# POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO ASOCIACIÓN AEROPUERTO DEL CAFÉ AEROCAFÉ

SEPTIEMBRE DE 2021

AEROPUERTO DEL CAFÉ
Creamos oportunidades

## Contenido

*"La Asociación Aeropuerto del Café AEROCAFÉ define la política de administración del riesgo como la expresión del compromiso frente a la administración adecuada de los riesgos de gestión, corrupción y de seguridad digital, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, a través de la definición de acciones de control detectivas y preventivas oportunas, con el fin de mitigar las posibles consecuencias para mantener los niveles de riesgo en aceptables".*

## INTRODUCCIÓN

Asociación Aeropuerto del Café AEROCAFÉ establece como marco de referencia el Modelo Integrado de Planeación y gestión MIPG para dirigir, planear, ejecutar, realizar seguimiento, evaluar y controlar las actividades que se realizan, a través de las dimensiones de Direccionamiento Estratégico y Control Interno, como eje fundamental el análisis del contexto organizacional interno y externo, la planeación institucional, los objetivos institucionales y las políticas sectoriales y específicas definidas por el gobierno nacional, regional y el modelo de operación por procesos.

Por lo anterior, la entidad define los lineamientos para la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales, tomando como referencia las orientaciones del MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno MECI, las disposiciones de la Guía para la Administración del Riesgo del DAFP y el Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital.

## OBJETIVO

Definir el marco general para la gestión del riesgo en todos los niveles de la entidad, así como los potenciales eventos de pérdida de continuidad del negocio, mediante la identificación y tratamiento de los riesgos de gestión, corrupción y seguridad digital que afecten el cumplimiento de la misionalidad y el logro de los objetivos institucionales teniendo en cuenta el contexto interno y externo, el modelo de operación por procesos, los niveles de aceptabilidad del riesgo y las responsabilidades para su reporte, monitoreo y seguimiento a partir de las líneas de defensa definidas por la entidad.

## ALCANCE DE LA POLÍTICA

La política para la administración de los riesgos de gestión, corrupción y seguridad digital es aplicable a todos los proyectos y acciones de la entidad ejecutadas por el talento humano y todos aquellos colaboradores que prestan servicios a través de las diferentes modalidades contractuales a la Asociación Aeropuerto del Café durante el ejercicio de sus funciones

## TÉRMINOS Y DEFINICIONES

**ACEPTACIÓN DEL RIESGO**: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

**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 institución para funcionar en el entorno digital.

**AMENAZAS:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

**ANÁLISIS DE RIESGO:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo.

**APETITO DEL 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 del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

**CAUSA:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

**CGDI:** Comité de Gestión y Desempeño Institucional.

**CICCI**: Comité Institucional de Coordinación de Control Interno.

**COMPARTIR EL RIESGO:** Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

**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.

**CONTEXTO EXTERNO**: Ambiente externo en el cual la Entidad busca alcanzar sus objetivos que puede ser: políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios.

**CONTEXTO INTERNO:** Ambiente interno en el cual la Entidad busca alcanzar sus objetivos, el cual puede ser: financieros, personal, procesos, tecnología, estratégicos, comunicación interna.

**CONTINGENCIA:** Posible evento futuro, condición o eventualidad Continuidad: Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.

**CONTINUIDAD:** Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.

**CONTROL:** Medida que modifica al riesgo (procesos, políticas, dispositivos, practicas u otras acciones.

**CRISIS (Emergencia):** Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

**FACTORES DE RIESGO:** Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgos o tienden a aumentar la exposición, pueden ser internos o externos de la entidad.

**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.

**IDENTIFICACIÓN DEL RIESGO:** Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

**IMPACTO:** Se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

**MAPA DE RIESGOS:** Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

**MIPG:** Modelo Integrado de Planeación y Gestión.

**MEC**I: Modelo Estándar de Control Interno.

**NIVEL DE ACEPTACIÓN DEL RIESGO:** Son los criterios de aceptación de riesgos establecidos que se emplean durante la etapa de evaluación de riesgos.

