INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL

Manual
Gestión de riesgos

Proceso
Fortalecimiento de SIG

Vigencia: 30 de abril de 2021
Versión: 02

1. OBJETIVO

Establecer las directrices para la identificación, valoración, documentación, monitoreo y evaluación de riesgos, con el fin de eliminar o mitigar las causas que puedan afectar el cumplimiento de los objetivos estratégicos y de los procesos.

2. ALCANCE

Aplica a todos los procesos y sedes del Instituto Distrital del Patrimonio Cultural - IDPC. Inicia con la definición de la Política de Administración de Riesgos y la metodología para la gestión de los riesgos, finalizando con el monitoreo, evaluación y mejora de los mismos.

3. TÉRMINOS Y DEFINICIONES

TÉRMINO	DEFINICIÓN
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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Activo de Información	Es cualquier elemento que procese información, la almacene o ayude a protegerla, pero, además, que genere valor para la entidad.
Administración del riesgo	Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia
Amenazas	Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre 2018.
Apetito de riesgo	Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Alta Dirección	Directivos con más alto cargo en el Instituto Distrital del Patrimonio Cultural. Definición propia.
Causa	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.

Causa inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, diciembre 2020.
Causa raíz	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Control	Medida que permite reducir o mitigar un riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Contexto	Definición de los parámetros internos y externos (de la Entidad) que se tendrán en cuenta para la gestión del riesgo. El contexto se utiliza para la definición de la Política de gestión del Riesgo.[1]
Contexto externo	Ambiente externo en el que la Entidad busca alcanzar sus objetivos[2]
Contexto interno	Ambiente interno en el que la Entidad busca alcanzar sus objetivos[3]
Continuidad del Negocio	Describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre 2018.
Información	Datos organizados de tal forma que tienen un significado.
Integridad	Propiedad de exactitud y completitud. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Impacto	Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

[1] [Tomado de la norma NTC-ISO 31000. 2. Términos y definiciones 2.9 Establecimiento del contexto]
[2] [Tomado de la norma NTC-ISO 31000. 2. Términos y definiciones 2.10. Contexto externo]
[3] [Tomado de la norma NTC-ISO 31000. 2. Términos y definiciones 2.11. Contexto interno]

	Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Mapa de riesgos	Documento con la información resultante de la gestión del riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre 2018.
Malware	Se refiere a las partes físicas, tangibles, de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.
Monitoreo	Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
Phishing	Hace referencia a un modelo de abuso informático, que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria).
Probabilidad	Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Ransomware	Es un tipo de programa dañino (malware) que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.
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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre 2018.
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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Riesgos 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).

	Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Riesgo inherente	Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Riesgo residual	El resultado de aplicar la efectividad de los controles al riesgo inherente. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Tolerancia al 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. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.
Vulnerabilidad	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5, Diciembre 2020.

4. 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 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 antitrámites y los mecanismos para mejorar la atención al ciudadano.

Ley 23 de 1982. Ley sobre derechos de autor.

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Decreto 807 de 2019. Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones.

Directiva presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.

Resolución Distrital 305 de 2008. Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Resolución 004 de 2017: Por la cual se modifica la Resolución 305 de 2008 de la CDS.

Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.

Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital.

Guía para la gestión del riesgo de corrupción – 2015 – Presidencia de la República: emitida por la Secretaría de Transparencia de la Presidencia de la República.

Manual Operativo del Modelo Integrado de Planeación y Gestión – versión 3 – diciembre de 2019 - Consejo para la Gestión y Desempeño Institucional.

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020: emitida por el Departamento Administrativo de la Función pública en Bogotá D.C.

5. POLÍTICAS DE OPERACIÓN

5.1 El presente manual hace parte integral de la política de administración del riesgo para el Instituto Distrital de Patrimonio Cultural.

5.2 El Manual Operativo del Modelo Integrado de Planeación y Gestión – versión 3 – diciembre de 2019 - Consejo para la Gestión y Desempeño Institucional frente a la gestión de riesgos establece los requisitos de gestión de riesgos que se deben tener en cuenta por parte del Instituto.

5.3 La Oficina Asesora de Planeación, previo al inicio del ejercicio analizará la coherencia entre la misión, visión, los objetivos estratégicos y de proceso para la correcta aplicación de la metodología de gestión de riesgos.

5.4 Para la aplicación de la metodología de gestión de riesgos se debe contar con las caracterizaciones de los procesos aprobadas y publicadas.

5.5 Los líderes de proceso deben identificar plenamente sus activos de seguridad de la información, como primera línea de defensa, para la aplicación de la metodología de gestión de riesgos.

