cmunoz\Documents\Downloads\conversacion.png | 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. | D:\cmunoz\Documents\Downloads\ordenador.png | Hurto activos |
|  | Posibles comportamientos no éticos de los empleados |
|  | Fraude interno (corrupción, soborno) |
| Tecnología | Eventos relacionados con la infraestructura tecnológica de la entidad. | D:\cmunoz\Documents\Downloads\sitio-web (1).png | Daño de equipos |
|  | Caída de aplicaciones |
|  | Caída de redes |
|  | Errores en programas |
| Infraestructura | Eventos relacionados con la infraestructura física de la entidad. | Corrimiento Tierras | Vectores, Fotos de Stock y PSD Gratis | Derrumbes |
| seguro contra incendios - Iconos gratis de negocio | Incendios |
|  | Inundaciones |
|  | Daños a activos fijos |
| Evento externo | Situaciones externas que afectan la entidad. | D:\cmunoz\Documents\Downloads\ordenador.png | Suplantación de identidad |
| D:\cmunoz\Documents\Downloads\dolares-no-aceptados.png | Asalto a la oficina |
|  | Atentados, vandalismo, orden público |

**Fuente:** Guía para la administración del riesgo y el diseño de controles en entidades públicas

Versión 5 diciembre 2020. DAFP. pág. 31.

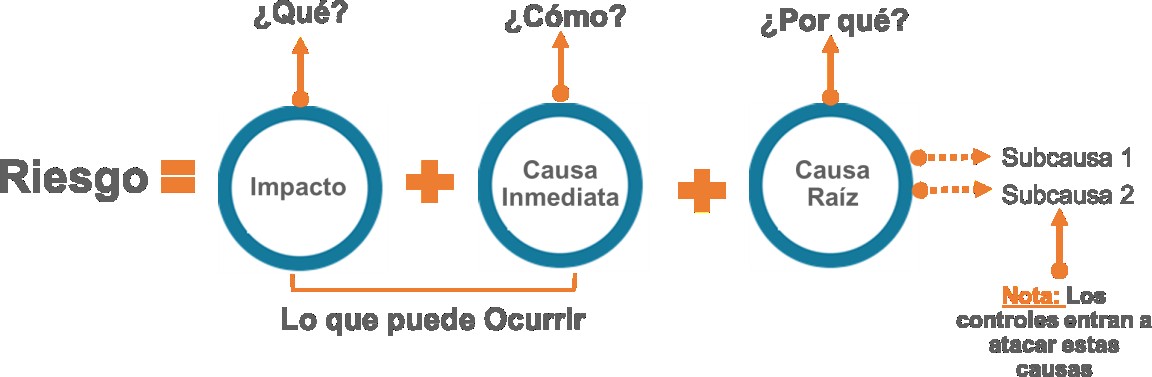
## Descripción del riesgo

Se debe realizar la **descripción** del **ri**esgo, ésta debe estar escrita de manera clara, sin que su redacción dé lugar a ambigüedades o confusiones.

Estructura para la descripción del riesgo:

* ¿QUÉ PUEDE SUCEDER? Identificar las consecuencias o impacto que puede ocasionar la materialización del riesgo y afecta el cumplimiento de los objetivos.
* ¿CÓMO PUEDE SUCEDER? Establecer la 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.
* ¿POR QUÉ PUEDE SUCEDER? Determinar la causa raíz corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Ilustración 4 Descripción del riesgo

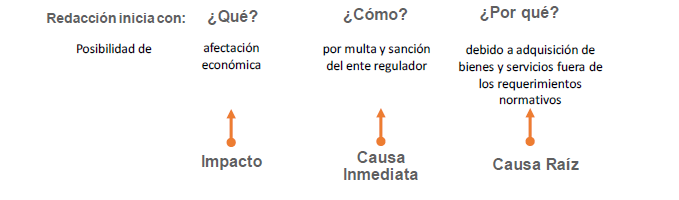


**Fuente**: Guía para la administración del riesgo y el diseño de controles en entidades públicasVersión 5 diciembre 2020. DAFP. pág. 32

Para la adecuada redacción del riesgo se debe Iniciar con la frase **posibilidad de**

Ejemplo:

Ilustración 5 Ejemplo Descripción del riesgo



**Fuente**: Guía para la administración del riesgo y el diseño de controles en entidades públicasVersión 5 diciembre 2020. DAFP. pág. 34

Así mismo, tenga en cuenta los posibles errores al momento de redactar un riesgo:

Tabla 2 Errores en la redacción de riesgos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Premisa** | No describir como riesgos omisiones ni desviaciones del control | No describir causas como riesgos | No describir riesgos como la negación de un control. | No existen riesgos transversales, lo que pueden existir son causas transversales |
| **Ejemplo** | Errores en la liquidación de la nómina por fallas en los procedimientos existentes. | Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación. | Retrasos en la prestación del servicio por no contar con digiturno para la atención. | Pérdida de expedientes. |

Nota: 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 debe revisar que se contenga cada uno de los componentes citados en la siguiente tabla:

Tabla 3 Descripción del riesgo de corrupción

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción u omisión** | **Uso del poder** | **Desviar la gestión de lo público** | **Beneficio privado.** |
| X | X | X | X |

Fuente: Adaptado Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 69.