**PROBABILIDAD:** Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

**RIESGO**: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

**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 CUMPLIMIENTO:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

**RIESGO DE GESTIÓN:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

**RIESGO DE IMAGEN:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

**RIESGO DE SEGURIDAD DIGITAL:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

**RIESGO DE TECNOLOGÍA:** Están relacionados con la capacidad tecnológica de la organización para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

**RIESGO ESTRATÉGICO:** Son las pérdidas ocasionadas por las definiciones estratégicas inadecuadas, errores en el diseño de planes, programas, estructura, integración del modelo de operación con el direccionamiento estratégico, asignación de recursos, estilo de dirección, ineficiencia en la adaptación a los cambios del sector, entre otros.

**RIESGO INHERENTE:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

**RIESGO FINANCIERO:** Se relacionan con el manejo de los recursos de entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

**RIESGO OPERACIONAL:** Es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la entidad por fallas en procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos.

**RIESGO RESIDUAL:** nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

**SIG:** Sistema Integrado de Gestión.

**TOLERANCIA AL RIESGO:** Preparación de la organización o de la parte involucrada para soportar el riesgo después del tratamiento del mismo con el fin de lograr sus objetivos.

**TRATAMIENTO DEL RIESGO:** Consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

**VALORACIÓN DEL RIESGO:** Busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.

**VULNERABILIDAD**: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

## RESPONSABILIDADES

La responsabilidad se encuentra definida a través de las Líneas de defensa y AEROCAFÉ las acoge según la siguiente tabla:

| LÍNEAS DE DEFENSA | RESPONSABLE | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|
| **Línea Estratégica** | Consejo Directivo<br>Comité de Gestión y Desempeño Institucional<br>Comité Institucional de Coordinación de Control Interno | • Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control.<br>• Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la Asociación Aeropuerto del Café AEROCAFÉ y capacidades para prestar servicios.<br>• Definir y aprobar la política para la administración del riesgo.<br>• Garantizar el cumplimiento de los planes de la entidad. |
| **Primera Línea** | Líderes de Proceso | • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.<br>• Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión.<br>• Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.<br>• Revisar de acuerdo con su competencia y alcance la documentación de continuidad de negocio.<br>• Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio.<br>• Informar al responsable de planeación o quien haga sus veces (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo.<br>• Reportar en el SIG los avances y evidencias de la gestión de los riesgos |

| LÍNEAS DE DEFENSA | RESPONSABLE | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|
| | | dentro de los plazos establecidos. |
| **Segunda Línea** | Responsable de planeación o quien haga sus veces | • Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el CGDI.<br>• Actualizar la documentación que soporta la estrategia de continuidad de negocio.<br>• Presentar al CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad.<br>• Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo.<br>• Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos.<br>• Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.<br>• Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.<br>• Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.<br>• Orientar y hacer seguimiento a las pruebas del plan de continuidad de |

| LÍNEAS DE DEFENSA | RESPONSABLE | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|
| | | negocio.<br>• Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI.<br>• Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. |
| **Segunda Línea** | Área Técnica<br>Director Jurídico<br>Coordinador Administrativo y Financiero | • Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo.<br>• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.<br>• Realizar el seguimiento al mapa de riesgos de su proceso.<br>• Reportar en el módulo de riesgos del SIG o delegar a un profesional de la dependencia o grupo a su cargo, el registro de los avances en la gestión del riesgo.<br>• Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo.<br>• Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad.<br>• Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia.<br>• Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. |

| LÍNEAS DE DEFENSA | RESPONSABLE | RESPONSABILIDAD FRENTE AL RIESGO |
|---|---|---|
| | | • Participar en las pruebas del plan de continuidad de negocio y en la implementación.<br>• El director jurídico el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico.<br>• Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. |
| **Tercera Línea** | Jefe de Control Interno | • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.<br>• Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.<br>• Asesorar a la primera línea de defensa de forma coordinada con el responsable de planeación o quien haga sus veces, en la identificación de los riesgos y diseño de controles.<br>• Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI.<br>• Recomendar mejoras a la política de operación para la administración del riesgo |

Igualmente, el responsable de planeación o quien haga sus veces realizarán las siguientes actividades durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta SIG para la gestión del riesgo.
- Liderar las mesas de trabajo de identificación del riesgo.
- Liderar las mesas de trabajo para determinación del análisis de impacto del negocio, documentación de los escenarios de riesgo y plan de continuidad de negocio institucional.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.
- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SIG.
- Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo.
- Documentar los escenarios de perdida de continuidad de negocio que se utilizan para el desarrollo y prueba del plan de continuidad de negocio.
- Presentar la propuesta para aprobación del líder del proceso.
- Una vez aprobado, comunicar al líder del proceso los resultados de las mesas de identificación y recordar la importancia de socializarlos al interior de su dependencia.
- Revisar que el cargue de información en el SIG esté acorde con lo aprobado.
- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos altos, extremos y de corrupción.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.