5.6 El dueño o responsable de cada Activos de Información, será responsable de la adecuada clasificación de la criticidad del Activo de Información, teniendo en cuenta los criterios de Confidencialidad, Integridad y Disponibilidad del mismo.

5.7 Los riesgos de seguridad digital se identificarán de acuerdo a los activos de información que hayan sido clasificados con criticidad “Alta” por el responsable del proceso y/o responsable designado según la valoración brindada a su confidencialidad, integridad y su disponibilidad, razón por la cual se consideraría que existe un riesgo de la información en alguno de éstos tres pilares.

5.8 De acuerdo con las amenazas y vulnerabilidades, se deberá identificar cuál (o cuáles) de los principios de seguridad de la información (confidencialidad, integridad o disponibilidad) se verán afectados por el riesgo.

5.9 Criterios de aceptación del riesgo de seguridad digital: La entidad solo aceptará aquellos riesgos ubicados en zonas “baja” y “moderada”; en cuanto a los riesgos ubicados en zonas “extrema” y “alta” deberán ser tratados.

5.10 La periodicidad de seguimiento a los riesgos de seguridad digital se realizará anualmente.

5.11 Para la identificación y análisis de los riesgos en los procesos, se debe tener en cuenta el contexto externo asociado al objetivo del proceso y el contexto asociado a las actividades del proceso.

5.12 Para la identificación y análisis de riesgos se pueden tomar como fuentes los planes de mejoramiento, encuestas de satisfacción, resultados de la gestión del proceso, informes de auditorías internas o externas, recomendaciones de la oficina asesora de Control Interno (entre otros).

5.13 La documentación de los riesgos de Gestión y Corrupción se deben realizar en el Mapa de Riesgos Institucional.

5.14 Los riesgos de Seguridad Digital se documentarán en la matriz definida para tal efecto en el Instituto.

5.15 Adicional a los riesgos de Gestión, Corrupción y Seguridad Digital, es importante identificar los riesgos de contratación, riesgos para la defensa jurídica, riesgos ambientales, entre otros; los cuales deben ser documentados en el instrumento definido por el ente rector.

5.16 Los riesgos de corrupción se gestionan a través de los lineamientos establecidos por la Ley 1474 de 2011 y el documento Estrategias para la construcción del plan anticorrupción y de atención al ciudadano.

5.17 El monitoreo y seguimiento de los riesgos se realiza de manera integral cada cuatro meses con los siguientes cortes: abril 30, agosto 31 y diciembre 31. El monitoreo se debe registrar en el formato de Mapa de Riesgos Institucional.

5.18 En los casos que un riesgo se materialice, el líder de proceso debe establecer un plan de mejora, adicionalmente debe realizar en el término de 15 días hábiles la revisión y evaluación del riesgo en su totalidad. Dicha información debe ser remitida a la Oficina Asesora de Planeación para su consolidación y validación.

De conformidad con las directrices de la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas"* las acciones a seguir en caso de materialización de riesgos de corrupción son:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente. La Oficina de Control Interno debe asegurar que los controles sean efectivos, se encuentren dirigidos al riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas se refieren a: *i)* Determinar la efectividad de los controles. *ii)*Mejorar la valoración de los riesgos. *iii)*Mejorar los controles. *iv)*Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción. *v)*Determinar si se adelantaron acciones de monitoreo. *v)*Revisar las acciones del monitoreo.

5.19 Es responsabilidad de los líderes de los procesos verificar el cumplimiento de los planes de manejo establecidos para los riesgos identificados teniendo en cuenta tiempo y cronogramas definidos.

5.20 Las actividades de control que se establezcan para el tratamiento de los riesgos, deben evidenciar la eficacia para la administración o gestión efectiva de los riesgos identificados, de tal manera que se puedan reducir las posibilidades de ocurrencia y los impactos que puedan llegar a generar.

5.21 Para la identificación y gestión de los riesgos de la selección de contratistas se aplicarán directrices emitidas por Colombia Compra Eficiente.

6. CONTENIDO

6.1 Declaración de la Política de Administración del Riesgo

El Instituto Distrital del Patrimonio Cultural, interesado en el logro de sus objetivos estratégicos, se compromete a realizar una adecuada administración y gestión de los riesgos; para ello contará con la colaboración y disposición de sus servidores públicos y contratistas de todos los procesos y dependencias de la entidad, quienes en ejecución de los roles de las líneas de defensa llevarán a cabo la identificación, análisis, valoración, monitoreo, control y evaluación de aquellos eventos que puedan afectar el cumplimiento de los objetivos estratégicos, así como la adecuada prestación de los servicios.

