**POLÍTICA Y METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO**

****

**IVAN MAURICIO SOTO**

**ALCALDE**

**BARRANCAS LA GUAJIRA PERIODO 2020-2023**

**TABLA DE CONTENIDO**

**INTRODUCCIÓN**

**1. ALCANCE**

**2. OBJETIVOS**

**3. MARCO NORMATIVO**

**4. CONTEXTO**

**5. RIESGOS INSTITUCIONALES**

**6. METODOLOGÍA APLICADA**

**7. PERIODICIDAD**

**8. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS**

**9. RESPONSABLES**

**10. DEFINICIONES**

**11. COMUNICACIÓN Y DIVULGACIÓN**

**12. MARCO CONCEPTUAL PARA NIVELES DE ACEPTACION DEL RIESGO**

**13. IDENTIFICACIÓN DEL RIESGO**

**14. VALORACIÓN DEL RIESGO**

**15. DISEÑO Y VALORACIÓN DE CONTROLES**

**16. MONITOREO, SEGUIMIENTO Y EVALUACION**

**17. BIBLIOGRAFIA**

I**NTRODUCCIÓN**

La política de administración del riesgos establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos, esta política es aplicable a todos los procesos, proyectos, productos de la Entidad y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

La Política para la Administración del Riesgo de la Alcaldía Municipal de Barrancas La Guajira recoge la estrategia liderada desde la Alta Dirección de la Entidad, enfocada en la identificación, tratamiento, manejo y seguimiento de los riesgos de Gestión, Corrupción y Seguridad y Privacidad de la Información a través de la creación de controles, que incidan en la prevención de la materialización del riesgo y acciones de contingencia en caso de que esto suceda, con el fin de garantizar el cumplimiento de los objetivos misionales de la Entidad.

La Política de Administración del Riesgo del Alcaldía Municipal de Barrancas La Guajira, denota el grado de compromiso de la entidad frente al cumplimiento de los objetivos estratégicos y del plan de acción institucional, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados.

Es importante resaltar que esta política toma como referente los lineamientos del Modelo Integrado de Planeación y Gestión MIPG, así como los del Modelo Estándar de Control Interno MECI, en lo referente a las líneas de defensa, el Decreto 2641 del 2012, la Norma Técnica Internacional Administración del Riesgo la Metodología ISO 31000:2018 y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” v5 2020, expedida el Departamento Administrativo de la Función Pública DAFP.

1. **ALCANCE**

La Administración del Riesgo en la Alcaldía Municipal de Barrancas La Guajira tendrá el siguiente alcance:

* **Riesgos de Gestión y Riesgos de Corrupción y Fraude:** Todos los procesos de la alcaldía municipal de Barrancas, La Guajira.
* **Riesgos del Sistema de Gestión de Seguridad de la Información - Seguridad Digital:** Los procesos que hacen parte del alcance del Sistema de Gestión de la Seguridad de la información (SGSI), como lo son los procesos misionales (Normalización y Culturización Contable, Centralización de la Información y Consolidación de la Información) y el proceso de Gestión TIC´s.

La política de la gestión del riesgo es aplicable a todos los procesos y procedimientos de la Alcaldía Municipal de Barrancas La Guajira a todas las acciones ejecutadas por los servidores durante el ejercicio de sus actividades.

Esta política de administración del riesgo contribuye al control interno de la entidad, y fomenta la cultura del autocontrol al interior de los procesos.

1. **OBJETIVOS**

* Establecer los lineamientos y criterios necesarios que orienten a la Alcaldía Municipal de Barrancas La Guajira para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos, valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
* Orientar la toma de decisiones oportunas y minimizar efectos adversos al interior de la entidad, con el fin de garantizar la continuidad a la gestión institucional y el logro de los objetivos estratégicos de la entidad.
* Incentivar el pensamiento basado en riesgos dentro de la entidad.
* Promover la mejora continua en cada uno de los procesos de la entidad.
* Realizar seguimiento y evaluación a la gestión de los riesgos asociados a los procesos de la entidad.
* Establecer una adecuada gestión mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante situaciones que afecten el cumplimiento misional y el logro de los objetivos.

**3. MARCO NORMATIVO**

* **Ley 87 de 1993:** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del Control Interno: Literal a) Proteger los recursos de la organización, buscando adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
* Ley 489 de 1998: Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.
* Directiva presidencial 09 de 1999 Lineamientos para la implementación de la política de lucha contra la corrupción.
* Decreto 1537 de 2001 Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las empresas y organismos del Estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (…) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).
* **Ley 1474 de 2011:** Estatuto Anticorrupción Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
* **Decreto 4637 de 2011:** Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República, quien establece lineamientos para la prevención de la corrupción.
* **Decreto 1649 de 2014 Funciones de la Secretaría de Transparencia:** 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de atención al ciudadano que deberán elaborar anualmente las entidades del orden nacional y territorial.
* **ISO 9001:2015**: Norma Técnica Colombiana, elaborada por la [Organización Internacional para la Estandarización](https://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Normalizaci%C3%B3n) (International Standarization Organization o ISO por sus siglas en inglés), determina los requisitos para un [Sistema de Gestión de la Calidad](https://es.wikipedia.org/wiki/Sistema_de_Gesti%C3%B3n_de_la_Calidad).
* **Decreto 1081 de 2015:** Señala como metodología para elaborarla estrategia de lucha contra la corrupción la contenida en el documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.
* **Decreto Nacional 1499 de 2017:** hace necesario adoptar para la Alcaldía municipal el MIPG, como el nuevo marco de referencia para el diseño e implementación del SIG, con el fin de fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades de la alcaldía municipal adecuar la institucionalidad del sistema y de las instancias correspondientes con el modelo nacional.
* **ISO 31000:2018:** Norma Técnica Internacional Administración del Riesgo- Principios y orientaciones.
* Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” v5 2020.

**4. CONTEXTO**

Para la identificación de riesgos la entidad realiza un análisis de su entorno estratégico a partir de los siguientes factores internos y externos:

**Factores Externos**

* **Económicos y financieros:** Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
* **Políticos:** Cambio de Gobierno, legislación, políticas públicas, regulación.
* **Sociales:** Demografía, responsabilidad social, orden público.
* **Tecnológicos**: Avances en tecnología, acceso a sistemas de información externos, Gobierno en línea.
* **Ambientales:** Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
* **Legales y reglamentarios**: Normativa externa.
* **Pandemia:** Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

**Factores Interno**

* **Financieros:** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
* **Personal:** Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
* **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 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.