## ESCENARIOS DE PÉRDIDA DE CONTINUIDAD DEL NEGOCIO

Los escenarios de riesgo pertenecen a descripciones de situaciones que agrupa la ocurrencia de uno o más riesgos que generan la pérdida de continuidad en las actividades institucionales.

Al presentarse los eventos que materializan uno o más de los escenarios de continuidad de negocio la entidad valora las características de la emergencia para autorizar la aceleración del plan de continuidad, asignar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor. Una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en el plan de continuidad de negocio para dar respuesta a la misma.

La Asociación Aeropuerto del Café AEROCAFÉ adopta el siguiente conjunto de escenarios de riesgo para el diseño de la estrategia de continuidad de negocio.

| ESCENARIO | DESCRIPCIÓN |
|---|---|
| **Emergencia Social** | Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto. |
| **Colapso de infraestructura física** | Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor |
| **Desastre Tecnológico** | Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos |
| **Crisis Financiera** | Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos |
| **Emergencia sanitaria** | Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del estado. |

## ETAPAS PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento.

## CONTEXTO

A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar en cada vigencia, se analiza el entorno estratégico de La Asociación Aeropuerto del Café AEROCAFÉ a partir de los siguientes factores internos, externos y de proceso, para el adecuado análisis de las causas del riesgo y gestión del mismo.

| CONTEXTO | | |
|---|---|---|
| **CONTEXTO EXTERNO** | Económicos y Financieros | Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. |
| | Políticos | Cambios de gobierno, legislación, políticas públicas, regulación |
| | Sociales y culturales | Demografía, responsabilidad social, orden público |
| | Tecnológicos | Avances e tecnología, acceso a sistemas de información externos, gobierno en línea |
| | Ambientales | Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible |
| | Legales y reglamentarios | Normatividad externa (Leyes, decretos, ordenanzas y acuerdos) |
| | Comunicación externa | Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad |
| **CONTEXTO INTERNO** | Financieros | Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada |
| | Personal | Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional |

| CONTEXTO | | |
|---|---|---|
| | Procesos | Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento |
| | Tecnología | Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información |
| | Estratégicos | Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo |
| | Comunicación interna | Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones |
| **CONTEXTO INTERNO DEL PROCESO** | Diseño del proceso | Claridad en la descripción del alcance y objetivo del proceso |
| | Interacciones con otros procesos | Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes |
| | Transversalidad | Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad |
| | Procedimientos asociados | Pertinencia en los procedimientos que desarrollan los procesos |
| | Responsables del proceso | Grado de autoridad y responsabilidad de los funcionarios frente al proceso |
| | Comunicación entre los procesos | Efectividad en los flujos de información determinados en la interacción de los procesos |
| | Activos de seguridad digital del proceso | Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano |

## IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO

La identificación del riesgo se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. A partir de este contexto se identifica el riesgo, el cual estará asociado a

aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del Proceso.

Para ello se formulan las siguientes preguntas clave:


## CORRUPCIÓN

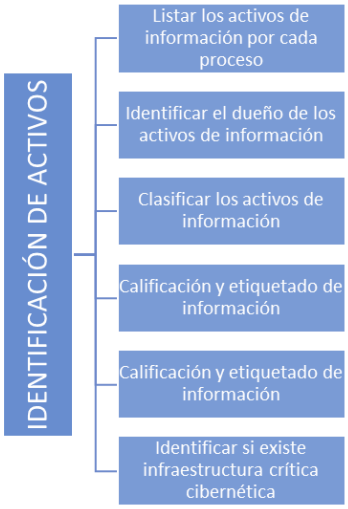
Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. “Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos”
(Conpes No. 167 de 2013).