La entidad establece los lineamientos y herramientas necesarias, para promover, controlar y responder a los acontecimientos potenciales o aquellos en los que puedan desencadenar situaciones de corrupción o incumplimiento de los objetivos propuestos.

▪ Roles y responsabilidades

Los roles y responsabilidades de todos los actores para la gestión de riesgo y de la entidad se basan en la aplicación del esquema de las cuatro (4) líneas de defensa orientado fundamentalmente al aseguramiento de la gestión y la prevención de la materialización de los riesgos en todos sus ámbitos, así;

Línea estratégica: Está a cargo de la alta dirección/Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación 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*[4], en ejercicio del mismo se desarrollarán las siguientes actividades:

- 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).

Primera línea de defensa: Está a cargo de los líderes de los procesos, proyectos y sus equipos de trabajo; *su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de*

[4] Manual Operativo del Modelo Integrado de Planeación y Gestión; Consejo para la Gestión y Desempeño Institucional Versión 3 diciembre de 2019, página 107.

riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol"[5]*,* en ejercicio del mismo se desarrollarán las siguientes actividades:

- 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 de defensa: Está bajo la responsabilidad, principalmente, del(a) Jefe Oficina Asesora de planeación, líderes de equipos de trabajo, enlaces del sistema de gestión y control de las dependencias, Comité de Contratación, Comité Directivo, Comité Sostenibilidad Contable, equipo autoevaluación y autocontrol, entre otros, que respondan de manera directa por el aseguramiento de la operación.

Su rol principal es asegurar 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; así mismo, consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la "autogestión"[6].

- Oficina asesora de planeación monitorea el adecuado diseño y funcionamiento de los controles, así como la ejecución planes acción dispuestos para la mitigación de los riesgos por parte de la primera línea de defensa y determina las recomendaciones para su fortalecimiento y mejora.
- Oficina Asesora de Planeación diseña y propone las directrices para la gestión de los riesgos conforme con las orientaciones normativas y técnicas, administra el mapa de riesgos de la entidad y brinda asesoría a la 1ª línea de defensa en gestión de riesgos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad.
- La oficina asesora de planeación en articulación con la Asesoría de control interno, presentan ante el Comité Institucional de Gestión y Desempeño y/o el Comité Institucional de Coordinación de Control Interno los resultados de la gestión del riesgo para evitar la materialización del riesgo y la toma de decisiones.
- Realizar monitoreo del diseño y aplicación de controles, así como la ejecución planes acción dispuestos para la mitigación de los riesgos por parte de la primera línea de defensa e informar la líder del proceso para la toma de decisiones.
- Formular en conjunto con la primera línea de defensa los planes de acción para los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento de los objetivos.

[5] Manual Operativo del Modelo Integrado de Planeación y Gestión; Consejo para la Gestión y Desempeño Institucional Versión 3 diciembre de 2019, página 107.
[6] Manual Operativo del Modelo Integrado de Planeación y Gestión; Consejo para la Gestión y Desempeño Institucional Versión 3 diciembre de 2019, página 108.

Tercera línea de defensa: Está línea se encuentra bajo la responsabilidad de la asesoría de control interno quienes desarrollarán su labor a través de los roles: Liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento[7].

- 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.
- 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.

6.2 Niveles de aceptación del riesgo

De acuerdo con los riesgos de gestión aprobados, y la evaluación después de controles se define el nivel de aceptación del riesgo de acuerdo a la siguiente tabla; para los riesgos de corrupción su condición es inaceptable, por tanto, su tratamiento estará enmarcado en reducir, evitar o transferir el riesgo.

Tabla 1. Nivel de aceptación riesgos de gestión

Zona de riesgo	Nivel de aceptación
Baja	Se ***asumirá*** el riesgo y se administra por medio de las actividades propias del proceso asociado. El seguimiento se realizará de acuerdo al numeral 6.3.2.3. del presente manual. Se incluye en el mapa de riesgo institucional.
Moderada	Se deben establecer acciones de control preventivas que permitan ***reducir*** la probabilidad de ocurrencia del riesgo. El seguimiento se realizará de acuerdo al numeral 6.3.2.3. del presente manual. Se incluye en el mapa de riesgo institucional.
Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan ***mitigar*** la materialización del riesgo. El seguimiento se realizará de acuerdo al numeral 6.3.2.3. del presente manual.

[7] Parafraseado del texto del Manual Operativo del Modelo Integrado de Planeación y Gestión; Consejo para la Gestión y Desempeño Institucional Versión 3 diciembre de 2019, página 108.

