

***POLITICA DE LA ADMINISTRACION DEL RIESGO DE LA BIBLIOTECA PÚBLICA PILOTO***

***2019***

**Código**

**Versión**

**Fecha**

**PT-GE-01**

**2**

**30/03/2019**

|  |
| --- |
|  |
| ***Manual para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital en la Biblioteca Pública Piloto*** |



**TABLA DE CONTENIDO**

[1 PRESENTACION 3](#_Toc4694941)

[2 MARCO LEGAL 4](#_Toc4694942)

[3 CONTEXTO DE LA ENTIDAD 5](#_Toc4694943)

[4 METODOLOGIA DE ADMINISTRACIÓN DEL RIESGO 6](#_Toc4694944)

[5 POLITICA DE ADMINISTRACIÓN DEL RIESGO: 7](#_Toc4694945)

[*5.1POLITICA DE ADMINISTRACION DE RIESGOS DE LA BIBLIOTECA PÚBLICA PILOTO:*](#_Toc4694946) 8

[*5.2 OBJETIVO*](#_Toc4694947) 9

[5.2.1Objetivo General](#_Toc4694948) 9

[5.2.2Objetivos Específicos](#_Toc4694949) 9

[5.2.3Alcance 10](#_Toc4694950)

[*5.3* *ESTRATEGIAS* 10](#_Toc4694951)

[*5.4* *RIESGOS QUE SE VAN A CONTROLAR* 11](#_Toc4694952)

[5.5 ESTRUCTURA PARA LA GESTIÓN DEL RIESGO: 13](#_Toc4694953)

[*5.6* *ACCIONES A DESARROLLAR* 13](#_Toc4694954)

[*5.7* *SEGUIMIENTO Y EVALUACIÓN A LA IMPLEMENTACION DE LA POLITICA* 19](#_Toc4694955)

[6 IDENTIFICACIÓN DE RIESGOS: 20](#_Toc4694956)

[6.1 CAUSAS Y CONSECUENCIAS 23](#_Toc4694957)

[**6.1.1**Identificación del Riesgo de corrupción**:** 24](#_Toc4694959)

**7 VALORACIÓN DE RIESGOS…**…………..………………………………………………..26

7.1 ANÁLISIS DE RIESGOS……………………..………………………………………26

7.2 CRITERIOS PARA VALORACIÓN DE RIESGOS…………………..………….27

7.3 EVALUACIÓN DE RIESGOS**……………………………….……………….………33**

7.3.1 DISEÑO DE CONTROLES…………………………………………………….34

7.3.2 PASOS PARA DISEÑAR LOS CONTROLES…..……………….………..….34

7.3.3. VALORACIÓN DE LOS CONTROLES………………………..………………36

[**7.4Tratamiento:……………………………………………………………………………..**3](#_Toc4694960)7

[8. PLAN DE TRATAMIENTO DE RIESGO](#_Toc4694961) 38

[9 MANTENIMIENTO Y SOSTENIBILIDAD DEL PROCESO DE ADMINISTRACIÓN DEL RIESGO](#_Toc4694962) 38

[9.1 La alta dirección deberá liderar el proceso de administración de riesgos de la Biblioteca Pública Piloto,](#_Toc4694963) 38

[9.2 El Comité de Coordinación de Control Interno aprobará las políticas generales de administración de riesgos y las políticas particulares para tratar los riesgos](#_Toc4694964) …………………………………………………..................................39

[9.3 Los responsables de los procesos serán los responsables de la dirección, implementación y el cumplimiento de las acciones, controles y mecanismos de evaluación de la efectividad en el manejo de los riesgos.](#_Toc4694965) 39

[9.4 Cada área designará los responsables para desarrollar e implementar las técnicas, metodologías y acciones para administrar el riesgo de acuerdo con las orientaciones que imparta la Oficina de Control Interno. 3](#_Toc4694966)9

[9.5 Los servidores públicos de la Entidad serán responsables de la reducción de los riesgos y de velar por la eficacia de los controles integrados en los procesos, actividades y tareas a su cargo. 3](#_Toc4694967)9

[10. RECURSOS](#_Toc4694968) 40

[11. COMUNICACIÓN Y CONSULTA](#_Toc4694969) 40

[12. INCUMPLIMIENTO DE LA POLITICA](#_Toc4694970) 40

[12. REGISTRO DE LA ADMINISTRACION DEL RIESGO](#_Toc4694971) 40

[13. ANEXOS](#_Toc4694972) 40

[14. BIBLIOGRAFIA](#_Toc4694973) 41

# **PRESENTACION**

La administración de riesgos como parte esencial de la gestión estratégica de la Biblioteca Pública Piloto de Medellín para América Latina, es el proceso mediante el cual, se tratan los riesgos relacionados con los objetivos de la entidad y sus procesos, con el fin de obtener un beneficio sostenido en cada uno de ellos y en su conjunto, de tal forma que se potencie la capacidad institucional para cumplirlos satisfactoriamente.

La gestión de riesgos debe ser un proceso continuo y en constante desarrollo y en su aplicación debe tratar técnicamente todos los riesgos que rodeen a las actividades pasadas, presentes y, sobre todo, futuras, desde los ámbitos de la Gestión, la Corrupción y la Seguridad digital.

En atención a la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, expedida por el Departamento Administrativo de la Función Pública en octubre de 2018 Versión 4, que busca unificar la gestión de todos los tipos de riesgos bajo un solo instrumento; Se adopta la presente actualización de la Política de Administración del Riesgo de la Biblioteca Pública Piloto.

El cambio conlleva a la actualización de la Política de Administración del riesgo, con el fin de hacer más sencilla la utilización de esta herramienta, manejar un solo instrumento y avanzar en la implementación de los lineamientos dispuestos en el Modelo Integrado de Planeación y Gestión (MIPG) formalizado en octubre de 2017.

# **MARCO LEGAL**

* En la Ley 87 de 1993, se encuentra el concepto de riesgos, al establecer como uno de los objetivos del control interno en el artículo 2 literal a) “proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan”. También el literal f) expresa: “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”.
* El 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 entidades y organismos del Estado establece:

Artículo 3. **De las Oficinas de Control Interno.** En desarrollo de las funciones señaladas en el artículo 9 de la Ley 87 de 1993, el rol que deben desempeñar las oficinas de control interno, o quien haga sus veces, dentro de las organizaciones públicas, se enmarcan en cinco tópicos, a saber: valoración de riesgos, acompañar y asesorar, realizar evaluación y seguimiento, fomentar la cultura de control, y relación con entes externos.