## SEGURIDAD DIGITAL

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información dentro del proceso:

“Integridad, confidencialidad o disponibilidad”

**Solo existen tres (3) tipos de riesgos**: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice. Para el riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.




## NIVELES DE CALIFICACIÓN PROBABILIDAD E IMPACTO

Consiste en 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).

## PROBABILIDAD RIESGOS DE GESTIÓN, CORRUPCIÓN, SEGURIDAD DIGITAL

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad

implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

| CRITERIOS PARA CALIFICAR LA PROBABILIDAD | | | |
|---|---|---|---|
| **DESCRIPTOR** | **DESCRIPCIÓN** | **FRECUENCIA** | **NIVEL** |
| **RARA VEZ** | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales) | No se ha presentado en los últimos 5 años. | 1 |
| **IMPROBABLE** | El evento puede ocurrir en algún momento | Al menos 1 vez en los últimos 5 años. | 2 |
| **POSIBLE** | El evento podrá ocurrir en algún momento. | Al menos 1 vez en los últimos 2 años | 3 |
| **PROBABLE** | Es viable que el evento ocurra en la mayoría de las circunstancias | Al menos 1 vez en el último año | 4 |
| **CASI SEGURO** | Se espera que el evento ocurra en la mayoría de las circunstancias | Más de 1 vez al año | 5 |

## TABLAS CALIFICACIÓN IMPACTO

Las tablas de calificación del Impacto definidas para los Riesgos de Gestión, Corrupción y Seguridad Digital se definen así:

## MEDICIÓN DE IMPACTO RIESGOS DE GESTIÓN

| PROBABILIDAD | | IMPACTO | | |
|---|---|---|---|---|
| **CATEGORÍA** | **DESCRIPCIÓN** | **CATEGORÍA** | **DESCRPCIÓN CUANTITATIVA** | **DESCRIPCIÓN CUALITATIVA** |
| **NIVEL 5. CASI SEGURO** | Se espera que el evento ocurra en la mayoría de las circunstancias - Más de 1 vez al año | **NIVEL 5. CATASTRÓFICO** | • Impacto que afecte la ejecución presupuestal en un valor igual o superior al 50%<br>• Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o superior al 50%<br>• Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o superior al 50%<br>• Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o superior al 50% del presupuesto general de la entidad | • Interrupción de las operaciones de la Entidad por más de cinco (5) días.<br>• Intervención por parte de un ente de control u otro ente regulador.<br>• Pérdida de Información crítica para la entidad que no se puede recuperar.<br>• Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.<br>• Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados |
| **NIVEL 4. PROBABLE** | Es viable que el evento ocurra en la mayoría de las circunstancias - Al menos 1 vez en el último año | **NIVEL 4. MAYOR** | • Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 20% e inferior al 50%<br>• Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 20% e inferior al 50% | • Interrupción de las operaciones de la Entidad por más de dos (2) días.<br>• Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.<br>• Sanción por parte del ente de |

| PROBABILIDAD | | IMPACTO | | |
|---|---|---|---|---|
| CATEGORÍA | DESCRIPCIÓN | CATEGORÍA | DESCRPCIÓN CUANTITATIVA | DESCRIPCIÓN CUALITATIVA |
| | | | • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 20% e inferior al 50%<br>• Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 20% e inferior al 50% del presupuesto general de la entidad. | control u otro ente regulador.<br>• Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.<br>• Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadano |
| **NIVEL 3. POSIBLE** | El evento podrá ocurrir en algún momento - Al menos 1 vez en los últimos 2 años | **NIVEL 3. MODERADO** | • Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 10% y menor al 20%<br>• Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 10% y menor al 20%<br>• Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 10% y menor al 20%<br>• Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 10% y menor al 20%del presupuesto general de la entidad. | • Interrupción de las operaciones de la Entidad por un (1) día.<br>• Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.<br>• Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.<br>• Reproceso de actividades y aumento de carga operativa<br>• Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.<br>• Investigaciones penales, fiscales |