Tabla 2. Nivel de aceptación riesgos de corrupción

Zona de riesgo	Nivel de aceptación
Baja	Ningún riesgo de corrupción podrá ser aceptado. El seguimiento se realizará de acuerdo con el numeral 6.3.2.3. del presente manual.
Moderada	Se deben establecer acciones de control preventivas que permitan ***reducir*** la probabilidad de ocurrencia del riesgo. El seguimiento se realizará de acuerdo con el numeral 6.3.2.3. del presente manual.
Alta y Extrema	Se adoptan medidas para: ***Reducir*** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. ***Evitar*** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. ***Transferir o compartir*** una parte del riesgo para reducir la probabilidad o el impacto del mismo. El seguimiento se realizará de acuerdo con el numeral 6.3.2.3. del presente manual.

6.3 Descripción de la Metodología

Antes de iniciar la metodología para la identificación y administración de riesgos se deben conocer y analizar los siguientes aspectos:

Establecimiento del contexto: Para la identificación del contexto se tendrá en cuenta el análisis o diagnóstico realizado para la formulación del Plan Estratégico Institucional (PEI).

- Contexto externo
- Contexto interno
- Contexto del proceso

Conocimiento de la entidad:

- Misión
- Visión
- Objetivos estratégicos
- Planeación institucional (Planes, programas y proyectos con los que se tiene relación)

Modelo de operación por procesos:

- Mapa de procesos aprobado
- Caracterización de proceso
- Objetivo del proceso
- Planes, programas o proyectos asociados

La metodología para el adecuado manejo de los riesgos consiste en los siguientes pasos:

6.3.1 Identificación del riesgo

En esta etapa se identifican los riesgos que pueden estar o no bajo el control de la organización. Para esto se debe conocer el contexto estratégico de la entidad, la caracterización de los procesos y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

6.3.1.1 Análisis de objetivos estratégicos y de los procesos

Se deben analizar los objetivos estratégicos y de proceso e identificar los posibles riesgos que afectan su cumplimiento. Los objetivos deben incluir el “qué”, el “cómo”, el “para qué”, el cuándo y el “cuánto”. Todos los objetivos deben estar alineados con la misión y la visión de la entidad y cumplir con la metodología SMART, es decir, contar con las siguientes características:

- Específico
- Medible
- Alcanzable
- Relevante
- Proyectado en el tiempo

En la matriz establecida para la formulación del mapa de riesgos de la entidad, se relaciona el *“Objetivo Estratégico”* y el *“Objetivo del proceso”,* permitiendo con ello identificar que los objetivos cumplan con las características anteriormente señaladas, la coherencia entre los objetivos y su alineación con los riesgos identificados.

6.3.1.2 Identificación de los puntos de riesgo

Se refiere a las actividades del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control.

6.3.1.3 Identificación de áreas de impacto

Es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materializarse un riesgo.

6.3.1.4 Identificación de factores de riesgo

Son las fuentes generadoras de riesgos.

En la siguiente tabla encontramos los factores de riesgo con algunos ejemplos:

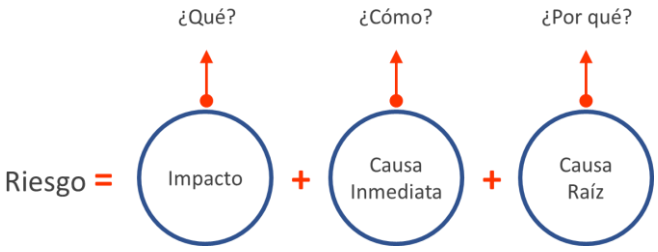
Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto de 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

6.3.1.5 Descripción del riesgo

La descripción del riesgo tiene los siguientes componentes dentro de su estructura:

El inicio de la redacción se hará con las palabras: “Posibilidad de”

Posteriormente se debe agregar la estructura que se muestra a continuación:



La definición de cada uno de los componentes de la estructura es:

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

En la redacción del riesgo es importante tener en cuenta las siguientes premisas:

- No describir como riesgos omisiones ni desviaciones del 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.

6.3.1.6 Clasificación del riesgo

Los riesgos identificados pueden ser agrupados en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

6.3.2 Valoración del riesgo

Con la valoración del riesgo se busca hacer un análisis para 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 riesgo inherente. Posteriormente se confrontan los resultados del análisis del riesgo inherente frente a los controles establecidos con el fin de determinar la zona de riesgo residual.

6.3.2.1 Análisis de riesgos

Con el análisis de los riesgos se busca establecer la probabilidad de ocurrencia del riesgo y el impacto que este causaría al momento de su materialización.

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo y está relacionada con la exposición al riesgo del proceso o la actividad. Esto se determina por el número de veces que se pasa por el punto de riesgo en el período de un año.