Artículo 4. **Administración de Riesgos.** Como parte Integral del fortalecimiento de los sistemas de control interno en las entidades públicas, las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas del control interno o quien haga sus veces evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetos organizacionales con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas y las oficinas de control interno e integradas de manera inherente a los procedimientos”.

# **CONTEXTO DE LA ENTIDAD**

El documento CONTEXTO DE LA BPP, determina el contexto general de la entidad, su complejidad, procesos, planeación institucional, entre otros aspectos, permitiendo conocer y entender la entidad, y su entorno. Este insumo permite el análisis de riesgos y la aplicación de la metodología en general.

El contexto establece el modelo de operación por procesos y hace relación a los instrumentos que definen la planeación institucional y los diferentes planes que desarrolla la Entidad en el marco de la Normatividad aplicable.

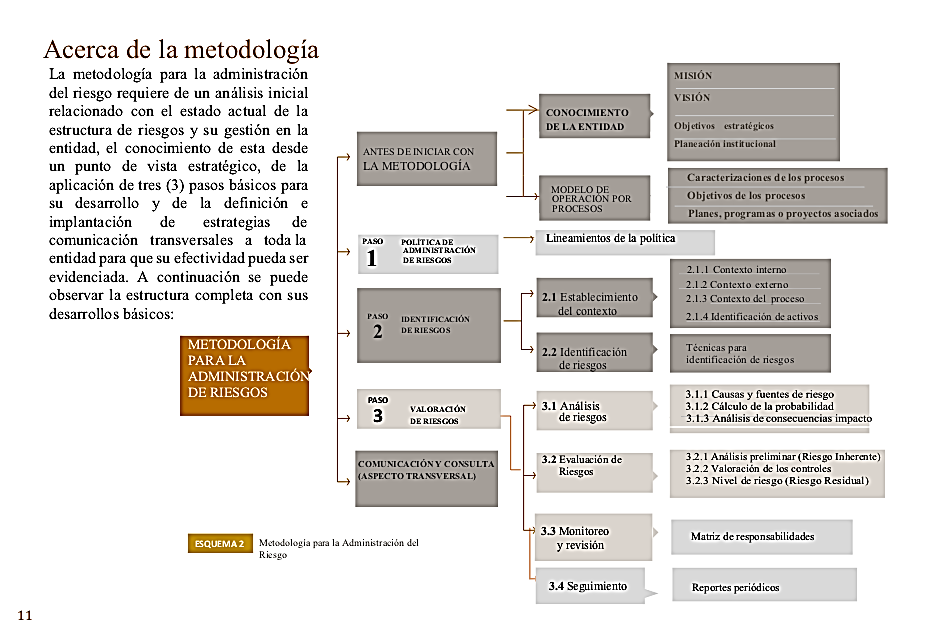
La planeación institucional se relaciona igualmente en cada una de las caracterizaciones de los procesos, desde los cuales se identifican los riesgos que atenten contra el cumplimiento de estos.

Las Directrices estratégicas como Misión, Visión, la Política del SIG y los objetivos estratégicos se identifican en el Plan Estratégico, como guías para dirigir los recursos y esfuerzos para dar cumplimiento al mandato legal aplicable a cada entidad.

**ESQUEMA 1**

# **METODOLOGIA DE ADMINISTRACIÓN DEL RIESGO**

Consiste en la aplicación de tres pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales. A continuación, se puede observar la estructura completa con sus desarrollos básicos:



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

Función pública octubre de 2018.

Los riesgos de la Biblioteca estarán determinados por los lineamientos de la Guía para la Administración del Riesgo V4 2018. En este sentido, los riesgos estarán clasificados por riesgos institucionales incluye los de corrupción y los riesgos de los procesos.

Anualmente se llevarán acciones para actualizar el contexto de la entidad, teniendo en cuenta los aspectos internos, externos y de los procesos que afectan el cumplimiento de los riesgos de gestión, de corrupción y de seguridad digital, seguirán los lineamientos establecidos en el documento Guía para la Gestión del Riesgo de Corrupción de la Secretaría de la Transparencia de la presidencia de la República y los lineamientos para los riesgos de Gestión que establece el Departamento Administrativo de la Función Pública (DAFP):

* Se analizará anualmente el contexto interno y externo, para la adecuada definición de los riesgos, este ejercicio se realizará por parte de la oficina de planeación la cual definirá la metodología a trabajar para definir el contexto.
* La oficina Asesora de Planeación en el primer trimestre del año diseñara una estrategia para la implementación de la política de Riesgos, definiendo un cronograma para la ejecución de las actividades.
* La oficina Asesora de Planeación revisara en el último trimestre del año, el estado institucional de la gestión de riesgos, la metodología y el nivel de la implementación de la política de administración de riesgos para tomar acciones que garanticen el mejoramiento de la efectividad de la organización.
* Elaborar anualmente informes generales de la gestión de riesgos, la metodología y el nivel de implementación de la política de administración de riesgos a nivel institucional para la dirección general.
* Los responsables de entregar las evidencias de los controles de los riesgos propuestos en el mapa de riesgos lo enviaran en las fechas programadas por la Subdirección de Planeación, mediante circular emitida cada año.

# **POLITICA DE ADMINISTRACIÓN DEL RIESGO:**

## ***POLITICA DE ADMINISTRACION DE RIESGOS DE LA BIBLIOTECA PÚBLICA PILOTO:***

La política de Administración del Riesgo de la Biblioteca Pública Piloto (BPP) de Medellín, hace parte de los compromisos que la alta dirección, en cabeza de la Dirección de la entidad, establecen para garantizar que la toma de decisiones en el entidad conlleve al cumplimiento de los objetivos estratégicos e institucionales y sectoriales, de manera transparente y en cumplimiento de la ley.

En este sentido la responsabilidad de la administración del riesgo buscará la mejora continua en la toma de decisiones, lo que conllevará al cumplimiento de los objetivos de la entidad, la misión institucional y la satisfacción de la comunidad.

La Biblioteca Pública Piloto, se compromete a controlar todos aquellos riesgos que pueden impedir el cumplimiento del direccionamiento estratégico, mediante una efectiva administración de los mismos, como herramienta de gestión que responda a las tendencias organizacionales actuales, considerando que:

Todos los líderes de procesos serán los responsables de la gestión de los riesgos identificados en su proceso de gestión.