**5. RIESGOS INSTITUCIONALES**

El mapa de riesgos institucional se consolidará a partir de aquellos riesgos de gestión ubicados en la zona extrema y alta, a estos se les efectuará seguimiento y monitoreo continuo por parte de los líderes de proceso o responsables asignados para tal fin, quienes deberán garantizar que los controles se ejecuten en los tiempos estipulados, evitando con ello la materialización de los riesgos.

**6. METODOLOGÍA APLICADA**

La metodología aplicada para la administración del riesgo será la contemplada en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” v 5 del 2020 expedida por el Departamento Administrativo de la Función Pública.

**7. PERIODICIDAD**

La revisión de los mapas de riesgos de gestión, Riesgos de corrupción y fraude ,y riesgos de seguridad y privacidad de la información - Seguridad Digital de la Alcaldía Municipal de Barrancas La Guajira , se realizará como mínimo Una (1) veces al año o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales en el contexto estratégico, cambios relevantes en los procesos y/o procedimientos, o cualquier hecho sobreviniente externo o interno que afecte la operación de la entidad.

El Asesor de Control Interno o quien haga sus veces, debe adelantar seguimiento a la gestión del riesgo de acuerdo con lo establecido en la “Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces”, MIPG y “Estrategias para la Construcción del Plan Anticorrupción y de atención al ciudadano” ésta última define los siguientes cortes de seguimiento a los riesgos de corrupción:

* **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
* **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
* **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

Adicionalmente se deberá presentar un informe cuatrimestral que contenga los resultados de los seguimientos a los riesgos de los procesos, con el fin de evidenciar la materialización, la creación, modificación o eliminación de alguno de ellos.

**8. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS**

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión- **(MIPG)** en la dimensión siete (7) “Control Interno” desarrolla a través de la Línea Estratégica y las tres (3) Líneas de Defensa de responsabilidad de la gestión del riesgo y control.

| **LÍNEAS DE DEFENSA** | **RESPONSABLE** | **RESPONSABILIDAD FRENTE AL RIESGO** |
| --- | --- | --- |
| **Estratégica** | **Alta Dirección, Comité Institucional de Coordinación de Control Interno** | Está conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.  Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad.  Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la Línea Estratégica:   * Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones. * Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica. * Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. * Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. * Evaluación de la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar). * Define el marco general para la gestión del riesgo y el control; y supervisa su cumplimiento. |
| **Primera línea** | **Líderes de proceso** | Esta línea de defensa les corresponde a los servidores 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. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.  Los aspectos clave para el Sistema de Control Interno (SCI) a tener en cuenta por parte de la 1ª Línea:   * El conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. * La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. * El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. * La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. * La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. |
| **Segunda línea** | **Oficina Asesora de Planeación** | Esta línea de defensa 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.  Aquí se incluyen a los funcionarios asesores y líder del área de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos, líder de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de la entidad. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica)  Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.  Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 2ª Línea son:   * Aseguramiento de que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. * Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. * Realizar el seguimiento al mapa de riesgos de su proceso. * Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. * Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. * Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. * La (El) Jefe de Oficina Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. * Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. * Trabajo coordinado con las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno. * Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora). * Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. * 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. * Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. * 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. * Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. * Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio. * Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del Comité de Coordinación de * Control Interno. |
| **Tercera línea** | **Oficina de Control Interno quien haga sus veces** | Esta línea está bajo la responsabilidad de la (el) profesional asesor de control interno; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.  El funcionario responsable y líder del proceso de control interno 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.  La interacción entre la 2ª línea de defensa (proveedores internos de aseguramiento) y la 3ª línea de defensa y estas con los proveedores externos de aseguramiento (organismos de control y otras instancias de supervisión o vigilancia) serán representadas en una matriz de doble entrada denominada mapa de aseguramiento18, herramienta considerada por el Instituto de Auditores como adecuada e idónea para coordinar las diferentes actividades de aseguramiento, visualizar el esfuerzo en común y mitigar los riesgos de una manera mucho más integral.  Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 3ª Línea:   * A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos. * Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. * 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. * Informar los hallazgos y proporcionar recomendaciones de forma independiente. * 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. * Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa * Recomendar mejoras a la política de operación para la administración del riesgo. |

**Tabla 1-Fuente:** Tomado de la política de administración de riesgos de la función pública**.**

# 9. RESPONSABLES

Las responsabilidades para la administración del riesgo, se definieron con base en las líneas de defensa, se encuentran descritas en el Anexo 1 del presente documento.

# 10. 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:** Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.
* **Análisis de Riesgos:** Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.
* **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
  + **Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito puede ser diferente para los distintos tipos de riesgo que la entidad debe o desea gestionar.
  + **Capacidad de riesgo**: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sea posible el logro de los objetivos de la entidad.
  + **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros pueden producir la materialización de un riesgo.
  + **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
  + **Causa raíz:** Causa principal o básica, correspondiente a las razones por las cuales se puede presentar el riesgo.
  + **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
  + **Control:** Media que permite reducir o mitigar un riesgo.
  + **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
  + **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
  + **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables o tolerables.
  + **Factores de riesgo:** Son las fuentes generadoras de riesgos.
  + **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:** Proceso de análisis para encontrar una potencial desviación de los objetivos.
  + **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
  + **Integridad:** Propiedad de exactitud y completitud.
  + **Mapa de calor:** Plano en el que se presentan simultáneamente las escalas de medición de impacto y de probabilidad, y que, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.
  + **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
  + **Materialización del Riesgo:** Ocurrencia o desarrollo del riesgo.
  + **Nivel de riesgo**: Es el valor que se determina a parir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional del alcanzar los objetivos.
  + **Objetivo de proceso**: Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción
  + **Oportunidad:** Eventos que permiten alcanzar un resultado esperado o aumentar los efectos deseables.
  + **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
  + **Política de Administración del Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
  + **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
* **Riesgo:** Efecto que 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, falla o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
* **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
* **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
* **Riesgo de fraude:** Posibilidad de que la Entidad incurra en una pérdida financiera o de otro tipo cuando una persona (que puede ser empleado, un cliente, o una persona vinculada a la Entidad) que actúa individualmente o en colusión, obtiene una ventaja o beneficio injusto en forma deshonesta o engañosa.
* **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000). Efecto de la incertidumbre sobre los objetivos.