En la siguiente tabla se muestran los criterios para definir el nivel de probabilidad (riesgos de seguridad digital):

	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces	60%

	por año.	
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: (Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) versión 5)

Una vez determinada la probabilidad, se debe proceder a determinar el impacto, para lo cual se identifica si es económico y/o reputacional. Si se llegaran a presentar ambos impactos se debe tomar el que sea evaluado con el nivel más alto.

En la siguiente tabla se muestran los criterios para definir el nivel de impacto (riesgos de seguridad digital):

Afectación	Económica / Presupuestal	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El pago afecta la imagen de algún área de la entidad.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general a nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: (Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) versión 5)

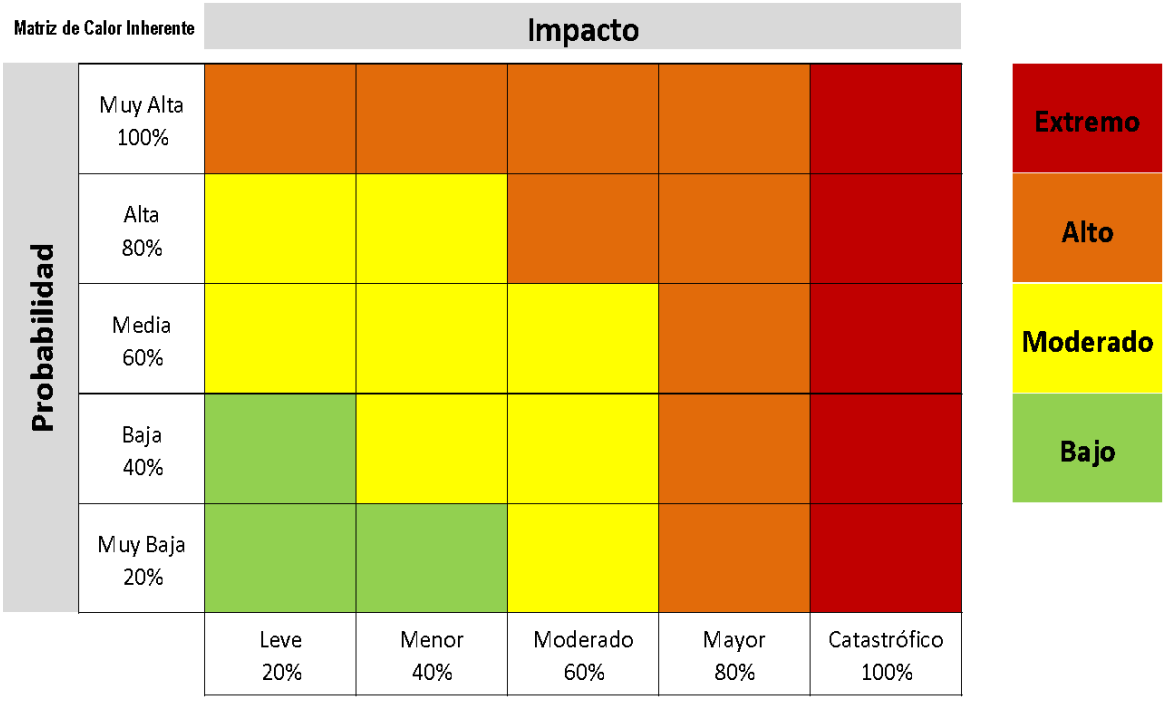
Debido a que las definiciones anteriores no requieren de un análisis subjetivo no es necesario utilizar el criterio experto, ya que los volúmenes de operaciones y los valores de la afectación son conocidos por el líder del proceso correspondiente.

6.3.2.2 Evaluación de riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial o riesgo inherente.

La evaluación de los riesgos se inicia por el análisis preliminar. En este análisis se combinan la probabilidad y el impacto y se determinan los niveles de severidad, los cuales se reflejan en la matriz de calor.

En la siguiente gráfica se muestra la matriz de calor y los niveles de severidad definidos en la misma.



Una vez realizado este paso se procede con la valoración de los controles. Un control está definido como la medida que permite reducir o mitigar el riesgo. En la valoración de los controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Para la descripción de los controles se establece la siguiente estructura:

- Responsable de ejecutar el control: Identificar el cargo del servidor que ejecuta el control, si el control es automático se debe identificar el sistema que realiza la actividad.
- Acción: Se determina mediante verbos que indican la acción que se ejecutará.
- Complemento: Detalles que permiten identificar claramente el objeto del control.