Para identificar los riesgos, se deberá tener en cuenta el objetivo del proceso, el contexto estratégico y los factores de contexto externo, interno y de proceso.

Para evaluar el impacto de los riesgos, los líderes de los procesos tomarán como guía la tabla propuesta por el Departamento Administrativo de la Función Pública versión 2018, teniendo en cuenta las particularidades de la Biblioteca Pública Piloto, en cuanto a su misión, recursos humanos, físicos y financieros.

Los procesos de gestión de la entidad reportarán a Planeación, el mapa de riesgos que contendrá todos los riesgos organizacionales identificados en el proceso incluyendo los riesgos de corrupción y de Seguridad Digital.

Desde Planeación, se diseñará el mapa de riesgos institucional con los riesgos organizacionales calificados en zona: Catastrófico, alto, moderado, insignificante, y los riesgos de corrupción, a partir de los mapas de riesgos reportados por cada proceso.

Cada líder de proceso será responsable de realizar monitoreo y control a los riesgos, mediante la ejecución del plan de acción para prevenir y mitigar los mismos, propendiendo por gestionar los riesgos hacia un nivel aceptable y teniendo en cuenta que los riesgos de corrupción son inaceptables.

El plan de acción se debe evaluar anualmente para realizar las modificaciones de los riesgos residuales a que haya lugar, sin embargo, la periodicidad para el seguimiento se realizará trimestralmente.

Desde la oficina de Control Interno, se realizará el seguimiento a los controles existentes y al plan de mitigación de los riesgos residuales de cada proceso y de corrupción durante las auditorías. Emitiendo las recomendaciones que correspondan, lo cual se reportará al Comité Institucional de Coordinación de Control Interno

## ***OBJETIVOS***

### Objetivo General

Establecer el procedimiento y la Política para la administración de los riesgos de la Biblioteca Pública Piloto, generando un esquema estructurado, consistente y continuo para la contextualización, identificación, análisis, valoración, tratamiento y manejo de los riesgos desde cada proceso. Permitiendo orientar a los responsables acerca de las acciones para su manejo en forma efectiva, con el fin de minimizar su ocurrencia y afectación al logro de los objetivos estratégicos, la misión institucional y proteger los recursos que se encuentren bajo la custodia y administración de la Entidad.

### Objetivos Específicos

* Asegurar que se desarrollen cada una de las etapas previstas para la actualización e implementación del mapa de riesgos de la entidad, dentro del marco de la política del componente de la Administración del Riesgo de la Biblioteca.
* Generar una visión sistémica acerca de la administración y evaluación de riesgos a partir de un Direccionamiento Estratégico adecuados, que fundamenten el desarrollo de las Actividades de Control.
* Proteger los recursos de la Entidad, resguardándolos contra la materialización de los riesgos.
* Introducir dentro de los procesos y procedimientos de la Biblioteca, las acciones de control resultado de la administración del riesgo.
* Involucrar y comprometer a los servidores públicos de la BPP, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos. Con el fin de facilitar y fortalecer el desarrollo de la entidad, manteniendo la buena imagen y las buenas prácticas; reconociendo la necesidad de identificar y tratar los riesgos en todos los procesos.
* Garantizar la confiabilidad y oportunidad de la información conforme al direccionamiento estratégico Institucional.
* Asegurar el cumplimiento de normas, leyes y regulaciones
* Propiciar el desarrollo efectivo de las actividades misionales en beneficio de la comunidad.

### Alcance

La Política de la Administración de Riesgos de la BPP, será prioritaria y estratégica, fundamentada en el mapa de procesos institucional, La administración de riesgos es aplicable a todos los procesos de la entidad.

En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información.



## ***ESTRATEGIAS***

Las estrategias para establecer cómo se van a desarrollar a largo, mediano y corto plazo, la política de Administración de Riesgo.

* Instituir metodologías para la Administración del Riesgo en la Entidad, de acuerdo a las requeridas vigentes por el MIPG.
* Identificar y precisar mecanismos de comunicación y divulgación de la Política de administración del riesgo en todos los niveles de la Entidad.

* Capacitar y acompañar para el desarrollo del enfoque de administración del riesgo en las actividades diarias.
* Hacer seguimiento a los riesgos más críticos en los procesos de la Biblioteca, la periodicidad para el seguimiento se realizará de acuerdo a lo establecido en la circular emitida por la Subdirección de Planeación.

## ***RIESGOS QUE SE VAN A CONTROLAR***

**Tipología de riesgos en la Biblioteca Pública Piloto:**

De acuerdo a la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se han identificado los siguientes tipos de riesgos: De proceso, institucionales y de corrupción.

* ***Riesgo Estratégico:*** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad.
* ***Riesgos de Imagen:*** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
* ***Riesgos Operativos:*** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

* ***Riesgos Financieros:*** Se relacionan con el manejo de los recursos de la 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. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.
* ***Riesgos 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.
* ***Riesgos de Tecnología:*** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión. Se asocian con la infraestructura tecnológica e informática (hardware y Software) que soportan las operaciones de la Entidad.
* ***Riesgos de corrupción:*** La posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
* ***Riesgos naturales/medioambientales***: relacionado con los daños que pueden producirse al entorno, ya sea propios de la naturaleza o provocados por el ser humano. cambio climático, contaminación, gestión de residuos.
* ***Riesgos laborales****: relacionados a los peligros existentes en nuestra tarea laboral o en nuestro propio entorno o lugar de trabajo, que puede provocar accidentes físicos, químicos, biológicos, ergonómicos, psicosociales.*
* ***Riesgo contractual:*** Se refiere al riesgo que corren los administradores de una compañía por no manejar en forma apropiada, los riesgos a nivel social, de gobernabilidad o de contratación por prestación de servicios, que pueden conducir a demandas legales u otras soluciones judiciales.
* ***Riesgos de información****: se asocia a la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la información agregada y desagregada.*
* ***Riesgos de seguridad digital:*** *Posibilidad 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.*

## **ESTRUCTURA PARA LA GESTIÓN DEL RIESGO:**

Determina los siguientes aspectos:

* La metodología a utilizar se basa en los lineamientos establecidos en el Manual de los riesgos de Gestión, de Corrupción y de Seguridad Digital, versión No 4, de octubre de 2018, la cual establece los pasos a seguir para implementación, tratamiento y seguimiento del mapa de riesgos a través del control de las actividades programadas para minimizar los riesgos.
* En el caso de los Riesgos de Seguridad Digital, la entidad debe asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Para su aplicación, la Entidad cuenta con el software XENCO, como herramienta para la ejecución financiera de los recursos físicos de la entidad, y, el software JANIUM, para realizar, **búsquedas de información con distintos niveles de complejidad** tanto en las colecciones propias de la institución como en otros recursos externos, a través de diferentes métodos y protocolos, permite llevar a cabo la **gestión de servicios útiles para los usuarios**.