Nota 1 a la entrada: Un efecto es una desviación de lo esperado: positivo o negativo.

Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de un evento, su consecuencia o probabilidad.

Nota 3 a la entrada: El riesgo se caracteriza a menudo por referencia a posibles "eventos" (como se define en la Guía ISO 73: 2009, 3.5.1.3) y "consecuencias" (como se define en la Guía ISO 73: 2009, 3.6.1.3), o una combinación de estos.

Nota 4 a la entrada: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la “probabilidad” asociada (como se define en la Guía ISO 73: 2009, 3.6.1.1) de ocurrencia.

Nota 5 a la entrada: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información.

Nota 6 a la entrada: El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

* **Riesgo inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riego inherente, dentro de unas escalas de severidad.
* **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
* **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.
* **Tratamiento del riesgo:** Proceso para modificar el riesgo.
* **Valoración del Riesgo:** Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.
* **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

# 11. COMUNICACIÓN Y DIVULGACIÓN

La Política y Metodología para la Administración de Riesgos busca crear conciencia en todos los servidores públicos de la Alcaldía Municipal de Barrancas La Guajira, en los distintos niveles y vinculaciones, sobre la importancia de la gestión preventiva y el autocontrol en la ejecución de las actividades y se desarrolla en dos niveles, en los cuales se adelantan acciones o estrategias de comunicación y divulgación según su propósito:

* **A nivel institucional**: Comprende la divulgación y socialización de la Política y Metodología de Administración del Riesgo y el Mapa de Riesgos, la cual estará a cargo de la Oficina Asesora de Planeación. Esta estrategia incluye la publicación en la página web de la entidad, del Mapa de Riesgos de Corrupción y el resultado de los seguimientos.
* **A nivel de procesos**: Comprende la divulgación de los Mapas de Riesgos por Proceso al interior de los respectivos equipos de trabajo, está a cargo de los Responsables de cada Proceso con el apoyo de los gestores de calidad.

# 

# 12. MARCO CONCEPTUAL PARA NIVELES DE ACEPTACION DEL RIESGO:

La entidad ha definido los niveles de aceptación teniendo en cuenta las siguientes fórmulas:

|  |  |  |
| --- | --- | --- |
| **Nivel de riesgo** |  | |
| Riesgo inherente | = | Probabilidad inherente vs Impacto |
| Riesgo Residual | = | Probabilidad inherente – (Probabilidad Inherente \* Control) vs Impacto inherente – (Impacto Inherente \* Control) |

Tiendo en cuenta el apetito, la tolerancia y la capacidad del riesgo, para la entidad los niveles de aceptación del riesgo residual son:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **UBICACIÓN EN EL MAPA DE CALOR**  **(Riesgo Residual)** | **NIVELES DE ACEPTACION** | **FORMULA** | **ACCION A TOMAR** |
| **GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN** | Bajo | Apetito del riesgo | # riesgos bajos / Total riesgos | Riesgos aceptado |
| Moderado | Tolerancia del riesgo | # riesgos moderados y altos / Total riesgos | Riesgo tolerado sin plan de acción (acciones para abordar riesgos) |
| Alto | Riesgo tolerado con plan de acción (acciones para abordar riesgos) |
| Extremo | Capacidad del riesgo | # riesgos extremos / Total riesgos | Riesgo soportado con acciones correctivas |
| **CORRUPCIÓN Y FRAUDE** | **Moderado** | **Apetito al riesgo** | # riesgos bajos / Total riesgos | Riesgo tolerado sin plan de acción (acciones para  abordar riesgos) |
| **Alto** | **Tolerancia del riesgo** | # riesgos moderados y altos / Total  riesgos | Riesgo tolerado con plan de acción (acciones para abordar riesgos) |
| **Extremo** | **Capacidad de riesgo** | # riesgos  extremos / Total riesgos | Riesgo soportado con acciones correctivas |

**Tabla 2. Clasificación de Niveles de Aceptación**

Estos conceptos se relacionan gráficamente así:

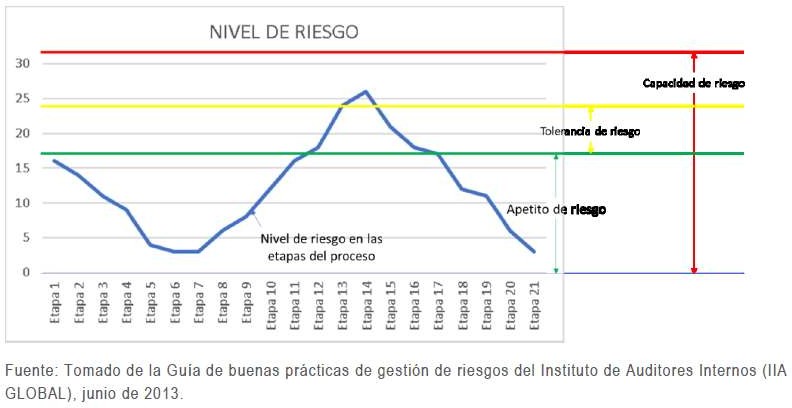


Figura 1: Definiciones de apetito, tolerancia y capacidad de riesgo.

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020

# 13. IDENTIFICACIÓN DEL RIESGO

# CONOCIMIENTO Y ANÁLISIS DE LA ENTIDAD:

Antes de iniciar con la metodología para administrar los riesgos es necesario comprender el contexto general de la entidad (cuestiones internas y externas) y establecer el Marco o Direccionamiento Estratégico el cual se define para la Alcaldía Municipal de Barrancas La Guajira cada cuatro años.

El Marco Estratégico de la Alcaldía Municipal de Barrancas La Guajira parte de un análisis de contexto que permite reconocer en dónde se encuentra la entidad al revisar y establecer su direccionamiento para el siguiente periodo de gobierno. Este contexto se compone del **contexto externo (**factores: políticos, económicos, financieros, sociales, culturales, tecnológicos, ambientales, legales y reglamentarios), **contexto interno** (misión, visión, estructura organizacional, funciones y responsabilidades, políticas, planeación institucional, objetivos y estrategias implementadas, recursos con los que se cuenta (económicos, personas, procesos, sistemas, tecnología, información), cultura organizacional y relaciones con las partes involucradas) y **contexto del proceso** (objetivo y alcance del proceso, interrelación con otros procesos, planes, programas o proyectos asociados y activos de seguridad digital del proceso) y como resultado se definen los ejes estratégicos y el despliegue de estos.