| PROBABILIDAD | | IMPACTO | | |
|---|---|---|---|---|
| CATEGORÍA | DESCRIPCIÓN | CATEGORÍA | DESCRPCIÓN CUANTITATIVA | DESCRIPCIÓN CUALITATIVA |
| | | | | o disciplinarias. |
| **NIVEL 2. IMPROBABLE** | El evento puede ocurrir en algún momento - Al menos 1 vez en los últimos 5 años | **NIVEL 2. MENOR** | • Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 1% y menor al 10%<br>• Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 1% y menor al 10%<br>• Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 1% y menor al 10%<br>• Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤1%del presupuesto general de la entidad. | • Interrupción de las operaciones de la Entidad por algunas horas.<br>• Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.<br>• Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. |
| **NIVEL 1. RARA VEZ** | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).<br><br>No se ha presentado en los últimos 5 años | **NIVEL 1. INSIGNIFICANTE** | • Impacto que afecte la ejecución presupuestal en un valor menor al 1%<br>• Pérdida de cobertura en la prestación de los servicios de la entidad ≤1%.<br>• Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor al 1%<br>• Pago de sanciones económicas por incumplimiento en la normatividad | • No hay interrupción de las operaciones de la entidad.<br>• No se generan sanciones económicas o administrativas.<br>• No se afecta la imagen institucional de forma significativa. |

| PROBABILIDAD | | IMPACTO | | |
|---|---|---|---|---|
| CATEGORÍA | DESCRIPCIÓN | CATEGORÍA | DESCRPCIÓN CUANTITATIVA | DESCRIPCIÓN CUALITATIVA |
| | | | aplicable ante un ente regulador, las cuales afectan en un valor menor al 1% del presupuesto general de la entidad. | |

## MEDICIÓN DE IMPACTO RIESGOS DE CORRUPCIÓN

La medición del impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

| MEDICIÓN DE IMPACTO RIESGOS DE CORRUPCIÓN | | | |
|---|---|---|---|
| **DESCRIPTOR** | **DESCRIPCIÓN** | **NIVEL** | **RESPUESTAS AFIRMATIVAS** |
| **MODERADO** | Afectación parcial al proceso y a la dependencia. Genera mediana consecuencia para la entidad. | 5 | 1-5 |
| **MAYOR** | Impacto negativo en la entidad. Genera altas consecuencias para la entidad. | 10 | 6-11 |
| **CATASTRÓFICO** | Consecuencias desastrosas sobre el sector. Genera consecuencias desastrosas para la entidad. | 20 | 12-19 |

| No. | PREGUNTA ¿SI EL RIESGO 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 misión del sector al cual pertenece la entidad? | | |
| 5 | ¿Generar pérdida de confianza de la entidad, afectando su reputación? | | |
| 6 | ¿Generar perdida de recursos económicos? | | |
| 7 | ¿Afectar la generación de los productos o la prestación de servicios? | | |

| No. | PREGUNTA<br>¿SI EL RIESGO SE MATERIALIZA PODRÍA? | RESPUESTA<br>SI | <br>NO |
|---|---|---|---|
| 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 perdida 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 les iones físicas o pérdida de vidas humanas? | | |
| 17 | ¿Afectar la imagen regional? | | |
| 18 | ¿Afectar la imagen nacional? | | |
| 19 | ¿Generar daño ambiental? | | |

# VALORACIÓN DE IMPACTO DE RIESGOS SEGURIDAD DIGITAL

| CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **CATEGORÍA** | **DESCRIPCIÓN CUANTITATIVA** | **DESCRIPCIÓN CUALITATIVA** | **NIVEL** |
| **CATASTRÓFICO** | Afectación en un valor igual o superior al 50%de la población.<br><br>Afectación en un valor igual o superior al 50% del presupuesto de seguridad de la información en la entidad.<br><br>Afectación muy grave del medio ambiente que requiere > 3 años de recuperación | Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.<br><br>Interrupción de las operaciones de la entidad por más de cinco 5 días | **5** |
| **MAYOR** | Afectación en un valor igual o mayor al 20% e inferior al 50% de la población.<br><br>Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto de seguridad de la información en la entidad.<br><br>Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación | Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación grave de la confidencialidad de la | **4** |

| CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **CATEGORÍA** | **DESCRIPCIÓN CUANTITATIVA** | **DESCRIPCIÓN CUALITATIVA** | **NIVEL** |
| | | información debido al interés particular de los empleados y terceros.<br><br>Interrupción de las operaciones de la entidad entre 2 y 4 días | |
| **MODERADO** | Afectación en un valor igual o mayor al 10% y menor al 20% de la población.<br><br>Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto de seguridad de la información en la entidad.<br><br>Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación. | Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.<br><br>Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.<br><br>Interrupción de las operaciones de la entidad por un (1) día. | **3** |
| **MENOR** | Afectación en un valor igual o mayor al 1% y menor al 10%de la población.<br><br>Afectación en un valor igual o mayor al 1% y menor al 10%del presupuesto de seguridad de la información en la entidad. | Afectación leve de la integridad.<br><br>Afectación leve de la disponibilidad.<br><br>Afectación leve de la confidencialidad.<br><br>Interrupción de las operaciones de la entidad | **2** |

| CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL | | | |
|---|---|---|---|
| **CATEGORÍA** | **DESCRIPCIÓN CUANTITATIVA** | **DESCRIPCIÓN CUALITATIVA** | **NIVEL** |
| | Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación | hasta por 8 horas (1 jornada laboral) | |
| **INSIGNIFICANTE** | Afectación en un valor menor al 1% de la población.<br><br>Afectación en un valor menor al 1% del presupuesto de seguridad de la información en la entidad.<br><br>No hay afectación medioambiental. | Sin afectación de la integridad.<br><br>Sin afectación de la disponibilidad.<br><br>Sin afectación de la confidencialidad<br><br>No hay interrupción de las operaciones de la entidad | **1** |

## CRITERIOS PARA LA EVALUACIÓN DE IMPACTO DE PÉRDIDA DE CONTINUIDAD DE NEGOCIO

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio se realiza a través de la valoración del impacto percibido por los líderes de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencia a los servicios con menor impacto percibido.

| CRITERIO | DESCRIPCIÓN |
|---|---|
| **FINANCIERO** | Nivel de pérdidas económicas |
| **REPUTACIONAL** | Nivel de pérdida de la confianza de los grupos de valor en la entidad |
| **LEGAL / REGULATORIO** | Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad |
| **CONTRACTUAL** | Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales |
| **MISIONAL** | Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales |

## ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”

| TIPO DE RIESGO | RESPONSABLE | ACCIÓN |
|---|---|---|
| **Riesgo de Corrupción** | Jefe Área Social y de Comunicaciones | • Informar al proceso de planeación estratégica sobre el hecho encontrado.<br>• Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente.<br>• Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento.<br>• Efectuar el análisis de causas y determinar acciones preventivas y de mejora.<br>• Actualizar el mapa de riesgos. |
| | Jefe de Control Interno | • Informar al líder de proceso, quien analizará la situación y definirá las acciones a que haya lugar.<br>• Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.<br>• Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder de proceso, para revisar el mapa de riesgos |
| **Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)** | Líder de proceso | • Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento.<br>• Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. |
| **Riesgos de Gestión y** | | |

| TIPO DE RIESGO | RESPONSABLE | ACCIÓN |
|---|---|---|
| **Seguridad digital (Zona Baja)** | | • Analizar y actualizar el mapa de riesgos.<br>• Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos. |
| **Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)** | Jefe de Control Interno | • Informar al líder de proceso sobre el hecho encontrado.<br>• Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder de proceso, para revisar el mapa de riesgos.<br>• Acompañar al líder de proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.<br>• Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente. |
| **Riesgos de Proceso y Seguridad digital (Zona Baja)** | | • Informar al líder de proceso sobre el hecho.<br>• Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder de proceso, para revisar el mapa de riesgos<br>• Acompañar al líder de proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.<br>• Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente. |

## ESTRATEGIAS PARA LA ACEPTACIÓN DEL RIESGO RESIDUAL

Acorde con los riesgos residuales aprobados por el Comité Institucional de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados, de la siguiente manera:

A partir de los criterios ERCA (Evitar, Reducir, Compartir y Aceptar), la entidad establece los siguientes niveles de aceptación a los riesgos identificados:

| TIPO DE RIESGO | ZONA DE RIESGO RESIDUAL | ESTRATEGIA DE TRATAMIENTO |
|---|---|---|
| **Riesgos de Gestión y Seguridad digital** | Baja | Se **ACEPTA** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte mensual de su desempeño. |
| | Moderada | Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad o el impacto de ocurrencia del riesgo, se hace seguimiento **BIMESTRAL** y se registran sus avances en el Módulo de Riesgos- SIG |
| | Alta y Extrema | Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **EVITAR** la materialización del riesgo. Se monitorea **MENSUALMENTE** y se registra en el Módulo de Riesgos - SIG |
| **Riesgos de Corrupción** | Baja | Ningún riesgo de corrupción podrá ser aceptado. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos. |
| | Moderada | Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra en el Módulo de Riesgos - SIG |

| TIPO DE RIESGO | ZONA DE RIESGO RESIDUAL | ESTRATEGIA DE TRATAMIENTO |
|---|---|---|
| | Alta y Extrema | Se adoptan medidas para:<br>**REDUCIR** la probabilidad, el impacto o ambos factores del riesgo; la estrategia conlleva a la implementación de controles.<br>**EVITAR** Se abandonan o modifican las actividades que dan lugar al riesgo, decidiendo no iniciar, no continuar o modificar de forma segura la actividad que causa el riesgo.<br>**COMPARTIR** con un tercero el tratamiento de una parte del riesgo para reducir la probabilidad, el impacto o ambos factores.<br>Periodicidad de seguimiento **MENSUA**L para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el Módulo de Riesgos – SIG |

## EVALUACIÓN DEL RIESGO

Su objetivo es comparar los resultados del análisis de riesgos con los controles establecidos, para determinar la zona de riesgo final, los pasos a seguir son:

| | |
|---|---|
| **Evaluación del riesgo** | Naturaleza del control |
| | Documentación del control |
| | Determinar riesgo residual |

## DISEÑO REDACCIÓN DE UN CONTROL

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, un control debe tener:

| | |
|---|---|
| **Diseño de Controles** | Responsable |
| | Periodicidad |
| | Propósito |
| | Cómo se realiza el control |
| | Que pasa con las excepciones |
| | Evidencia de la ejecución |

# ANÁLISIS Y EVALUACIÓN DEL DISEÑO DEL CONTROL

| CONTROLES DE RIESGOS | | | | | | |
|---|---|---|---|---|---|---|
| Descripción del Control | Naturaleza del Control | | Criterios para la evaluación<br>Aspectos a evaluar en el diseño del control | Evaluación | | |
| | Preventivo | Detectivo | | | | |
| | | | ¿Existe un responsable asignado a la ejecución del control? | Asignado | No Asignado | |
| | | | | 15% | 0% | |
| | | | ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control? | Adecuado | No Adecuado | |
| | | | | 15% | 0% | |
| | | | ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna? | Oportuna | Inoportuna | |
| | | | | 15% | 0% | |
| | | | ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, ¿etc.? | Prevenir | Detectar | No es control |
| | | | | 15% | 10% | 0% |
| | | | ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo? ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo? | Confiable | No Confiable | |
| | | | | 15% | 0% | |

| CONTROLES DE RIESGOS | | | | | | |
|---|---|---|---|---|---|---|
| **Descripción** | **Naturaleza del Control** | | **Criterios para la evaluación** | **Evaluación** | | |
| | | | ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna? | Se investigan y resuelven oportunamente | No se investigan y resuelven oportunamente | |
| | | | | 15% | 0% | |
| | | | ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión? | Completa | Incompleta | No existe |
| | | | | 10% | 5% | 0% |
| **TOTAL** | | | | **100%** | | |

Cada control va a tener la misma importancia, por lo tanto, el consolidado de los controles para mitigar un riesgo, se realizará promediando el número de controles asociados al riesgo.
El resultado de las calificaciones del control o promedio en el diseño de los controles, que este por debajo de 96 %, se debe establecer un plan de acción, para el adecuado diseño del control.

| CALIFICACIÓN DISEÑO DE LOS CONTROLES | DEFINICIÓN |
|---|---|
| **Fuerte 96% - 100%** | El control o controles están bien diseñado para mitigar el Riesgo |
| **Moderado 86% - 95%** | Con Observaciones en la evidencia del control |
| **Débil 0% - 85%** | El control tiene debilidades en su diseño para mitigar el riesgo |