* La periodicidad para el monitoreo y revisión de los riesgos, así como el seguimiento de los riesgos de corrupción se definen en el numeral 5.7
* Incluir los niveles de riesgo aceptado para la entidad y su forma de manejo.
* Incluir la tabla de impactos institucional (Ver Tabla Ilustrativa 3. Niveles para calificar el impacto o consecuencias, pág. 31).

## ***ACCIONES A DESARROLLAR***



**Niveles para Calificar el Impacto:** Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos). Ver Tabla Ilustrativa 3. Criterios para calificar el Impacto pág. 31

La política identifica las opciones institucionales para tratar y manejar los riesgos basándose en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración de riesgos, a su vez transmite la posición de la dirección y establece las guías de acción necesarias a todos los servidores de la Biblioteca Pública Piloto.

Para tratar y manejar los riesgos se deben tener en cuenta las siguientes opciones de manejo, las cuales pueden considerarse de manera independiente, interrelacionadas o en conjunto.

* ***Evitar el riesgo:*** tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

*Acciones a Desarrollar:*

* ***Implementación de controles:*** Es la principal opción considerada; *los controles de tipo preventivo expresados en políticas*, estrategias y lineamientos, han sido clasificados en generales y específicos para los efectos alusivos a la administración del riesgo.

Los primeros, dirigidos y orientados al cumplimiento de la gestión institucional; mientras que los segundos, son lineamientos concretos para la ejecución de los procesos; respecto a los de origen externo, es exigible su cumplimiento.

* ***Modelo de gestión ética:*** El fortalecimiento de una cultura de gestión ética fundamentada en un código de integridad adoptado, ha sido una de las principales estrategias abordadas a fin de que los servidores se comprometan en la aplicación de prácticas y formas concretas de actuación que permitan minimizar toda clase de riesgos en el desarrollo de sus funciones.
* ***Programas de mantenimiento preventivo para equipos:***programas de mantenimiento preventivo y correctivo para equipos y bienes como son el de la infraestructura tecnológica de la información de material y documentos bibliográficos y patrimoniales, software administrativo, equipos de cómputo, sistemas de información, plantas eléctricas, aires acondicionados, entre otros.

De igual manera, al realizar la evaluación de los procesos, la Oficina de Control Interno establecerá si se están aplicando los controles, así como su efectividad en el manejo de los riesgos identificados en éstos, a fin de sugerir correctivos e iniciar acciones periódicas de mejoramiento, respecto a la administración del riesgo de la entidad.

* ***Reducir el riesgo:*** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

**Véase** Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.)

<https://tienda.icontec.org/wp-content/uploads/pdfs/GTC137.pdf>

*Acciones a desarrollar*

* ***Optimización de los procedimientos:*** Propuestas de mejoras o cambios a los procesos y procedimientos existentes, o la formulación de nuevos.

Caracterizar el perfil de los usuarios o destinatarios de los servicios que presta la BPP, así como el perfil de los proveedores potenciales de los insumos, bienes y servicios requeridos para el funcionamiento institucional.

Obtener información de los usuarios, destinatarios o beneficiarios acerca de las necesidades y expectativas, problemas e inconformidades relacionados con la prestación de los servicios y el cumplimiento de las funciones asignadas.

Identificar y priorizar los procesos misionales o estratégicos y evaluar su funcionamiento.

Determinar los criterios y métodos necesarios para la medición de los resultados de la gestión a cargo de las dependencias y áreas misionales.

Identificar y evaluar, con la activa participación de sus servidores públicos, aquellos factores externos y los riesgos de mayor ocurrencia que puedan llegar a incidir de manera negativa en los resultados de la gestión.

* ***Fortalecimiento del ejercicio del autocontrol:*** La importancia radica, en que cada servidor, independientemente de su nivel jerárquico, tenga la capacidad de evaluar su trabajo, detectar desviaciones, efectuar correctivos, mejorar y solicitar ayuda cuando lo considere necesario, para que la ejecución de los procesos, actividades y tareas bajo su responsabilidad, garanticen el ejercicio de una función administrativa transparente y eficaz, la Oficina de Control Interno de la entidad, promueve su práctica.
* ***Fortalecimiento del ejercicio de la autoevaluación de la gestión:*** Al medir cada proceso, la efectividad y los resultados de su gestión en tiempo real, verificar su capacidad para cumplir con las metas, a fin de tomar las medidas correctivas que sean necesarias para el cumplimiento de los objetivos institucionales, se está fortaleciendo y aplicando este principio del Sistema de Control Interno en la entidad; es así como periódicamente se desarrollan reuniones de reflexión y evaluación de la gestión de los diferentes procesos, con el propósito de tomar decisiones relacionadas con el mejoramiento de su desempeño.
* ***Compartir o transferir el riesgo:*** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

*Acciones a desarrollar*

Cierta clase de riesgos identificados por las dependencias no aparecen en el mapa de riesgos institucional, en razón a que se consideraron únicamente aquellos que afectaran específicamente el objetivo de los procesos.

Sin embargo y teniendo en cuenta que hay una serie de eventos que indirectamente influyen en el desarrollo de la gestión, ante cualquier clase de afectación que se presente en los servidores, como en los bienes de su propiedad, su tratamiento parte del establecimiento apropiado de una estrategia que saque del escenario institucional estos riesgos asegurables, cubriéndolos mediante el uso adecuado de pólizas y garantías.

* ***Asumir un riesgo:*** luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

*Acciones a Desarrollar*

Para tal fin, se contemplan las siguientes acciones que deben ser adoptadas en el corto y mediano plazo:

* Estructuración de criterios orientadores, respecto al tratamiento de los riesgos residuales y sus efectos en la gestión institucional.
* Programas de sensibilización del mapa de riesgos institucional, como del plan del manejo de los riesgos, dirigido a todos los servidores públicos.
* Convocar a los servidores públicos a aplicar los lineamientos establecidos para la administración del riesgo y a su participación activa para la aprehensión de las nuevas prácticas propuestas, que exigen valores y principios éticos, calidad en la información generada y compartida, decisiones oportunas y eficaces, así como racionalidad en los recursos.