El conocimiento del contexto facilita la identificación de riesgos y oportunidades para el cumplimiento de los objetivos estratégicos.

**FACTORES DE RIESGO**

Son las fuentes generadoras de riesgos como lo son:

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

# 

# CLASIFICACION DEL RIESGO

Los riesgos se clasifican así:

|  |  |  |  |
| --- | --- | --- | --- |
| **TIPO** | **CLASIFICACION** | **DESCRIPCIÓN** | |
| **RIESGOS DE GESTION** | **EJECUCION Y ADMINISTRACION**  **DE PROCESOS** | Pérdidas derivadas de errores en la ejecución y administración de procesos. | |
| **FALLAS**  **TECNOLÓGICAS** | Errores en *hardware*, *software*, telecomunicaciones, interrupción de  servicios básicos. | |
| **RELACIONES LABORALES** | Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación. | |
| **USUARIOS, PRODUCTOS Y**  **PRÁCTICAS** | Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente  a éstos. | |
| **DAÑOS A ACTIVOS FIJOS/ EVENTOS**  **EXTERNOS** | Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público. | |
| **LEGALES** | Posibilidad de ocurrencia de eventos que afecten la situación  jurídica o contractual de la entidad debido a su incumplimiento o desacato a la normativa vigente. | |
| **RIESGOS DE SEGURIDAD DE LA INFORMACION** | | Pérdida de  confidencialidad, | Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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. |
| Pérdida de integridad  Pérdida de disponibilidad de los activos de información |

|  |  |  |
| --- | --- | --- |
| **RIESGOS DE FRAUDE** | **FRAUDE EXTERNO** | Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad). |
| **FRAUDE INTERNO** | Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo  de lucro para sí mismo o para terceros. |
| **RIESGOS DE CORRUPCIÓN** | | Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. |

**Tabla 3. Clasificación de Riesgos**

# DESCRIPCION DEL RIESGO:

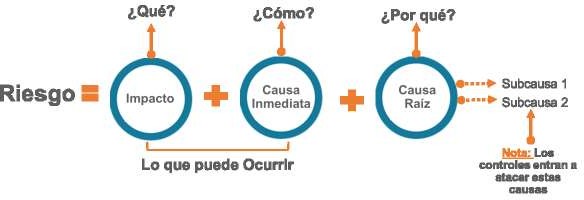
Los **Riesgos se identifican a partir de**l documento que establezca el direccionamiento estratégico, que estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los **objetivos estratégicos o del proceso**.

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para las personas ajenas a él. A continuación se relaciona la estructura que facilita su redacción y claridad. Se inicia con la frase **“POSIBILIDAD DE”.**

Desglosando la estructura tenemos:

* **Impacto:** Aquí definimos el ¿Qué puede pasar?, los factores de impacto a los que puede estar expuesta la entidad son:
* **Afectación Económica:** afectación presupuestal de la entidad
* **Afectación Reputacional:** afectación de la imagen de la entidad.
* **Causa inmediata:** nos responde al ¿Cómo puede pasar?, son las situaciones más evidentes por las cuales se puede materializar el riesgo.
* **Causa raíz:** nos dá respuesta al ¿Por qué puede pasar?. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas. Esta es la base para la definición de los controles.

El esquema para la redacción del riesgo es:



**Figura 2.** Estructura propuesta para la redacción del riesgo y ejemplo

# Recomendaciones:

* No describir como omisiones ni desviaciones de control.
* *Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.*
* No describir causas como riesgos.
* *Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.*
* No describir riesgos como la negación de un control.
* *Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.*
* No existen riesgos transversales, lo que pueden existir son causa transversales.
* *Ejemplo: pérdida de expedientes.*
* Evitar iniciar con palabras negativas como: “No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en…”
* Generar en el lector o escucha la imagen del evento como si ya estuviera sucediendo.
* Pregúntese si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es “no”, lo descrito puede ser la causa o la consecuencia del riesgo.

**Riesgos de Corrupción y Fraude**

Corresponde al líder de proceso o proyecto la identificación de los riesgos de corrupción y fraude, que podrían afectar el logro de los objetivos de los procesos de la Alcaldía Municipal de Barrancas La Guajira , los cuales están asociados al uso de poder y a la pérdida financiera.

Se puede determinar si un riesgo es de corrupción o fraude, si se marca con una X en la descripción del riesgo las situaciones señaladas en la siguiente tabla:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Descripción del riesgo** | **Acción u omisión** | **Uso del poder** | **Desviar la gestión de lo público** | **Perdida Financiera** | **Beneficio privado** |
| Riesgo de **Corrupción** | X | X | X |  | X |
| Riesgo de **Fraude** |  |  | X | X | X |

**Tabla 3. Determinación del Riesgo de Corrupción y Fraude**

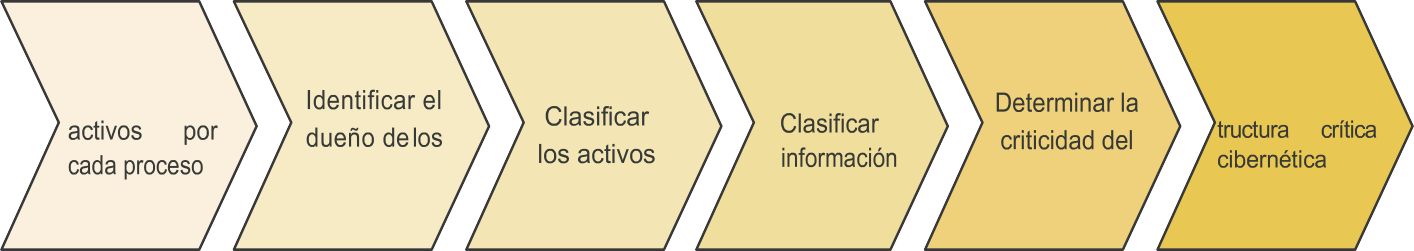
# Riesgos de Seguridad de la Información:

Corresponde al líder del Sistema de Gestión de Seguridad y Privacidad de la Información y al líder del proceso o proyecto la identificación de los riesgos de la Información. Estos 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”.