## Clasificación del riesgo

Se debe realizar la clasificación de riesgos según las siguientes categorías:

Tabla 4 Clasificación de Riesgos

| Tipo | Clasificación | Descripción |
| --- | --- | --- |
| Gestión | **Ejecución y administración de procesos** | Pérdidas derivadas de errores en la ejecución y administración de procesos. |
| Gestión | **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. |
| Gestión | **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. |
| Gestión | **Fallas tecnológicas** | Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos. |
| Corrupción | **Fraude externo** | Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad). |
| Corrupción | **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. |
| Corrupción | **Soborno** | Cuando una persona da u ofrece “dinero u otra utilidad para que se realice u omita un acto propio del cargo de un funcionario público, o para que se ejecute uno contrario a sus deberes oficiales” |
| Seguridad Digital | **Pérdida de la confidencialidad** | Determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. |
| Seguridad Digital | **Pérdida de la integridad** | Determina la exactitud y completitud de la información, permitiendo que la información sea precisa, coherente y completa desde su creación hasta su destrucción. |
| Seguridad Digital | Pérdida de la disponibilidad | Determina la accesibilidad y utilización de la información por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. |

Fuente: Adaptado Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 35

## VALORACIÓN DE RIESGOS – RIESGO INHERENTE.

En este paso se debe establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

## Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y sus consecuencias o impacto, calificándolos y evaluándolos con el fin de estimar la zona de riesgo inherente.

Se sugiere realizar este análisis con el grupo de personas que más conozcan del proceso y que por sus conocimientos o experiencia puedan determinar la probabilidad y el impacto del riesgo de acuerdo con los rangos señalados así:

#### **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo, asociada a la exposición al riesgo del 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.

Tabla 5 Criterios parar calificar la probabilidad

|  |  |  |
| --- | --- | --- |
|  | **Frecuencia de la Actividad** | **Probabilidad** |
| Muy Baja | La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año | 20% |
| Baja | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año | 40% |
| Media | La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año | 60% |
| Alta | La actividad que conlleva el riesgo se ejecuta  mínimo 500 veces al año y máximo 5000 veces por año | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año | 100% |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 39.

#### **Impacto**: se definen los impactos económicos y reputacionales como las variables principales, cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Tabla 6 Criterios para definir el nivel de impacto

|  |  |  |
| --- | --- | --- |
|  | **Afectación Económica** | **Reputacional** |
| Leve 20% | Afectación menor a 130  SMLMV | El riesgo afecta la imagen de algún área de la organización. |
| Menor-40% | Entre 130 y 650 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 650 y 1300 SMLMV | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos. |
| Mayor 80% | Entre 1300 y 6500 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 6500 SMLMV | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país |

Fuente: Adaptado Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 40.

#### Para determinar el Impacto para los riesgos de corrupción**,** se mide según el efecto que pueda causar el hecho al cumplimiento de los fines de la entidad, bajo los niveles: Catastrófico, Mayor o Moderado, dado que estos riesgos siempre serán significativos.

#### De acuerdo con lo anterior, se deben responder las siguientes preguntas**:**

Tabla 7 Criterios para determinar impacto de corrupción

|  |  |  |  |
| --- | --- | --- | --- |
| **IMPACTO CORRUPCIÓN** | | | |
| **No.** | **SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...** | **RESPUESTA** | |
| **SI** | **NO** |
| 1 | ¿Afectar al grupo de funcionarios del proceso? |  |  |
| 2 | ¿Afectar el cumplimiento de metas y objetivos de la dependencia? |  |  |
| 3 | ¿Afectar el cumplimiento de misión de la Entidad? |  |  |
| 4 | ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad? |  |  |
| 5 | ¿Generar pérdida de confianza de la Entidad, afectando su reputación? |  |  |
| 6 | ¿Generar pérdida de recursos económicos? |  |  |
| 7 | ¿Afectar la generación de los productos o la prestación de servicios? |  |  |
| 8 | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos? |  |  |
| 9 | ¿Generar pérdida de información de la Entidad? |  |  |
| 10 | ¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente? |  |  |
| 11 | ¿Dar lugar a procesos sancionatorios? |  |  |
| 12 | ¿Dar lugar a procesos disciplinarios? |  |  |
| 13 | ¿Dar lugar a procesos fiscales? |  |  |
| 14 | ¿Dar lugar a procesos penales? |  |  |
| 15 | ¿Generar pérdida de credibilidad del sector? |  |  |
| **16** | **¿Ocasionar lesiones físicas o pérdida de vidas humanas?** |  |  |
| 17 | ¿Afectar la imagen regional? |  |  |
| 18 | ¿Afectar la imagen nacional? |  |  |
| 19 | ¿Generar daño ambiental? |  |  |
| **TOTAL, RESPUESTAS AFIRMATIVAS** | | **0** | |
| Responder afirmativamente de 1 a 5 pregunta(s) genera un impacto **Moderado**  Genera medianas consecuencias sobre la entidad  Responder afirmativamente de 6 a 11 preguntas genera un impacto **Mayor**  Genera altas consecuencias sobre la entidad.  Responder afirmativamente de 12 a 19 preguntas genera un impacto **Catastrófico**.  Genera consecuencias desastrosas para la entidad | | | |