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser *factibles y efectivas*, y pueden ser entre otras: la implementación de nuevos controles que no existen, revisar y ajustar los controles existentes no efectivos, documentar controles, divulgar las acciones de control y entrenar o capacitar para su aplicación de ser necesario, comunicar las políticas, definir estándares, optimizar procesos y procedimientos incorporando mejores prácticas de entidades o procesos similares o realizar cambios físicos.

La selección de las acciones más convenientes debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica y se puede realizar con base en los siguientes criterios:

* La valoración del riesgo a manejar
* El balance entre el costo de la implementación de cada acción contra el beneficio de la misma.
* El balance entre el valor del beneficio esperado versus el riesgo de no emprender acción.

Para la ejecución de las acciones, se deben identificar las áreas o dependencias responsables de llevarlas a cabo, *definir un cronograma* y *unos indicadores* que permitan realizar el seguimiento y verificar el cumplimiento para tomar medidas correctivas cuando sea necesario, todo esto siguiendo los procedimientos y formatos para documentar acciones de mejora.

Al final los resultados deberán obtener los beneficios registrados en la Norma Técnica Colombiana NTC-ISO31000:

* Aumentar la probabilidad de alcanzar los objetivos.
* Fomentar la gestión proactiva.
* Cumplimiento de los requisitos legales y reglamentarios.
* Mejorar los controles.
* Usar eficazmente los recursos.
* Mejorar la prevención de pérdidas y la gestión de incidentes.
* Establecer una base confiable para la toma de decisiones y la planificación.

**NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO**: Establece “los niveles aceptables de desviación relativa a la consecución de los objetivos” (NTC GTC 137 Numeral 3.7.16), los mismos están asociados a la estrategia de la entidad y pueden considerarse para cada uno de los procesos.

Los riesgos de corrupción son inaceptables.

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo.

Los riesgos aceptados están sujetos a monitoreo.

## ***SEGUIMIENTO Y EVALUACIÓN A LA IMPLEMENTACION DE LA POLITICA***

* *¿Quién realiza el seguimiento y la evaluación?*

El seguimiento a los diferentes riesgos será responsabilidad de los líderes del proceso y el responsable de la oficina de Control Interno. Este se hará trimestralmente y se entregará a la Subdirección de planeación, para garantizar la trazabilidad, y eficacia del tratamiento de los riesgos.

* *¿Cómo se hace el seguimiento y la evaluación?*

Cada proceso deberá:

* Como mínimo realizar un ejercicio de actualización del mapa de riesgos una vez al año y establecer si continúa con los riesgos formulados, o si es necesario reformular los riegos o adicionar otros riesgos que considere importantes para el control del objetivo del proceso.
* Revisar los registros de ocurrencia de los riesgos cuatro (4) veces al año, es decir, en abril, julio, octubre y a finales de diciembre, para tomar las acciones correctivas pertinentes.

El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión del MIPG de “Control interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

|  |  |  |
| --- | --- | --- |
| 1 ª. L Í N E A D E D E F E N S A | 2 ª. L Í N E A D E D E F E N S A | 3ª. L Í N E A D E D E F E N S A |
| Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. | Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende | Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa |

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

# 

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

Función pública octubre de 2018.

# **IDENTIFICACIÓN DE RIESGOS:**

Al iniciar la etapa de identificación de riesgos se utilizó herramientas y técnicas de trabajo con el equipo humano de la BPP, como lo son:

* Realizar talleres de trabajo por procesos con responsables de estos, para la identificación de riesgos.
* Análisis y definición de objetivos: Le corresponde a la Segunda Línea de Defensa, el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos
* Análisis de objetivos estratégicos: analizar los objetivos estratégicos, su despliegue estratégico e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.
* Análisis de los objetivos de proceso: Analizar el despliegue estratégico desde la Misión a los Objetivos de procesos, asegurando que los objetivos de proceso contribuyan a los objetivos estratégicos.
* ESTABLECIMIENTO DEL CONTEXTO CÒDIGO F-GE-04 Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. Se debe establecer revisar el contexto interno, externo de la entidad y el contexto del proceso y sus activos de seguridad digital. Pueden establecerse un contexto particular al que se enfrentan los procesos ante los riesgos de corrupción.

|  |  |
| --- | --- |
| **ANALISIS DE CONTEXTO** | |
| **CONTEXTO** | **CONDICIONES DE CONTEXTO** |
| CONTEXTO EXTERNO | **Político**s: cambios de gobierno, regulación, legislación |
| **Económicos y financieros:** disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. |
| **Sociales y culturales:** 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:** Normatividad externa (leyes, decretos, ordenanzas y acuerdos). |
| CONTEXTO INTERNO | **Financieros**: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. |
| **Personal:** competencia del personal, disponibilidad del personal, seguridad y salud en el trabajo. |
| **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 DE 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 de activos de seguridad de la información: Le corresponde a la primera línea de defensa, realizar la identificación de activos en cada proceso. tales como (aplicaciones de la organización, servicios web, redes, información física o digital, bases de datos tecnologías de información -TI-, tecnologías de operación - TO-) que utiliza la organización para funcionar en el entorno digital. Así́ la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento tanto interno como su funcionamiento de cara al ciudadano, aumentando así́ su confianza en el uso del entorno digital.
* Acompañar y asesorar a los responsables de los procesos en la implementación del Componente de la Administración del Riesgo, para lograr la identificación de los riesgos de la entidad.
* Trabajar en coordinación con los servidores públicos designados por cada proceso en aquellas actividades requeridas para la consolidación e implementación del mapa de riesgo de la BPP.
* Alcanzar el proceso de consolidación, ajuste e implementación del mapa de riesgos institucional, en el cual se identifiquen los riesgos, definan las acciones que eviten, disminuyan o mitiguen los riesgos identificados e incluir los riesgos de posibles actos de corrupción, proyectando su respectivo control y seguimiento.

## **CAUSAS Y CONSECUENCIAS**

En este proceso es importante que los servidores públicos, contratistas adopten un papel proactivo, en el sentido, que visualicen sus contextos estratégicos y misionales los factores o eventos que pueden afectar el curso institucional, dada la especialidad temática que manejan en cada sector o contexto. Por medio de la capacitación y los formatos que hubiere lugar.