Como se señaló anteriormente, existen tres 3 tipos de riesgos de seguridad de la información: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información. Para cada tipo de riesgo se seleccionan las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se pueda materializar.

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 Identificación de activos. Los siguientes son los pasos que sirven de guía para identificar los activos de información:

# ¿Cómo identificar los activos de información?:



**Paso 1.**

**Paso 2.**

**Paso 3.**

**Paso 5.**

**Paso 4.**

**Paso 6.**

Identificar si

Listar los existe infraes-

la

activos

activo

Figura 3. Identificación de activos de la información.

# NOTA:

* La agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
* Para mayor información consultar Anexo 4. *Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas*, de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5 de diciembre de 2020.

# 14. VALORACIÓN DEL RIESGO

La valoración del riesgo 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 o propio de la actividad también llamado ***“RIESGO INHERENTE”*.**

**ANALISIS DE RIESGO**

Consiste en establecer la probabilidad de ocurrencia y el nivel de consecuencia o impacto del riesgo, con el fin de estimar su **probabilidad** de ocurrencia e **impacto/ consecuencia** si no se controla **(RIESGO INHERENTE).**

**Determinar la PROBABILIDAD:** se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? Está asociada a la exposición al riesgo del proceso o actividad que se está analizando, se trata en este caso de un hecho que no se ha presentado pero es posible, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, o tratándose de hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo.

A continuación se establecen los criterios para definir el nivel de probabilidad:

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **FRECUENCIA DE LA ACTIVIDAD** | **FRECUENCIA DE EVENTOS** | **PROBABILIDAD** |
| **MUY BAJA** | La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año. | El evento puede ocurrir solo en circunstancias  excepcionales (poco comunes o anormales). | 20% |
| **BAJA** | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año. | El evento puede ocurrir en algún momento. | 40% |
| **MEDIA** | La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año. | El evento podrá ocurrir en algún momento. | 60% |
| **ALTA** | La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5.000 veces por año. | Es viable que el evento ocurra en la mayoría de las circunstancias. | 80% |
| **MUY ALTA** | La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año. | Se espera que el evento ocurra en la mayoría de las circunstancias. | 100% |

**Tabla 4. Criterios para definir el nivel de PROBABILIDAD de ocurrencia de los riesgos.**

**Nota:** En materia de tecnología (incluye disponibilidad de aplicativos) se tiene en cuenta 1 hora de funcionamiento = 1 vez.

**Determinar el IMPACTO**/**CONSECUENCIA:** Este se determina para establecer las consecuencias o efectos del riesgo, con el fin de estimar la zona de riesgo en caso de no controlarse **(RIESGO INHERENTE).** Para definir la tabla de criterios, las variables principales que se tienen en cuenta son impactos económicos y reputacionales.

Cuando se presente más de un impacto en un solo riesgo con diferentes niveles, se debe tomar el nivel más alto.

Para el Riesgos de **Corrupción y Fraude** se tiene en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos. En este orden de ideas, no se contemplan los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

|  |  |  |
| --- | --- | --- |
| **NIVEL** | **VALOR**  **IMPACTO / CONSECUENCIA RIESGOS** | |
| **Riesgos de Gestión y de Seguridad de la Información** | **Riesgos de Corrupción y Fraude** |
| **LEVE** | 20% | N/A |
| **MENOR** | 40% |
| **MODERADO** | 60% | 60% |
| **MAYOR** | 80% | 80% |
| **CATASTRÓFICO** | 100% | 100% |

Tabla 5. Criterios para definir el nivel de impacto/consecuencia riesgos de la entidad vs riesgos de corrupción y Fraude

El **impacto / consecuencia** se establece, de acuerdo con los siguientes criterios:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **RIESGOS DE GESTION** | | | | |
| **NIVEL** | | **CUANTITATIVAS - ECONOMICA** | | **CUALITATIVAS - REPUTACIONAL** |
| **CATASTROFICO 100%** | | -Impacto que afecte la ejecución presupuestal en un valor ≥50%.  Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%.  -Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor  ≥50%.  -Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad. | | -Interrupción de las operaciones de la entidad por más de cinco (5) días.  Intervención por parte de un ente de control u otro ente regulador.  Pérdida de información crítica para la entidad que no se puede recuperar.  Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.  Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados. |
| **MAYOR 80%** | | -Impacto que afecte la ejecución presupuestal en un valor ≥20%.  - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. | | -Interrupción de las operaciones de la entidad por más de dos (2) días.  - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. |
| **RIESGOS DE GESTION** | | | | |
| **NIVEL** | **CUANTITATIVAS - ECONOMICA** | | **CUALITATIVAS - REPUTACIONAL** | |
| **MAYOR 80%** | -Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor  ≥20%.  -Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad. | | -Sanción por parte del ente de control u otro ente regulador.  -Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.  -Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o  ciudadanos. | |
| **MODERADO 60%** | -Impacto que afecte la ejecución presupuestal en un valor ≥5%.   * Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor   ≥5%.   * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad. | | -Interrupción de las operaciones de la entidad por un (1) día.   * Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. * Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. * Reproceso de actividades y aumento de carga operativa. * Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. * Investigaciones penales, fiscales o disciplinarias. | |
| **MENOR 40%** | -Impacto que afecte la ejecución presupuestal en un valor ≥1%.   * Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor   ≥1%.   * 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.   * Quejas de los usuarios relacionadas con la indebida aplicación de la Ley disciplinaria vigente, dentro de las actuaciones disciplinarias. * Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. | |
| **LEVE 20%** | -Impacto que afecte la ejecución presupuestal en un valor ≥0,5%.   * Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor   ≥0,5%.   * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad. | | -No hay interrupción de las operaciones de la entidad.   * No se generan sanciones económicas o administrativas. * No se afecta la imagen institucional de forma significativa. | |

Tabla 6. Criterios para definir el nivel de impacto/consecuencia – RIESGOS

Para calificar el **impacto / consecuencia del riesgo de corrupción y fraude** se debe responder el siguiente cuestionario:

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **PREGUNTA: Si el Riesgo de Corrupción o Fraude 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, servicios o 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? |  |  |

Tabla 7. Preguntas para calificar el impacto / consecuencia – RIESGO DE CORRUPCIÓN Y FRAUDE