Fuente: Adaptado Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 72.

Nota: Si la respuesta a la pregunta 16 es afirmativa, el riesgo inmediatamente se considera catastrófico. Por cada riesgo de corrupción identificado.

## Evaluación de riesgo inherente

El riesgo inherente se establece con la estimación de la probabilidad y el impacto que pueda causar la materialización del riesgo. Se debe ubicar en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo.

Tabla 8 Matriz de calor (niveles de severidad del riesgo)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Probabilidad** | **Mapa De Calor** | | | | |
| **Muy Alta (100%)** | Alto | Alto | Alto | Alto | Extremo |
| **Alta (80%)** | Moderado | Moderado | Alto | Alto | Extremo |
| **Media (60%)** | Moderado | Moderado | Moderado | Alto | Extremo |
| **Baja (40%)** | Bajo | Moderado | Moderado | Alto | Extremo |
| **Muy Baja (20%)** | Bajo | Bajo | Moderado | Alto | Extremo |
|  | **Leve (20%)** | **Menor (40%)** | **Moderado (60%)** | **Mayor (80%)** | **Catastrófico (100%)** |
|  | **Impacto** | | | | |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 42.

En el formato DESI-FM-018 Mapa de Riesgos de Proceso al seleccionar la probabilidad y el impacto de las listas desplegables, se realiza automáticamente la intersección, como resultado se obtiene el riesgo inherente.

Tabla 9 Riesgo Inherente

|  |  |  |
| --- | --- | --- |
| **CALIFICACIÓN DEL RIESGO** | | **EVALUACIÓN DEL RIESGO INHERENTE** |
| **PROBABILIDAD** | **IMPACTO** | **ZONA DE RIESGO** |
|  |  |  |

Fuente: Formato DESI-FM-018 Mapa de Riesgos.

## VALORACIÓN DE CONTROLES

## Definición y clasificación de controles:

Un control se define como la medida que permite reducir o mitigar el riesgo, los responsables de implementar y monitorear los controles son la primera línea del proceso y debe redactarse bajo la siguiente estructura:

* Responsable de ejecutar el control: identifica quién 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. (Verificar, Validar, Cotejar, Comparar y revisar entre otros)
* Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control. (periodicidad, cómo se realiza, evidencia y desviación)

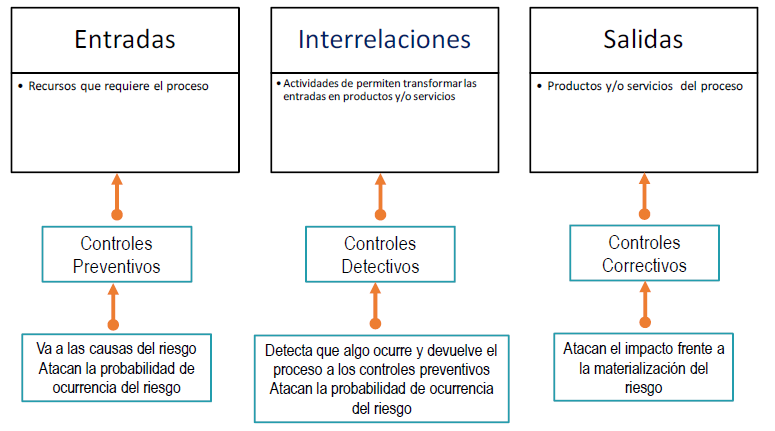
Los controles se tipifican de acuerdo a la etapa del proceso, por lo cual es necesario establecer su tipología con mayor precisión, así:

**Controles Preventivos:** 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

**Controles Defectivos:** 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.

Ilustración 6 Ciclo del proceso y las tipologías de controles



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 44.