La tipología de los controles y los procesos establece cuándo se activa un control y corresponde a:

- **Controles preventivos:** Va a las causas del riesgo y son accionados a la entrada del proceso, antes de que se origine la actividad originadora del riesgo. Ataca la probabilidad de ocurrencia del riesgo. (Peso 25%)

- **Controles detectivos:** Detecta que algo ocurre y devuelve el proceso a los controles preventivos, son accionados durante la ejecución del proceso. Atacan la probabilidad de ocurrencia del riesgo. (Peso 15%).

- **Controles correctivos:** Son accionados en la salida del proceso y después de que se materializa el riesgo. Atacan el impacto frente a la materialización del riesgo. (Peso 10%)

La tipología relacionada con la forma en que se ejecutan los controles corresponde a:

- Controles manuales: son ejecutados por personas. (Peso 25%)
- Controles automáticos: son ejecutados por un sistema. (Peso 15%)

Los controles también cuentan con unos atributos informativos que le dan formalidad al mismo y permiten conocer el entorno de control y complementar el análisis con elementos cualitativos. Estos controles no tienen una incidencia directa en su efectividad. Estos atributos son:

Documentación.
- Documentado: Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
- Sin documentar: Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.

Frecuencia.
- Continua: El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
- Aleatoria: El control se aplica aleatoriamente a la actividad que conlleva el riesgo.

Evidencia.
- Con registro: El control deja un registro permite evidencia la ejecución del control.
- Sin registro: El control no deja registro de la ejecución del control.

Cada uno de los controles aplicados disminuye la severidad del control de acuerdo con el peso indicado en su definición.

6.3.2.3 Estrategias para combatir el riesgo

Frente al riesgo residual se hace el análisis de la estrategia que se utilizará para combatirlo. Las estrategias pueden ser:

- **Reducir:** Si el riesgo es alto se determina tratarlo mediante transferencia o mitigación del mismo.

- **Transferencia:** Tercerizar el proceso o trasladarlo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero el impacto reputacional lo asume la entidad.

- **Mitigar:** Implementación de acciones que mitiguen el nivel de riesgo. Esto se hace a través de un plan de acción en el que se debe especificar: a) responsable, b) fecha de implementación y c) fecha de seguimiento. No necesariamente se refiere a un control adicional.

- **Aceptar**: Se asume el riesgo conociendo los efectos de su materialización.

- **Evitar:** Si el riesgo es demasiado alto se decide no asumir la actividad que genera este riesgo.

6.3.2.4 Herramientas para la gestión del riesgo

Además del mapa de riesgos resultante de la aplicación de la presente metodología se tienen las siguientes herramientas:

Gestión de eventos

Un evento es un riesgo materializado. Algunas de las fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda
- Las PQRD
- Oficina Asesora Jurídica
- Líneas internas de denuncia

Indicadores clave de riesgo

Son una colección de datos históricos relacionados con algún evento y cuyo comportamiento puede indicar una mayor o menor exposición a ciertos riesgos. Permiten capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, así se podrá evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

En la siguiente tabla se muestran algunos ejemplos de estos indicadores:

Proceso Asociado	Indicador	Métrica
Sistemas	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
Gestión financiera	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
Atención al usuario	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema

	conceptos no adecuados	
Administrativo y financiero	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
Talento humano	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

6.3.2.5 Monitoreo y revisión

El plan de tratamiento del riesgo se basa en la ejecución de las tareas definidas como acciones para mitigar o acciones de mejora, determinadas en el Mapa de Riesgos; para tal fin, deben establecerse los responsables de éstas y fijar fechas para su implementación sin olvidar que también deben velar por el cumplimiento en el desarrollo e implementación de dichas tareas.

De manera cuatrimestral se debe realizar seguimiento a la ejecución de controles y acciones de mitigación, además de identificarse si se materializó o no el riesgo, en caso de que el riesgo se materialice se debe elaborar y ejecutar un plan de mejoramiento que ataque la causa raíz por la que se materializó el riesgo adicionalmente debe analizarse la pertinencia de las actividades de mejora establecidas en el Mapa de Riesgos.

La información del monitoreo y resultado del seguimiento a los riesgos debe ser remitida a la Oficina Asesora de Planeación para la correspondiente socialización y publicación de los resultados obtenidos.

El proceso de Seguimiento y Evaluación, liderado por la Asesoría de Control Interno, debe proporcionar un aseguramiento a la Alta Dirección, sobre el diseño y efectividad de las acciones de administración de riesgo para ayudar a asegurar que los riesgos estén adecuadamente definidos, sean gestionados apropiadamente y que el sistema de control interno esté operando efectivamente.

Adicionalmente, en el marco de la evaluación, resalta aquellos aspectos que consideren una amenaza para el cumplimiento de los objetivos y metas del IDPC, por lo cual se pronuncia sobre la pertinencia y efectividad de los controles establecidos.