De acuerdo con el resultado anterior, el número de preguntas contestadas afirmativamente permitirá ubicar el riesgo según la siguiente tabla y determinar el impacto / consecuencias del riesgo de corrupción y fraude:

|  |  |  |
| --- | --- | --- |
| **DESCRIPTOR** | **CANTIDAD DE PREGUNTAS**  **AFIRMATIVAS** | **IMPACTO / CONSECUENCIAS**  **CUALITATIVO** |
| **CATASTRÓFICO 100%** | DOCE a DIECINUEVE  preguntas | Genera consecuencias desastrosas para la entidad |
| **MAYOR 80%** | SEIS a ONCE preguntas | Genera altas consecuencias sobre la entidad. |
| **MODERADO 60%** | UNA a CINCO pregunta(s) | Genera medianas consecuencias sobre la entidad |

Tabla 8. Calificación impacto / consecuencia – RIESGO CORRUPCION Y FRAUDE

|  |  |  |
| --- | --- | --- |
| **RIESGO DE SEGURIDAD DE LA INFORMACION** | | |
| **NIVEL** | **CUANTITATIVAS - ECONOMICA** | **CUALITATIVAS - REPUTACIONAL** |
| **CATASTRÓFICO 100%** | -Afectación mayor o igual al 50% de la población.  -Afectación mayor o igual al 50% del presupuesto anual de seguridad digital.  -Afectación muy grave del medio ambiente que requiere de mayor o igual a 3 años de recuperación. | -Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros.   * Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. * Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y   Terceros. |
| **MAYOR 80%** | -Afectación en un valor igual o mayor al 20% e inferior al 50% de la población.  -Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto anual de seguridad digital.  -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.  -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.  -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. |
| **MODERADO 60%** | -Afectación en un valor igual o mayor al 10% y menor al 20% de la población.  -Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto anual de seguridad digital.  - Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación. | -Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.  -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.  -Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. |
| **MENOR 40%** | -Afectación en un valor igual o mayor al 1% y menor al 10% de la población.  -Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto anual de seguridad digital.  -Afectación leve del medio ambiente requiere de Afectación leve del medio  ambiente requiere de 1 a 3 meses de recuperación. | -Afectación leve de la integridad.  -Afectación leve de la disponibilidad.  -Afectación leve de la confidencialidad. |
| **LEVE 20%** | -Afectación en un valor menor al 1% de la población.  -Afectación en un valor menor al 1% del presupuesto anual de seguridad digital.  -No hay afectación medioambiental. | -Sin afectación de la integridad.  -Sin afectación de la disponibilidad.  -Sin afectación de la confidencialidad. |

Tabla 9. Criterios para calificar el impacto / consecuencia – RIESGO DE SEGURIDAD DE LA

# EVALUACIÓN DEL RIESGO – NIVEL DE RIESGO INHERENTE (SEVERIDAD)

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial **(RIESGO INHERENTE).** Para establecer el nivel de riesgo inherente (sin aplicación de controles) y residual (con aplicación de controles) se utilizan los Mapas de Calor, que permiten ubicar el riesgo en la zona de acuerdo con la calificación de la **probabilidad** y el **impacto / consecuencia.**

Para todos los riesgos de **gestión y de seguridad de la información**, se definen cuatro zonas de severidad en el mapa de calor como se menciona a continuación:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IMPACTO** | | | | | | |
| **PROBABILIDAD** | **Muy alta 100%**  **Alta 80%**  **Media 60%**  **Baja 40%**  **Muy baja 20%** |  |  |  |  |  |
|  |  |  |
|  |
|  |  |
| **Leve 20%** | | | **Menor 40%** | **Moderado 60%** | **Mayor 80%** | **Catastrófico 100%** |

|  |
| --- |
| **ZONA DE RIESGO** |
| **Extremo** |
| **Alto** |
| **Moderado** |
| **Bajo** |

**Figura 4.** Mapa de Calor Riesgo Inherente

# Riesgo de Corrupción y Fraude

**A APLIC**

**Moderado 60%**

**Catastrófico 100%**

**Mayor 80%**

**Muy baja 20%**

**RRUPCION**

**CO**

**Baja 40%**

**SGOS DE**

**RIE**

**Media 60%**

**S**

**ARA LO**

**P**

**Alta 80%**

**ABLE**

**ZON**

**Muy alta 100%**

**IMPACTO**

**PROBABILIDAD**

**Figura 5. Mapa de calor para riesgos de corrupción y fraude**

# 15. DISEÑO Y VALORACIÓN DE CONTROLES

Los controles o actividades de control son medidas que permiten reducir o mitigar las causas que hacen que el riesgo se materialice, por eso la importancia en su diseño y evaluación.

# Determinación de controles

La identificación de los controles se realiza a cada riesgo a través de entrevistas con los líderes de procesos o servidores expertos en su quehacer, de igual forma son los responsables de implementar y monitorear dichos controles con el apoyo de su equipo de trabajo.

El propósito es comparar los resultados del análisis de riesgo inherente (sin controles) con los controles establecidos, para determinar la zona de riesgo final o *“riesgo residual”*, los pasos a seguir son:

**Determinar control**

* Preventivo
* Detectivo
* Correctivo

Documentar el control

Determinar el riesgo residual

# Redacción de un control

Al momento de definir las actividades de control por parte de los Líderes de los Procesos y sus equipos en trabajo (primera línea de defensa), es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitiguen las causas que generan la materialización del riesgo. Esto se debe tener en cuenta desde la redacción del mismo. Un control debe tener:



**Figura 6. Etapas para la redacción de un control.**

**Ejemplo:**

El profesional de Contratación cada vez que se va a realizar un contrato, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor. En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación. Como evidencia deja Lista de Chequeo diligenciada con la información de la carpeta del cliente, y correos solicitando la información faltante en los casos que aplique.

# Tipología del Propósito de los Controles

Se deben seleccionar actividades de **control preventivo, detectivo y correctivo** que por sí solos ayuden a la mitigación las **causas** que originan los riesgos. Para cada causa debe existir un control. Un control puede ser tan eficiente que ayude a mitigar varias causas.

A través del ciclo de los procesos es posible establecer cuándo se activa un control, y por lo tanto, establecer su tipología con mayor precisión.