En esta etapa se requiere obtener los siguientes resultados:

* Determinar las causas de las situaciones identificadas como riesgos para la entidad.
* Describir las fuentes del riesgo.
* Precisar los eventos con base en el análisis de contexto para la entidad y del proceso

## Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos, y los institucionales, en el caso de riesgos de corrupción se deben gestionar todos los riesgos, incluyendo los referentes a los trámites y servicios.

¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto

¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo al desarrollo del proceso, la probabilidad de ocurrencia del riesgo.

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

Determinar los posibles efectos por la materialización del riesgo.

**Formato de descripción del riesgo de gestión**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **RIESGO** | **DESCRIPCIÓN** | **TIPO** | **CAUSAS** | **CONSECUENCIAS** |
|  |  |  |  |  |

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

Función pública octubre de 2018.

### Identificación del Riesgo de corrupciónRiesgo de corrupción:

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

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

***Acción u Omisión + Uso del poder +***

***Desviación de la gestión de lo público +***

***El beneficio Privado***

Los riesgos de corrupción se establecen sobre procesos.

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

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

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Matriz definición del riesgo de corrupción** | | | | |
| Descripción del riesgo | Acción u omisión | Uso del poder | Desviar la gestión de lo público | Beneficio privado |
| **Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato** | X | X | X | X |

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

Función pública octubre de 2018.

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

**Formato de descripción del riesgo de corrupción**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | **DESCRIPCIÓN** | **TIPO** | **CAUSAS** | | **CONSECUENCIAS** | | |
|  |  |  |  |  | |  |  | |

**Formato de descripción del riesgo de seguridad digital:**

|  |  |  |  |
| --- | --- | --- | --- |
| **INCLUYE ACTIVO-AMENAZA-VULNERABILIDADES** | | | |
| **R I E S G O** | **ACTIVO** | **D E S C R I P C I Ó N D E L R I E S G O** | **A M E N A Z A** | **T I P O** | **C A U S A S /**  **V U L N E R A ­B I L I D A D E S** | | **C O N S E C U E N C I A S** |
|  |  |  |  |  |  | |  |

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

Función pública octubre de 2018.

**7. Valoración de riesgos**

**7.1Análisis de riesgos:**

De acuerdo con los lineamientos establecidos por el DAFP, se determinan los dos aspectos para el análisis de los riesgos identificados, ***Probabilidad* e *impacto*,** teniendo en cuenta la tabla de valoración para la probabilidad, y las tres (3) tablas de valoración para el impacto, que varían dependiendo del tipo de riesgo que estemos valorando: Gestión, Corrupción, o Seguridad digital.

*Análisis de la probabilidad*

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.

**7.2 CRITERIOS PARA VALORACIÓN DE RIESGOS**

**CRITERIOS PARA CALIFICAR LA PROBABILIDAD:**

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **D E S C R I P TO R** | **D E S C R I P C I Ó N** | **F R E C U E N C I A** |
| 5 | **Casi seguro** | Se espera que el evento ocurra en la mayoría de las circunstancias. | Más de 1 vez al año. |
| 4 | **Probable** | Es viable que el evento ocurra en la mayoría de las circunstancias. | Al menos 1 vez en el último año. |
| 3 | **Posible** | El evento podrá ocurrir en algún momento. | Al menos 1 vez en los últimos 2 años. |
| 2 | **Improbable** | El evento puede ocurrir en algún momento. | Al menos 1 vez en los últimos 5 años. |
| 1 | **Rara vez** | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales). | No se ha presentado en los últimos 5 años |

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

Función pública octubre de 2018

**CRITERIOS PARA CALIFICAR EL IMPACTO DE LOS RIESGOS DE GESTIÓN:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NIVEL** | | **I M PA C T O**  **( C O N S E C U E N C I A S )**  **C U A N T I TAT I V O** | | **I M PA C T O**  **( C O N S E C U E N C I A S )**  **C U A L I TAT I V O** | |
| **CATASTRÓFICO** | | - 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** | | - Impacto que afecte la ejecución presu­puestal en un valor ≥20%.  - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.  - 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. | | - 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.  - 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. | |
| **MENOR** | - 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 pre­supuesto 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.  - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplina­rias.  - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. | |
| **INSIGNIFICANTE** | - 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. | |

**CRITERIOS PARA CALIFICAR EL IMPACTO DE RIESGOS DE SEGURIDAD DIGITAL:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NIVEL** | **VALOR**  **DEL**  **IMPACTO** | **C R I T E R I O S D E I M PACTO**  **PA R A R I ES G O S D E S EGURIDA D D I G I TAL**  **CUANTITATIVO CUALITATIVO** | | | | | | |
| **INSIGNIFICANTE** | 1 | Afectación ≥X% de la población.  Afectación ≥X% del presupuesto anual de la entidad.  No hay afectación medioambiental. | | | Sin afectación de la integridad.  Sin afectación de la disponibilidad.  Sin afectación de la confidencialidad | | | |
| **MENOR** | 2 | Afectación ≥X% de la población.  Afectación ≥X% del presupuesto anual de la entidad.  Afectación leve del medio ambiente requiere de ≥X días de recuperación. | | | Afectación leve de la integridad.  Afectación leve de la disponibilidad.  Afectación leve de la confidencialidad. | | | |
| **MODERADO** | 3 | Afectación ≥X% de la población.  Afectación ≥X% del presupuesto anual de la entidad.  Afectación leve del medio ambiente requiere de ≥X semanas 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. | | | |
|  |  |  | | |  | | | |
| **MAYOR** | 4 | | Afectación ≥X% de la población.  Afectación ≥X% del presupuesto anual de la entidad.  Afectación importante del medio ambiente que requiere de ≥X meses 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. | | |
| **CATASTRÓFICO** | 5 | | | Afectación ≥X% de la población.  Afectación ≥X% del presupuesto anual de la entidad.  Afectación muy grave del medio ambiente que requiere de ≥X 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. |

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

Función pública octubre de 2018

***I M P O R TA N T E***

Cada entidad deberá adaptar los criterios a su realidad.

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

Una vez establecido los criterios de valoración probabilidad Vs Impacto, se define el nivel del riesgo en el mapa de calor.

**Mapa de calor**

Se toma la calificación de probabilidad resultante de la tabla *“Matriz de priorización de probabilidad”*, *y la calificación de Impacto de acuerdo a las tablas de valor.*

Ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo.