Nota: Una vez que el plan de tratamiento se haya ejecutado en las fechas y con las disposiciones de recursos previstas, se debe valorar nuevamente el riesgo y verificar si el nivel disminuyó o no (es decir, si se desplazó de una zona mayor a una menor en el mapa de calor) y luego, compararlo con el último nivel de riesgo residual.

6.3.3 Lineamientos para riesgos de corrupción

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.

Los componentes del riesgo de corrupción son:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado

El Instituto ha incorporado en la matriz del mapa de riesgos los componentes de la definición del riesgo de corrupción para determinar si los riesgos identificados corresponden a riesgos de gestión o riesgos de corrupción.

Esta calificación se hace al momento de la definición de los riesgos.

Para riesgos de corrupción

Nivel	Descriptor	Descripción	Frecuencia
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 sólo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

Riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto leve y menor, que sí aplican para los demás riesgos.

Para el análisis del impacto de los riesgos de corrupción se deben responder (Si –No) las siguientes preguntas

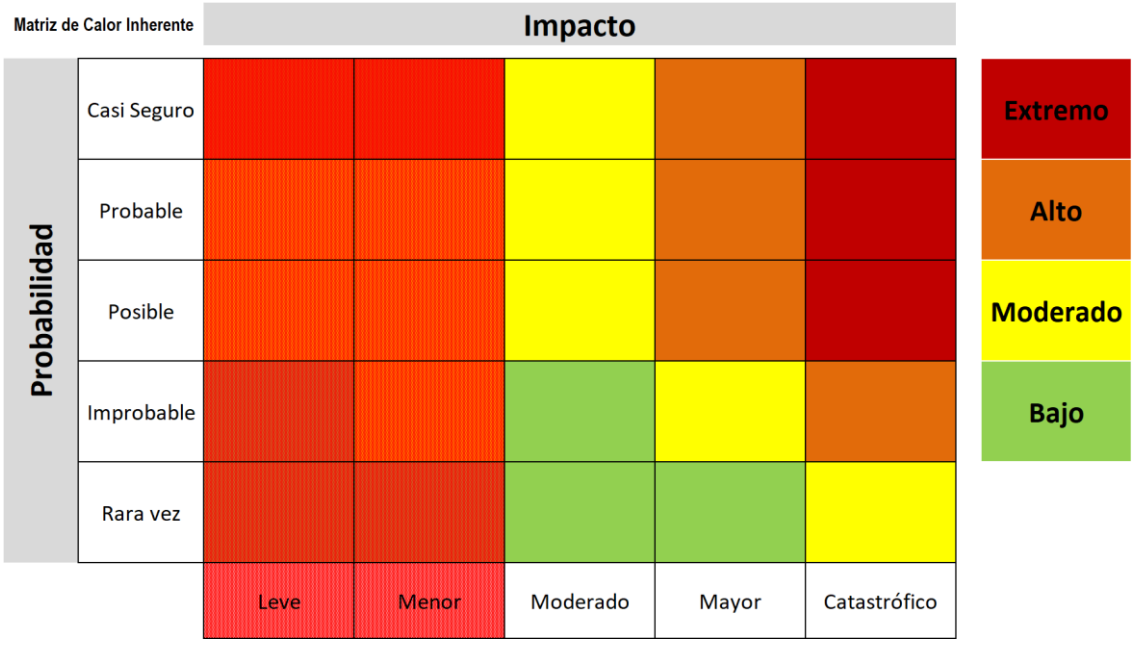
1. ¿Afectar al grupo de funcionarios del proceso?
2. ¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3. ¿Afectar el cumplimiento de misión de la entidad?
4. ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?
5. ¿Generar pérdida de confianza de la entidad, afectando 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?

Con base en las respuestas generadas evalúe el impacto de la siguiente manera:

- 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.

En la siguiente gráfica se muestra la matriz de calor y los niveles de severidad definidos en la misma para los riesgos de corrupción.