* Atacan el impacto frente a la materialización del riesgo.
* Control accionado después de que se materializa el

riesgo. Estos controles tienen costos implícitos.

**CONTROLES CORRECTIVOS**

* Detecta que algo ocurre y devuelve el proceso a los

controles preventivos. Atacan la probabilidad de ocurrencia del riesgo.

* Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo,

pero generan reproceso.

**CONTROLES DETECTIVOS**

* Va a las causas del riesgo.

Atacan la probabilidad de ocurrencia del riesgo

* Control accionado antes de que se realice la actividad originadora del riesgo, se

busca establecer las condiciones que aseguren el resultado final esperado.

**CONTROLES PREVENTIVOS**

**Figura 7.** Tipologías de Controles

De acuerdo con la **forma** como se ejecutan los controles tenemos:

* **Control manual:** controles que son ejecutados por personas.
* **Control automático:** son ejecutados por un sistema.

Es importante que para la adecuada mitigación de los riesgos no baste solo con que un control este bien diseñado, el control **debe ejecutarse por parte de los responsables tal como se diseñó.**

# Análisis y evaluación de controles (Atributos)

A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Los aspectos sin peso son atributos informativos que no tienen incidencia directa en la efectividad del control, sin embargo, permiten darle formalidad a éste.

Los aspectos de Tipo e Implementación, son atributos que tienen incidencia directa en la efectividad del control, su valoración suma máximo 50% y mínimo 25%.

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITERIO DE**  **EVALUACIÓN** | **DESCRIPCION** | **ASPECTO A EVALUAR EN EL DISEÑO DEL**  **CONTROL** | **PESO** |
| **1. Responsable** | Adecuado | El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control | - |
| Inadecuado | - |

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITERIO DE**  **EVALUACIÓN** | **DESCRIPCION** | **ASPECTO A EVALUAR EN EL DISEÑO DEL**  **CONTROL** | **PESO** |
| **2. 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 | - |
| **3. Tipo** | Prevenir | Va hacia las causas del riesgo, aseguran el resultado final esperado. | 25% |
| Detectar | Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos. | 15% |
| Corregir | Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su  implementación. | 10% |
| **4.** Implementación | Automático | Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización. | 25% |
| Manual | Controles que son ejecutados por una persona, tiene implícito el error humano. | 15% |
| **5. Estado de la 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. | - |
| **7. Evidencia de la ejecución del control** | 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. | - |
| **TOTAL VALORACION CONTROL # Máximo 50%, mínimo 25%** | | | |

Tabla 10. Atributos para el diseño de controles

**Nota**: Siempre que se realicen ajustes a los controles se deben ajustar los documentos, y de igual forma si se hacen ajustes a los documentos del proceso se deben ajustar los controles involucrados.

**NIVEL DE RIESGO RESIDUAL**

Corresponde al resultado de aplicar la efectividad de los controles al riesgo inherente. A continuación se muestran las fórmulas para la aplicación de controles y establecer el riesgo residual:

Riesgo Residual = Probabilidad inherente – (Probabilidad Inherente \* Control) Impacto inherente – (Impacto Inherente \* Control)

**Nota:**

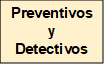
En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente (impacto inherente), es importante señalar que no es posible su movimiento en el mapa de calor para el impacto.

Cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. La solidez del conjunto de controles se define acorde a la tabla10 por cada riesgo. Con la calificación obtenida se realiza un desplazamiento en el mapa de calor, así: si el control afecta la probabilidad se avanza hacia abajo. Si afecta el impacto se avanza a la izquierda:

**Controles Correctivos**

**Atacan Impacto**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IMPACTO** | | | | | | |
| **PROBABILIDAD** | **Muy alta** |  |  |  |  |  |
| **100%** |
| **Alta** |  |  |  |
| **80%** |
| **Media** |  |  |  |  |  |
| **60%** |
| **Baja** |  |  |  |  |  |
| **40%** |
| **Muy baja** |  |  |  |  |  |
| **20%** |
| **Leve 20%** | | | **Menor 40%** | **Moderado 60%** | **Mayor 80%** | **Catastrófico 100%** |





**Atacan Probabilidad**

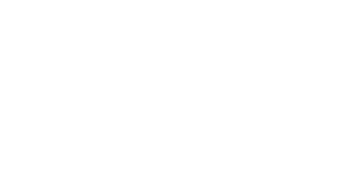
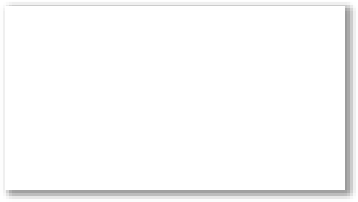
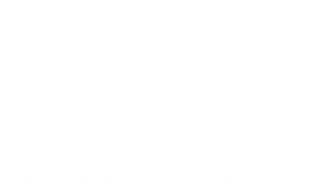
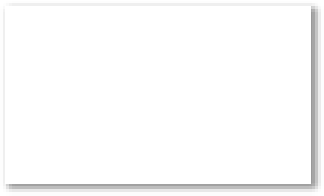
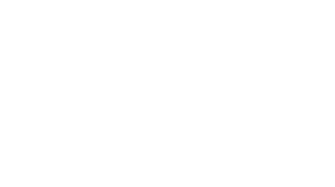
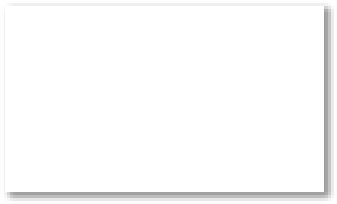
**Figura** **8.** Movimiento en el mapa de calor acorde con el tipo de control riesgo residual

Una vez realizado el análisis y evaluación de los controles se valora nuevamente la probabilidad e impacto/consecuencia del riesgo, determinando si los controles ayudan o no a la disminución probabilidad e impacto/consecuencia del riesgo y se procede a ubicar el **riesgo residual** en el **Mapa de Riesgo Residual.**

# NIVELES DE ACEPTACIÓN DEL RIESGO RESIDUAL

De acuerdo con la valoración de cada riesgo residual y su ubicación en la zona de riesgo (extremo, alto, moderado, bajo) se establece su opción de manejo. Esto se define a partir del nivel del riesgo residual (con controles), de la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Dependiendo del valor del riesgo residual, este se puede:



**MITIGAR**

Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

**TRANSFERIR**

Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

**EVITAR:**

Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

**ACEPTAR:**

Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

**REDUCIR:**

Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

Figura 9. Criterios de aceptación del Riesgo Residual.