Así mismo, se clasifican de acuerdo a cómo se implementan:

**Control manual: E**jecutados por personas.

**Control automático:** Ejecutados por un sistema.

## Análisis y evaluación de los controles

Se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización, asi:

Tabla 10 Criterios para la evaluación de los controles

| **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% |
| 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: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 46.

## EVALUACIÓN DE CONTROLES - RIESGO RESIDUAL:

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para identificar la efectividad de los controles se debe tener en cuenta que 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, ejemplo:

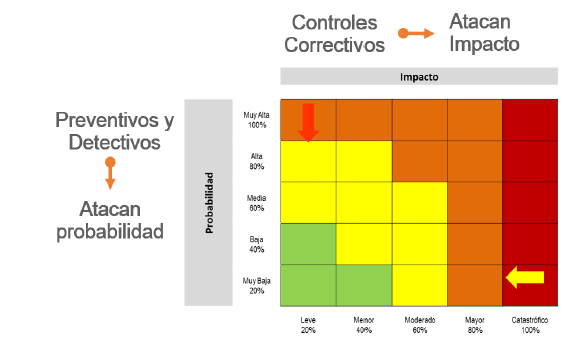
Tabla 11 Aplicación de controles para establecer el riesgo residual

| **Datos relacionados con la probabilidad e impacto inherentes** | | **Datos valoración de controles** | | **Cálculos requeridos** |
| --- | --- | --- | --- | --- |
| Probabilidad inherente | 60% | Valoración control 1 preventivo | 40% | 60%\* 40% = 24%  60% - 24% = **36%** |
| Valor probabilidad para aplicar 2º control | 36% | Valoración control 2 detectivo | 30% | 36%\* 30% = 10,8%  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 Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 49.

**Nota:** El fin de los atributos informativos es conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Ilustración 7 Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 47.

En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, por lo cual, no será posible su movimiento en la matriz para el impacto.

## TRATAMIENTO DE RIESGOS

Es la decisión que toma la primera línea de defensa frente al nivel del riesgo residual. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, puede ser aceptar, reducir o evitar, según el apetito del riesgo:

* **Zona de riesgo BAJA**: ACEPTAR el riesgo y se determina ASUMIR el mismo conociendo los efectos de su posible materialización. (Ningún riesgo de corrupción podrá ser aceptado)
* **Zona de riesgo** **MODERADA**: REDUCIR el riesgo, se establece plan de acción que MITIGUE el nivel de riesgo.
* **Zona de riesgo** **ALTA**: REDUCIR el riesgo, se establece plan de acción que MITIGUE el nivel de riesgo o REDUCIR el riesgo y se considera TRANSFERIR el riesgo tercerizando el proceso/actividad o trasladar el riesgo a través de seguros o pólizas.
* **Zona de riesgo EXTREMA**: REDUCIR el riesgo, se establece plan de acción que MITIGUE el nivel de riesgo o REDUCIR el riesgo y se determina TRANSFERIR el riesgo tercerizando el proceso/actividad o trasladar el riesgo a través de seguros o pólizas o EVITAR y se determina NO realizar la actividad que genera este riesgo.

Existen planes coadyuvantes para el tratamiento de riesgos tales, como:

## Plan de acción

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.

## Plan de contingencia

El Plan de contingencia, es determinado por los procesos, se registra en el mapa de riesgos y se aplica únicamente cuando un riesgo se materializa, debe documentar claramente cómo actuar ante una posible eventualidad.

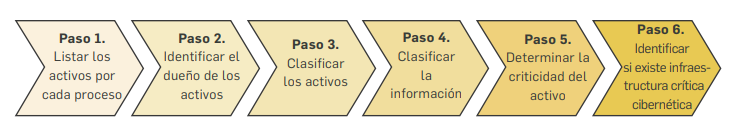
## RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

## Identificación de los activos de seguridad de la información

Un activo es cualquier elemento que tenga valor para la organización. Sin embargo, en el contexto de la seguridad digital, son activos elementos tales como: aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento[[3]](#footnote-4). Los procesos deben realizar la identificación de los activos de información y documentar el inventario de activos, así podrán saber lo que deben hacer para proteger y garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano.

La identificación y valoración de activos debe ser realizada por la **Primera Línea de Defensa – Líderes de Proceso**, en cada proceso donde aplique la gestión del riesgo de seguridad digital[[4]](#footnote-5).

Ilustración 8 Esquema Pasos para identificar los activos

Fuente: Adaptado Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 diciembre 2020. DAFP. pág. 80.

1. **Listar los activos por cada proceso:** En cada proceso deberán listarse los activos indicando algún consecutivo, nombre y descripción breve de cada uno.
2. **Identificar el dueño de los activos:** Cada uno de los activos identificados deberá tener un dueño designado (área/ dependencia), Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
3. **Clasificar los activos**: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros (ver tabla 12).