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

Función pública octubre de 2018

**CRITERIOS PARA CALIFICAR EL IMPACTO DE LOS RIESGOS DE CORRUPCIÓN:**

|  |
| --- |
|  |
| **PREGUNTA :**  **S I E L R I E S G O D E C O R R U P C I Ó N S E**  **M AT E R I A L I Z A P O D R Í A . . .** | | **RESPUESTA** | | |
| **S Í** | | **N O** |
| **1** | ¿Afectar al grupo de funcionarios del proceso? | X | | |
| **2** | ¿Afectar el cumplimiento de metas y objetivos de la dependencia? | X | | |
| **3** | ¿Afectar el cumplimiento de misión de la entidad? | X | | |
| **4** | ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad? | X | | |
| **5** | ¿Generar pérdida de confianza de la entidad, afectando su reputación? | X | | |
| **6** | ¿Generar pérdida de recursos económicos? | X | | |
| **7** | ¿Afectar la generación de los productos o la prestación de servicios? | X | | |
| **8** | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos? | X | | |
| **9** | ¿Generar pérdida de información de la entidad? | X | | |
| **10** | ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente? | X | | |
| **11** | ¿Dar lugar a procesos sancionatorios? | X | | |
| **12** | ¿Dar lugar a procesos disciplinarios? | X | | |
| **13** | ¿Dar lugar a procesos fiscales? | X | | |
| **14** | ¿Dar lugar a procesos penales? | X | | |
| **15** | ¿Generar pérdida de credibilidad del sector? | X | | |
| **16** | ¿Ocasionar lesiones físicas o pérdida de vidas humanas? | X | | |
| **17** | ¿Afectar la imagen regional? | X | | |
| **18** | ¿Afectar la imagen nacional? | X | | |
| **19** | ¿Generar daño ambiental? | X | | |
| ***Una vez, diligenciadas las 19, respuestas, se cuenta el número de preguntas que se respondieron con “SI” y el número de preguntas que se respondieron con “NO”***  ***Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado.***  ***Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.***    ***Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.*** | | **10** | | |
| ***MODERADO*** | | ***Genera medianas consecuencias sobre la entidad*** | | |
| ***MAYOR*** | | ***Genera altas consecuencias sobre la entidad.*** | | |
| ***CATASTRÓFICO :*** | | ***Genera consecuencias desastrosas para la entidad*** | | |

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

Función pública octubre de 2018

**7.3 Evaluación de riesgos:**

Una vez ubicados los riesgos en la matriz de priorización, se identifica las causas, consecuencias, controles existentes documentados con el fin de determinar la posición del riesgo en la matriz de vulnerabilidad

Con la participación de los Servidores Públicos, identificar los puntos de control existentes en los diferentes procesos, los cuales permitan obtener información para efectos de la toma decisiones y para la evaluación de los riesgos.

Con la realización de esta etapa se busca que la Biblioteca Pública Piloto, obtenga los siguientes resultados:

* Identificación de los controles existentes para los riesgos identificados y analizados.
* Priorización de los riesgos de acuerdo con los resultados obtenidos de confrontar la evaluación del riesgo con los controles existentes, a fin de establecer aquellos que pueden causar mayor impacto a la entidad en caso de materializarse.

Es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas.

**7.3.1. DISEÑO DE CONTROLES:**

Antes de valorar los controles es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes:

**¿Cómo defino o establezco un control para que en su diseño mitigue de manera adecuada el riesgo?**

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

***7.3.2. Pasos para diseñar un control***

***VARIABLES***

***A EVALUAR PARA EL***

***ADECUADO DISEÑO***

***DE CONTROLES***

***VARIABLES***

***A EVALUAR PARA EL***

***ADECUADO DISEÑO***

***DE CONTROLES***

## 

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

Función pública octubre de 2018

## **7.3.3. VALORACIÓN DE LOS CONTROLES:**

Para valorar los controles, que permitan mitigar los riesgos, se debe tener en cuenta lo siguiente:

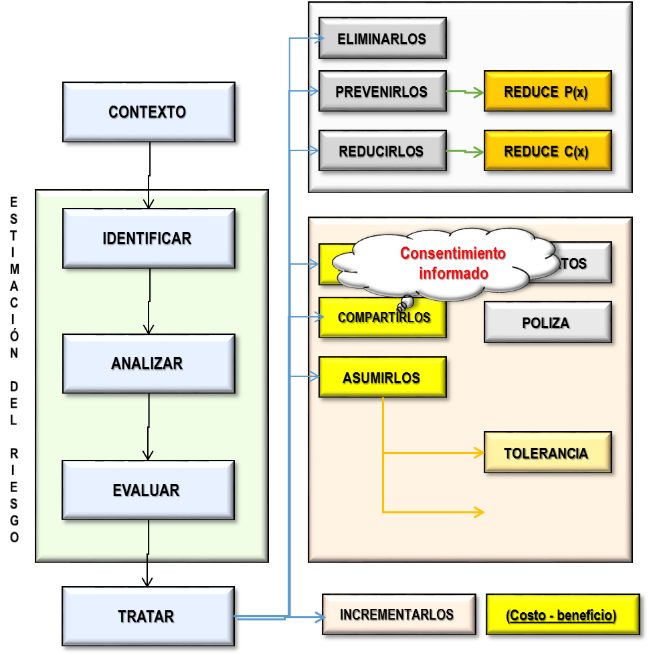
* El control debe estar bien diseñado para controlar el riesgo.
* Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecu­tarse por parte de los responsables tal como se diseñó.
* El control se ejecuta como fue DISEÑADO Y DE MANERA CONSISTENTE

Análisis y evaluación de los controles para la mitigación de los riesgos.

|  |
| --- |
|  |
| **C R I T E R I O**  **D E**  **E VA LUA C I Ó N** | **A S P E C T O A**  **E VA LUA R**  **E N E L D I S E Ñ O**  **D E L C O N T R O L** | **O P C I O N E S**  **D E R E S P U E S TA** | | | |
| **1. Responsable** | ¿Existe un responsable asignado a la ejecu­ción del control? | Asignado | | No asignado | |
| ¿El responsable tiene la autoridad y adecua­da segregación de funciones en la ejecución del control? | Adecuado | | | Inadecuado |
| **2. Periodicidad** | ¿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 | |
| **3. Propósito** | ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, compa­rar, revisar, etc.? | Prevenir  o detectar | | No es un control | |
| **4. Cómo se realiza la actividad de control** | ¿La fuente de información que se utiliza en el desarrollo del control es información confia­ble que permita mitigar el riesgo? | Confiable | | No confiable | |
| **5. Qué pasa con las observaciones o desviaciones** | ¿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. | |
| **6. Evidencia de la ejecución del control** | ¿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 | |

## **7.4Tratamiento:**

Es la preparación e implementación de los planes para el tratamiento del riesgo, las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener; los responsables de aprobar el plan y los responsables de implementarlo; acciones propuestas; requisitos de recursos, incluyendo las contingencias; medidas y restricciones de desempeño; requisitos de monitoreo y reporte; y tiempo y cronograma.