A partir de los criterios RAE (Reducir, Aceptar y Evitar), la entidad establece las siguientes acciones para los niveles de aceptación a los riesgos así:

|  |  |
| --- | --- |
| CRITERIOS | ACCIONES |
| **ACEPTAR** | Se debe asumir el riesgo y el impacto de su materialización en caso que se presente. |
| **EVITAR** | Se debe eliminar, evitar o cambiar la actividad generadora del riesgo. |
| **REDUCIR** | Adoptar acciones para abordar riesgos encaminadas a reducir, mitigar o transferir el riesgo, no necesariamente las acciones es un control adicional. |

Tabla 11. Acciones para los niveles de aceptación del Riesgo Residual

De acuerdo con la ubicación en la zona del riesgo residual se deben implementar los siguientes niveles de aceptación:

|  |  |  |
| --- | --- | --- |
| **ZONA DE RIESGO** | **NIVEL DE ACEPTACIÓN DEL RIESGO RESIDUAL** | |
| **Gestión y Seguridad de la Información** | **Corrupción y Fraude** |
| **Bajo** | **ACEPTAR - EVITAR** | **Ningún** riesgo de corrupción podrá ser aceptado. |
| **Moderado** | **EVITAR** - **REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A**  **MITIGAR EL RIESGO) - ACEPTAR** | **REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A**  **MITIGAR EL RIESGO) - EVITAR** |
| **Alto** | **EVITAR** - **REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)**  Los riesgos ubicados en esta zona deben  contar con un indicador de riesgo, para monitorear el comportamiento | **EVITAR** - **REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)**  Los riesgos ubicados en esta zona deben  contar con un indicador de riesgo, para monitorear el comportamiento |
| **Extremo** | **EVITAR** - **REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)**  Los riesgos ubicados en esta zona deben contar con un indicador de riesgo, para monitorear el comportamiento | **EVITAR** - **REDUCIR (TRANSFIRIENDO O IMPLEMENTAR ACCIONES PARA ABORDAR RIESGOS DIRIGIDAS A MITIGAR EL RIESGO)**  Los riesgos ubicados en esta zona deben contar con un indicador de riesgo, para monitorear el comportamiento |

Tabla 12. Niveles de aceptación del Riesgo Residual.18

**16. MONITOREO Y REVISION**

Anticipándose a los eventos negativos relacionados con la materialización de los riesgos, y asegurando el logro de los objetivos estratégicos que se ha trazado la Alcaldía Municipal de Barrancas La Guajira, se desarrollan a través de las líneas de defensa, la gestión del riesgo y control, mediante la asignación de roles y responsabilidades de todos los actores del riesgo y control, alineando el monitoreo y seguimiento con Control Interno.

La actualización de la política de riesgos se deberá hacer cada año al inicio de la vigencia y el monitoreo de los riesgos se deberá realizar máximo semestralmente y generar el informe de autoevaluación, el cual deberá ser socializado por el Líder del proceso a la totalidad de los servidores públicos de su dependencia y remitido a la Oficina Asesora de Planeación y la Oficina de Control Interno, junto con las actas de la socialización, en cumplimiento del procedimiento establecido.

|  |  |  |
| --- | --- | --- |
| **LÍNEA DE DEFENSA** | **RESPONSABLES** | **ACTIVIDADES** |
| **Línea Estratégica** | **Alta dirección-Comité Coordinación de Control Interno.** | * Revisar los cambios en el "Direccionamiento Estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. * Establecer la Política de Administración del Riesgo. * Específicamente el Comité Institucional de Coordinación de Control Interno, evaluar y dar línea sobre la administración de los riesgos en la entidad. * Realimentar a la Alta Dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. * Hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles. * Realizar seguimiento y análisis periódico a los riesgos. * Revisar el cumplimiento a los objetivos institucionales y de procesos incluidos los indicadores, e identificar en caso de que no se estén cumpliendo. * Revisar los planes de acción establecidos 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. |
| **Primera Línea** | **Líderes de proceso** | * Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales. * Definir y diseñar los controles a los riesgos. * Revisar que las actividades de control de sus procesos eliminen las causas y se encuentren documentadas y actualizadas en los procedimientos. * Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. * Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos, como aquellos que se están ocasionando que no se logre el cumplimiento de sus objetivos y metas. * Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos. * Efectuar seguimiento a los riesgos y controles de cada proceso y proponer las mejoras a que, haya a lugar. * Comunicar deficiencias a la alta dirección o a las partes responsables para tomar las medidas correctivas, según corresponda. |

|  |  |  |
| --- | --- | --- |
| **Segunda Línea** | **Oficina Asesora en el proceso de Planeación** | * Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada. * Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude. * Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar recomendaciones y seguimiento para el fortalecimiento de los mismos. * Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento. * Consolidar los seguimientos a los mapas de riesgo. riesgos, cuando haya lugar. * Proporcionar información sobre los avances y resultados de la gestión institucional y de la gestión del riesgo y proponer acciones de mejora que contribuyan a alcanzar los resultados esperados. * Suministrar información a la alta dirección sobre el monitoreo llevado a cabo a la gestión del riesgo y proponer las acciones de mejora a que haya a lugar. |
| **Tercera Línea** | **Oficina de Control Interno y quien haga sus veces** | * Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa. * Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. * Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. * Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas. * Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción. * Evaluar si los controles son efectivos para mitigar los riesgos institucionales; en caso de identificar debilidades, hacer recomendaciones. * Hacer seguimiento a los planes de mejoramiento y verificar el impacto de los mismos en la mejor de la gestión institucional. * Establecer y mantener un sistema de monitoreado de hallazgos y recomendaciones. |

**Tabla 13:** Roles y responsabilidad en el proceso de monitoreo, seguimiento y evaluación

# 17. BIBLIOGRAFIA

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP, Versión 5, de Diciembre de 2020 y anexos

**AUTORIZACIONES:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **NOMBRE** | **CARGO** | **FIRMA** |
| **Elaboró** | Javier José Salinas Acosta | Profesional Asesor | **Acta del Comité Institucional de Coordinación de Control Interno** |
| **Revisó y Aprobó** | Comité Institucional de Coordinación de Control Interno | |