Tabla 12 Clasificación de Activos

| **CLASIFICACION**  **DE ACTIVOS** | **DESCRIPCION** |
| --- | --- |
| **Hardware** | Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información |
| **Información** | Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| **Componentes de red** | Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros |
| **Know-How - Servicios** | Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software) |
| **Software** | Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades |
| **Intangibles** | Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el goodwill, entre otros |
| **Personas** | Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades. |
| **Instalaciones** | Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa |

Fuente: Adaptado Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018

1. **Clasificar la información:** Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información

**CONFIDENCIALIDAD** se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Tabla 13 Clasificación de acuerdo con la confidencialidad

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

Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC pag16

**INTEGRIDAD**: se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

Tabla 14 Clasificación de acuerdo con la integridad

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

Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC pág. 17

**DISPONIBILIDAD:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

Tabla 15 Clasificación de acuerdo con la disponibilidad

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

Fuente: Guía para la Gestión y Clasificación de Activos de Información MINTIC pág. 18

1. **Determinar la criticidad del activo: se** debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

Tabla 16 Niveles de clasificación

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

**Fuente**: Guía para la Gestión y Clasificación de Activos de Información MINTIC pág. 13

## Identificación riesgos de seguridad de la información

Para la identificación de riesgos de seguridad de la información, es necesario contar con la matriz de activos de información consolidada, donde el activo de información se clasifique de acuerdo con los atributos de confidencialidad, integridad y disponibilidad y que su evaluación del nivel de criticidad sea **ALTO.**

las actividades de esta etapa deben ser enfocadas a los riesgos potenciales que ocasionen una incidencia negativa sobre el desarrollo de los objetivos de los procesos.

Los tipos que se pueden identificar son los siguientes tres (3) riesgos inherentes de seguridad de la información:

* Pérdida de la confidencialidad
* Pérdida de la integridad
* Pérdida de la disponibilidad

Para el riesgo **identificado 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.

## Identificación de amenazas y vulnerabilidades

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

Se deben identificar las amenazas de los activos: en la siguiente tabla se listan las amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

Tabla 17 Amenazas más comunes

| **TIPO** | **AMENAZA** |
| --- | --- |
| **Daño físico** | Fuego |
| Agua |
| Contaminación |
| Accidente Importante |
| Destrucción del equipo o medios |
| Polvo, corrosión, congelamiento |
| **Eventos naturales** | Fenómenos climáticos |
| Fenómenos sísmicos |
| Fenómenos volcánicos |
| Fenómenos meteorológicos |
| Inundación |
| **Perdida de los servicios esenciales** | Fallas en el sistema de suministro de agua o aire acondicionado |
| Perdida de suministro de energía |
| Falla en equipo de telecomunicaciones |
| **Perturbación debida a la radiación** | Radiación electromagnética |
| Radiación térmica |
| Impulsos electromagnéticos |
| **Compromiso de la información** | Interceptación de señales de interferencia comprometida |
| Espionaje remoto |
| Escucha encubierta |
| Hurto de medios o documentos |
| Hurto de equipo |
| Recuperación de medios reciclados o desechados |
| Divulgación |
| Datos provenientes de fuentes no confiables |
| Manipulación con hardware |
| Manipulación con software |
| Detección de la posición |
| **Fallas técnicas** | Fallas del equipo |
| Mal funcionamiento del equipo |
| Saturación del sistema de información |
| Mal funcionamiento del software |
| Incumplimiento en el mantenimiento del sistema de información. |
| **Acciones no autorizadas** | Uso no autorizado del equipo |
| Copia fraudulenta del software |
| Uso de software falso o copiado |
| Corrupción de los datos |
| Procesamiento ilegal de datos |
| **Compromiso de las funciones** | Error en el uso |
| Abuso de derechos |
| Falsificación de derechos |
| Negación de acciones |
| Incumplimiento en la disponibilidad del personal |

Fuente: Adaptado Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018

Se deben identificar las vulnerabilidades (debilidades) en la siguiente tabla se lista más comunes:

Tabla 18 Vulnerabilidades más comunes

| **Tipo** | **Vulnerabilidades** |
| --- | --- |
| **Hardware** | Mantenimiento insuficiente |
| Ausencia de esquemas de reemplazo periódico |
| Sensibilidad a la radiación electromagnética |
| Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad) |
| Almacenamiento sin protección |
| Falta de cuidado en la disposición final |
| Copia no controlada |
| **Software** | Ausencia o insuficiencia de pruebas de software |
| Ausencia de terminación de sesión |
| Ausencia de registros de auditoría |
| Asignación errada de los derechos de acceso |
| Interfaz de usuario compleja |
| Ausencia de documentación |
| Fechas incorrectas |
| Ausencia de mecanismos de identificación y autenticación de usuarios |
| Contraseñas sin protección |
| Software nuevo o inmaduro |
| **Red** | Ausencia de pruebas de envío o recepción de mensajes |
| Líneas de comunicación sin protección |
| Conexión deficiente de cableado |
| Tráfico sensible sin protección |
| Punto único de falla |
| **Personal** | Ausencia del personal |
| Entrenamiento insuficiente |
| Falta de conciencia en seguridad |
| Ausencia de políticas de uso aceptable |
| Trabajo no supervisado de personal externo o de limpieza |
| **Lugar** | Uso inadecuado de los controles de acceso al edificio |
| Áreas susceptibles a inundación |
| Red eléctrica inestable |
| Ausencia de protección en puertas o ventanas |
| **Organización** | Ausencia de procedimiento de registro/retiro de usuarios |
| Ausencia de proceso para supervisión de derechos de acceso |

Fuente: Adaptado Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018

Tabla 19 Ejemplos de vulnerabilidades y amenazas

| **TIPO DE ACTIVO** | **EJEMPLOS DE VULNERABILIDADES** | **EJEMPLOS DE AMENAZAS** |
| --- | --- | --- |
| **HARDWARE** | Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento | Incumplimiento en el mantenimiento del sistema de información. |
| Ausencia de esquemas de reemplazo periódico | Destrucción de equipos o medios. |
| Susceptibilidad a la humedad, el polvo y la suciedad | Polvo, corrosión y congelamiento |
| Sensibilidad a la radiación electromagnética | Radiación electromagnética |
| Ausencia de un eficiente control de cambios en la configuración | Error en el uso |
| Susceptibilidad a las variaciones de voltaje | Pérdida del suministro de energía |
| Susceptibilidad a las variaciones de temperatura | Fenómenos meteorológicos |
| Almacenamiento sin protección | Hurtos medios o documentos. |
| Falta de cuidado en la disposición final | Hurtos medios o documentos. |
| Copia no controlada | Hurtos medios o documentos. |
| **SOFTWARE** | Ausencia o insuficiencia de pruebas de software | Abuso de los derechos |
| Defectos bien conocidos en el software | Abuso de los derechos |
| Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo | Abuso de los derechos |
| Disposición o reutilización de los medios de almacenamiento sin borrado adecuado | Abuso de los derechos |
| Ausencias de pistas de auditoria | Abuso de los derechos |
| Asignación errada de los derechos de acceso | Abuso de los derechos |
| Software ampliamente distribuido | Corrupción de datos |
| En términos de tiempo utilización de datos errados en los programas de aplicación | Corrupción de datos |
| Interfaz de usuario compleja | Error en el uso |
| Ausencia de documentación | Error en el uso |
| Configuración incorrecta de parámetros | Error en el uso |
| Fechas incorrectas | Error en el uso |
| Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario | Falsificación de derechos |
| Tablas de contraseñas sin protección | Falsificación de derechos |
| Gestión deficiente de las contraseñas | Falsificación de derechos |
| Habilitación de servicios innecesarios | Procesamiento ilegal de datos |
| Software nuevo o inmaduro | Mal funcionamiento del software |
| Especificaciones incompletas o no claras para los desarrolladores | Mal funcionamiento del software |
| Ausencia de control de cambios eficaz | Mal funcionamiento del software |
| Descarga y uso no controlado de software | Manipulación con software |
| Ausencia de copias de respaldo | Manipulación con software |
| Ausencia de protección física de la edificación, puertas y ventanas | Hurto de medios o documentos |
| Fallas en la producción de informes de gestión | Uso no autorizado del equipo |
| Ausencia de pruebas de envío o recepción de mensajes | Negación de acciones |
| Líneas de comunicación sin protección | Escucha encubierta |
| Tráfico sensible sin protección | Escucha encubierta |
| Conexión deficiente de los cables | Fallas del equipo de telecomunicaciones |
| Punto único de fallas | Fallas del equipo de telecomunicaciones |
| Ausencia de identificación y autentificación de emisor y receptor | Falsificación de derechos |
| Arquitectura insegura de la red | Espionaje remoto |
| Transferencia de contraseñas en claro | Espionaje remoto |
| Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) | Saturación del sistema de información |
| Conexiones de red pública sin protección | Uso no autorizado del equipo |
| Ausencia del personal | Incumplimiento en la disponibilidad del personal |
| Procedimientos inadecuados de contratación | Destrucción de equipos y medios |
| Entrenamiento insuficiente en seguridad | Error en el uso |
| Uso incorrecto de software y hardware | Error en el uso |
| Falta de conciencia acerca de la seguridad | Error en el uso |
| Ausencia de mecanismos de monitoreo | Procesamiento ilegal de los datos |
| Trabajo no supervisado del personal externo o de limpieza | Hurto de medios o documentos. |
| Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería | Uso no autorizado del equipo |
| **LUGAR** | Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos |  |
| Ubicación en área susceptible de inundación |  |
| Red energética inestable |  |
| Ausencia de protección física de la edificación (Puertas y ventanas) |  |
| **ORGANIZACION** | Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso de los derechos |
| Ausencia de proceso formal para la revisión de los derechos de acceso | Abuso de los derechos |
| Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad) | Abuso de los derechos |
| Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información | Abuso de los derechos |
| Ausencia de auditorias | Abuso de los derechos |
| Ausencia de procedimientos de identificación y valoración de riesgos | Abuso de los derechos |
| Ausencia de reportes de fallas en los registros de | Abuso de los derechos |
| administradores y operadores |  |
| Respuesta inadecuada de mantenimiento del servicio | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de acuerdos de nivel de servicio o insuficiencia de estos | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de procedimientos de control de cambios | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de procedimiento formal para la documentación del MSPI | Corrupción de datos |
| Ausencia de procedimiento formal para la supervisión del registro del MSPI | Corrupción de datos |
| Ausencia de procedimiento formal para la autorización de la información disponible al público | Datos provenientes de fuentes no confiables |
| Ausencia de asignación adecuada de responsabilidades en seguridad de la información | Negación de acciones |
| Ausencia de planes de continuidad | Falla del equipo |
| Ausencia de políticas sobre el uso de correo electrónico | Error en el uso |
| Ausencia de procedimientos para introducción del software en los sistemas operativos | Error en el uso |
| Ausencia de registros en bitácoras | Error en el uso |
| Ausencia de procedimientos para el manejo de información clasificada | Error en el uso |
| Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos | Error en el uso |
| Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información | Hurto de equipo |
| Ausencia de política formal sobre la utilización de computadores portátiles | Hurto de equipo |
| Ausencia de control de los activos que se encuentran fuera de las instalaciones | Hurto de equipo |
| Ausencia de política sobre limpieza de escritorio y pantalla | Hurto de medios o documentos |
| Ausencia de autorización de los recursos de procesamiento de información | Hurto de medios o documentos |
| Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad | Hurto de medios o documentos |
| Ausencia de revisiones regulares por parte de la gerencia | Uso no autorizado de equipo |
| Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad | Uso no autorizado de equipo |
| Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales. | Uso de software falsificado o copiado |