Tomado: Norma Técnica Colombiana NTC-ISO 31000

Las opciones para el tratamiento pueden incluir las siguientes: Evitar el riesgo; Incrementar el riesgo para perseguir una oportunidad; Retirar una fuente de riesgos: Cambiar la probabilidad; Cambiar la consecuencia: Compartir el riesgo con una o varias partes; Retener el riesgo mediante unas decisiones informada.

* *Elaboración del Mapa de Riesgo:* De acuerdo con los lineamientos establecidos por el DAFP, cuadro resumen que muestre cada uno de los pasos llevados a cabo para su levantamiento. Todas las acciones contempladas dentro del mapa, unido a la información reportada por los indicadores, suministrará la información requerida para el seguimiento respectivo a los mapas.

# **8. PLAN DE TRATAMIENTO DE RIESGO**

El Mapa de riesgo de la Biblioteca Pública Piloto, se organiza de acuerdo con el mapa de procesos vigente, y se hace un análisis para identificar:

* Número de riesgos identificados por proceso.
* Tipo o clasificación de riesgo, para analizar en cual parte de la estructura de la entidad se encuentra la dificultad, para tomar medidas al respecto y luego del seguimiento y monitoreo, revisar el mejoramiento en la gestión.
* La zona de riesgo en que se encuentra cada uno de procesos, para que la Oficina de Control Interno, haga el monitoreo y seguimiento respectivo.

# **MANTENIMIENTO Y SOSTENIBILIDAD DEL PROCESO DE ADMINISTRACIÓN DEL RIESGO**

La definición de procedimientos y acciones correctivas y preventivas, basados en los resultados de evaluación y monitoreo, permitirán lograr el mejoramiento continuo y la sostenibilidad del proceso de administración del riesgo a nivel institucional.

La Oficina de Control Interno, comunicará y presentará los resultados y propuestas de mejoramiento y tratamiento de las situaciones detectadas con respecto a los riesgos institucionales, lo cual llevará a tomar decisiones necesarias para la corrección de las desviaciones que se presenten frente a los objetivos y metas planteadas.

# 9.1 La alta dirección deberá liderar el proceso de administración de riesgos de la Biblioteca Pública Piloto, acorde con la legislación vigente aplicable y la normatividad interna.

## El Comité de Coordinación de Control Interno aprobará las políticas generales de administración de riesgos y las políticas particulares para tratar los riesgos más importantes en cada proceso organizacional. Tendrá, además, la función de evaluar el cumplimiento y efectividad de las políticas de riesgos, a través del análisis y establecimiento de indicadores que midan ambos aspectos.

## Los responsables de los procesos serán los responsables de la dirección, implementación y el cumplimiento de las acciones, controles y mecanismos de evaluación de la efectividad en el manejo de los riesgos.

## Cada área designará los responsables para desarrollar e implementar las técnicas, metodologías y acciones para administrar el riesgo de acuerdo con las orientaciones que imparta la Oficina de Control Interno.

## Los servidores públicos de la Entidad serán responsables de la reducción de los riesgos y de velar por la eficacia de los controles integrados en los procesos, actividades y tareas a su cargo.

# **RECURSOS**

La implementación del presente documento institucional cuenta con el compromiso de la Alta Dirección, para lo cual se dispone de los recursos físicos, económicos, tecnológicos, así como del talento humano con que cuenta la BPP.

Para que se obtengan resultados efectivos, eficiente y eficaces se requiere de la permanente participación de los todos los servidores públicos, para que se divulgue, apropie y se ponga en práctica procesos y procedimientos, que permitan darle oportuna solución a cualquier evento que propicie la ocurrencia de los riesgos relacionados, por proceso, procedimientos, dependencia o servidor público responsable.

Esto debe ser correspondiente entre la alta dirección institucional y los demás servidores públicos. Igualmente, las instancias de control, evaluación y seguimiento serán activas a fin de cumplir los objetivos y propósitos, en concordancia con el acatamiento del ordenamiento legal.

Se espera entonces la apropiación de herramientas e instrumentos contenidos en este documento, para que sean eficientemente realizadas las acciones descritas y con ello poder atender debidamente los posibles eventos que activen algún riesgo institucional.

# **COMUNICACIÓN Y CONSULTA**

*Oficialización y Comunicación*

Con el fin de contribuir a que la administración del riesgo se convierta en parte integral del desarrollo de los procesos de la Biblioteca, así como de la cultura organizacional, la BPP realizó, reunión con todos los líderes o responsables de los procesos para hacer una sensibilización en la administración y seguimiento al mapa de riesgos.

# **INCUMPLIMIENTO DE LA POLITICA**

El incumplimiento de la política se clasificará de dos formas: Por acción o por omisión. De la materialización de ellas se derivarán las medidas de carácter administrativo o disciplinario necesarias que garanticen la normalización de la situación, subsanen el evento sucedido o eliminen la causa raíz del problema identificado.

# **REGISTRO DE LA ADMINISTRACION DEL RIESGO**

Para garantizar la trazabilidad, la BPP, mantendrá registros asociados a los siguientes temas: Seguimiento y Monitoreo, ajustes, mejora, metodologías usadas, sensibilización y publicación en el sitio web.

Para lograr lo anterior se realizó reuniones de trabajo por proceso, las cuales fueron soportados mediante registros de asistencia.

# **ANEXOS**

* Mapa de riesgos de los procesos
* Mapa de riesgos de corrupción.
* Mapa de riesgo de seguridad digital
* Mapa de riesgos Institucional

# **BIBLIOGRAFIA**

Departamento Administrativo de la Función Pública DAFP- Guía para la Administración del Riesgo. Bogotá. 2018.

Instituto Colombiano de Normas Técnicas y Certificación ICONTEC-. Norma Técnica Colombiana NTC-ISO31000. Abril 2011.

Departamento Administrativo de la Función Pública DAFP- Manual Operativo del Modelo Integrado de Planeación y Gestión 2017