Se debe confirmar por parte de los líderes de proceso la ejecución de cada control, de acuerdo a la siguiente tabla:

+

| CALIFICACIÓN DE EJECUCIÓN DE LOS CONTROLES | DEFINICIÓN |
|---|---|
| **Fuerte** | Siempre se ejecuta por parte de los responsables |
| **Moderado** | Algunas veces se ejecuta por parte de los responsables |
| **Débil** | Nunca se ejecuta el control. |

=

| PONDERACIÓN DISEÑO DE CONTROLES | EJECUCIÓN DE CONTROLES | SOLIDEZ DEL CONTROL |
|---|---|---|
| **Fuerte** | Fuerte | Fuerte |
| | Moderado | Moderado |
| | Débil | Débil |
| **Moderado** | Fuerte | Moderado |
| | Moderado | Moderado |
| | Débil | Débil |
| **Débil** | Fuerte | Débil |
| | Moderado | Débil |
| | Débil | Débil |

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, y considerando si lo controles ayudan o no a la disminución de impacto o la probabilidad, procedemos a la elaboración del Mapa de Riesgo Residual (después de los controles)

## SEGUIMIENTO A LAS ACCIONES DE CONTROL DEL RIESGO EN CADA PROCESO

- Según la periodicidad definida para cada riesgo, el delegado de riesgos en cada proceso y el líder del mismo verifica las acciones preventivas y registra el avance junto con la evidencia en el SIG.
- El delegado de riesgo en cada proceso y el líder del mismo analizan los resultados del seguimiento y establece acciones inmediatas ante cualquier desviación
- El líder de proceso comunica las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.
- El líder de proceso se asegura que se documenten las acciones de corrección o prevención en el plan de mejoramiento
- El delegado de riesgo en cada proceso y el líder del mismo revisa y actualiza, con el acompañamiento del responsable de planeación o quien haga sus veces el mapa de riesgo cuando se modifique las acciones o la ubicación del riesgo.

## PERIODO DE REVISIÓN RIESGOS INSTITUCIONALES

Los riesgos se identifican y/o validan en cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción institucional, asegurando la articulación de éstos con los compromisos de cada proceso.

A partir de los criterios ERCA (Evitar, Reducir, Compartir y Aceptar), la Entidad establece la siguiente periodicidad de seguimiento a los riesgos identificados:

| ZONA DE RIESGO RESIDUAL | PERIODICIDAD | |
|---|---|---|
| | RIESGOS GESTIÓN Y SEGURIDAD DIGITAL | RIESGOS DE CORRUPCIÓN |
| **Bajo** | Se realiza en el reporte mensual de su desempeño | Periodicidad **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos. |
| **Moderado** | Se administra mediante seguimiento **BIMESTRAL** y se registran sus avances en el Modelo de Riesgos-SIG | |
| **Alto** | La Administración de estos riesgos será con periodicidad sugerida al menos **MENSUAL** y su adecuado control se registra en el Modelo de Riesgos - SIG | |
| **Extremo** | La Administración de estos riesgos será con periodicidad sugerida al menos **MENSUAL** y su adecuado control se registra en el Modelo de Riesgos - SIG | |

## HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

Función Pública determina que el Módulo de Riesgos del SIG es el instrumento para identificar, valorar, evaluar y administrar los riesgos, de corrupción y de seguridad digital, por tanto, toda información asociada con los riesgos es provista por dicha herramienta, para lo cual el responsable de planeación o quien haga sus veces identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información y dispone un manual de uso para el servicio de todos los procesos.

Para una mayor comprensión de la política de operación para la administración del riesgo, se define que los anexos son parte fundamental de este documento técnico,

por tanto, se recomienda su consulta y conocimiento por parte de todos los servidores públicos de la Asociación Aeropuerto del Café AEROCAFÉ.

Manual operativo MIPG
Política para la Administración del Riesgo Asociación Aeropuerto del Café AEROCAFÉ
Guía para la Administración del riesgo de DAFP
Módulo de riesgos SIG