**Fuente:** ISO 27005

## Controles asociados a la seguridad de la información

Para mitigar/tratar los riesgos de seguridad de la información emplear 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.

# MONITOREO Y SEGUIMIENTO

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos para asegurar el logro de los objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. Se realiza el seguimiento y monitoreo así:

Primera línea

Se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla, mitiga los riesgos y reporta sus seguimientos a la 2ª línea.

Por lo que remitirán **cuatrimestralmente** a la Oficina Asesora de Planeación en el formato DESI-FM-019 Monitoreo al Mapa de Riesgos por Proceso diligenciado.

Segunda línea

Monitorea la ejecución de los controles establecidos por la 1ª línea de defensa revisando que sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de actividades de control establecidas en el Plan de Acción del mapa de riesgo, verificación se mantenga un enfoque basado en riesgos.

La segunda línea de defensa de los riesgos de seguridadde la información está a cargo de la mesa de activos, conformada por profesionales designados de la Secretaría General, Oficina Asesora Jurídica y la Oficina Asesora de Planeación.

Tercera línea

Evalúa de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos y los que inadecuadamente son cubiertos por la 2ª línea de defensa en las auditorias programadas en el Plan Anual de Auditorías.

Evalúa a través de las auditorías internas, las actividades adelantadas por la segunda línea de defensa frente al análisis de contexto y de identificación del riesgo que deben aplicar los procesos para su identificación de riesgos.

# AJUSTES Y MODIFICACIONES:

Se podrán llevar a cabo los ajustes orientados a mejorar y las modificaciones necesarias de los mapas de riesgos de los procesos. En este caso, deberán remitirse a la Oficina Asesora de Planeación a través del Sistema de Correspondencia de la entidad, para el cargue en el punto de uso de la unidad SISGESTIÓN en la versión siguiente de la vigencia.

De acuerdo con el monitoreo y seguimiento realizado es importante revisar al final de cada vigencia si los mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo. Para poder determinarlo, se analizará si no se han presentado hechos significativos como son:

* Cambios importantes en el entorno que puedan generar nuevos riesgos.
* Riesgos materializados
* Observaciones o hallazgos por parte de la Oficina de Control Interno o bien por parte de un ente de control, respecto a la idoneidad y efectividad de los controles.

Para la eliminación de cualquier riesgo el líder del proceso debe presentar una justificación y ésta deberá ser aprobada por el Comité Institucional de Gestión y Desempeño.

# LINEAMIENTOS PARA EL MANEJO DE RIESGOS MATERIALIZADOS

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad. Cuando se materializa un riesgo, es necesario realizar los ajustes necesarios con acciones tales como:

1. Aplicar el Plan de contingencia, que se encuentra en el mapa de riesgos del proceso.
2. Informar a las autoridades de la ocurrencia del hecho de corrupción.
3. Volver a realizar la valoración del riesgo (causas, probabilidad, impacto)
4. Revisar controles y ajustarlos
5. Evaluar si se necesitan nuevos controles.
6. Realizar un monitoreo permanente.

En caso de que el riesgo no se hubiese identificado, el proceso debe formularlo y dar el tratamiento correspondiente de acuerdo con la presente política.

La Oficina Asesora de Planeación, documenta una base histórica de riesgos materializados, según el reporte de los procesos y presenta los resultados al CIGD.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por**  **Líderes (Estratégico u Operativo) del Proceso:** | **Aprobado por:** |
| **MARIA NATALIA NORATO**  **Contratista OAP -DESI**  **PAULA LIZZETTE RUIZ**  **Contratista OAP -DESI** | Firma: | Firma: |
| **Acompañamiento Asesor OAP:** |
| **JULIO CESAR GUAPACHA**  **Contratista OAP- DESI** |
| **DIANA MARCELA REYES TOLEDO**  Jefe Oficina Asesora de Planeación | **DIANA MARCELA REYES TOLEDO**  Jefe Oficina Asesora de Planeación |

**CONTROL DE CAMBIOS:**

| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO** |
| --- | --- | --- | --- |
| 1 | Se estructura política de riesgo teniendo en cuenta la metodología del Departamento Administrativo de la Gestión Pública DAFP, y el cronograma establecido en el plan anticorrupción y de atención al ciudadano. | ABRIL 2016 | Jefe Oficina Asesora de Planeación |
| 2 | Se ajustó la metodología según lineamientos normativos de Departamento Administrativo de la Gestión Pública DAFP y la Presidencia de la Republica. Se actualiza normatividad MECI:2014 | DICIEMBRE 2016 | Martha Patricia Aguilar Copete |
| 3 | Se ajustó la política, la metodología de identificación evaluación y tratamiento de riesgos conforme a la normatividad vigente | OCTUBRE  2017 | Jefe Oficina Asesora de Planeación |
| 4 | Se actualiza la codificación del documento conforme al nuevo mapa de procesos. | ENERO 2019 | Jefe Oficina Asesora de Planeación |
| 5 | Se actualizo la política de administración de riesgo y su metodología de acuerdo con la Guía para la administración del riesgo de gestión, Corrupción y seguridad Digital y el Diseño de controles en Entidades Públicas agosto de 2018 | ENERO 2019 | Jefe Oficina Asesora de Planeación |
| 6 | Se agregan criterios adicionales para el proceso de gestión del laboratorio en los Criterios para calificar el impacto de riesgos de gestión y se ajustan los lineamientos en caso de materializarse un riesgo | SEPTIEMBRE  2019 | Jefe Oficina Asesora de Planeación |
| 7 | Se ajustó el documento para alinear política a los Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas e incorporar la EGTI-PL-002-V1 Plan de tratamiento de riesgo y EGTI-DI-013V1 política de Seguridad para la gestión de Riesgos | JUNIO 2020 | Martha Patricia Aguilar Copete  Jefe Oficina Asesora de Planeación |
| 8 | Se incorporó la identificación del riesgo de corrupción - soborno | SEPTIEMBRE  2020 | Jefe Oficina Asesora de Planeación |
| 9 | Se ajustó el documento para alinear política a la guía para la administración del riesgo y el diseño de controles en entidades públicas v5 | NOVIEMBRE  2021 | Jefe Oficina Asesora de Planeación |
| 10 | Se ajustó la redacción de la declaración de la política, se ajustaron los roles y responsabilidades de conformidad al manual operativo del Modelo Integrado de Planeación y Gestión – MIPG vigente, se ajustó un objetivo estratégico y la periodicidad del monitoreo para realizarse cuatrimestralmente.  Mediante Comité extraordinario de Coordinación de Control Interno 006 2022 se aprueba la presente versión del Manual de la Política de Administración del riesgo. | NOVIEMBRE  2022 | Jefe Oficina Asesora de Planeación |

1. Intosai: Guía para las normas de control interno del sector público http://www.Intosai.org [↑](#footnote-ref-2)
2. Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, Corrupción y seguridad digital versión 4 [↑](#footnote-ref-3)
3. Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas. [↑](#footnote-ref-4)
4. Ibídem. [↑](#footnote-ref-5)