Definición del riesgo inherente

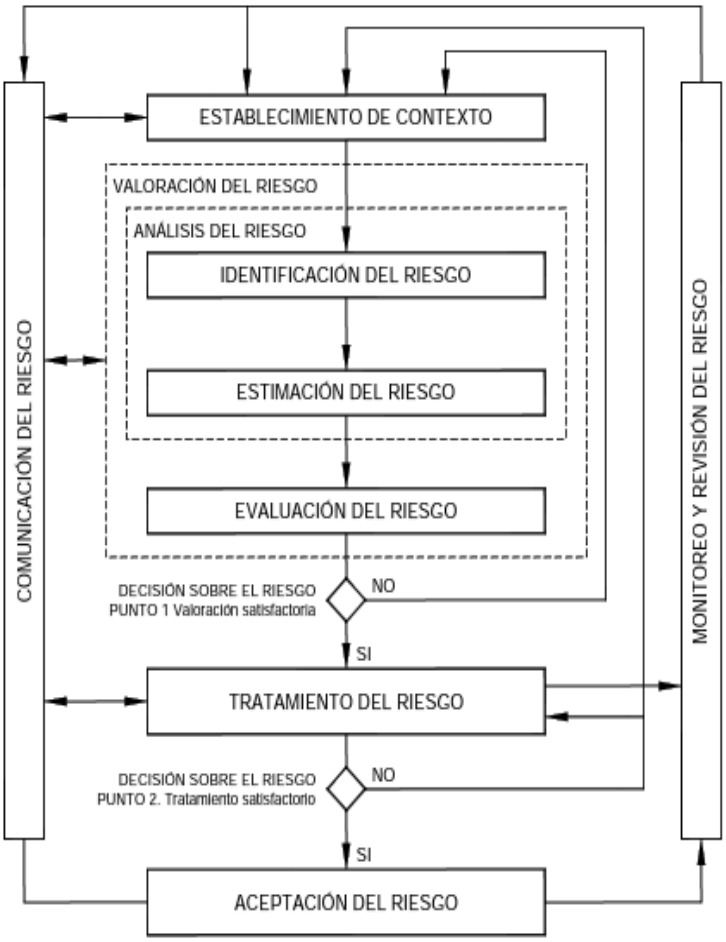
Con la información registrada se toma la calificación de probabilidad resultante del análisis realizado, para el ejemplo se tomará la probabilidad de ocurrencia en **"probable"** y la calificación de impacto en **"mayor"**, ubique la calificación de probabilidad en la fila y la de impacto en las columnas

correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel Alto – color naranja, así se podrá determinar el riesgo inherente.

6.3.4 Lineamientos para la Gestión de Riesgos de Seguridad Digital

La gestión de riesgos del modelo de seguridad y privacidad de la información está basada en las normas NTC-ISO/IEC 27005, NTC-ISO 31000 y alineado a la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) versión 5 y sus actualizaciones; de igual manera el Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas.

Ilustración 1. Proceso de gestión del riesgo MSPI - ISO 27005



6.3.4.1. Identificación Activos de Información

Para realizar la identificación de riesgos de seguridad digital, como primer paso es necesario identificar los activos de información de los procesos de la entidad.

Tabla Conceptualización activos de información

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

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

La identificación y clasificación de los activos de información debe ser realizada por la Primera línea de defensa (Líderes de proceso), en cada proceso donde aplique la gestión del riesgo de seguridad digital, con la orientación del Oficial de Seguridad de la Información de la entidad.

6.3.4.1 Identificación del Riesgo

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos de seguridad digital del proceso (“Confidencialidad, Integridad, o Disponibilidad”) los cuales pueden afectar el logro del objetivo del proceso.

Por lo tanto, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad.
- Pérdida de la integridad.
- Pérdida de la disponibilidad.

6.3.4.2 Identificación de amenazas y vulnerabilidades

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar la materialización de los tres tipos de riesgo anteriormente mencionados y que se han identificado en el proceso.

A manera de ejemplo se citan las siguientes amenazas:

Tabla. Amenazas Comunes

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua o energía.
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos

	Falsificación de derechos

Fuente: ISO/IEC 27005:2009

- **Amenazas dirigidas por el hombre:** Empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla. Amenazas comunes dirigidas por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso Ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques a los sistemas Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad	Asalto a un empleado

Fuente: ISO/IEC 27005:2009

Tabla. Vulnerabilidades comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada

Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios

	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005:2009

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Es de tener en cuenta que se podrán analizar otras vulnerabilidades o amenazas de acuerdo al contexto de los procesos y activos de información analizados, consultando las fuentes de las tablas anteriormente enunciadas.

● 6.3.4.3 Valoración del riesgo de seguridad Digital

Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Tabla. Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica.	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa.	Mensual	Media
Contabilidad, cartera.	Semanal	Alta
***Tecnología (incluye disponibilidad de aplicativos), tesorería. ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.	Diaria	Muy alta

Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.		

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

Para determinar la probabilidad de ocurrencia del riesgo y su impacto, revisar lo establecido el numeral 6.3.2, Valoración del Riesgo.

● 6.3.4.4 Controles

Un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

✓ La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos. En este caso sí aplica el criterio experto.

✓ Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo y el Oficial de Seguridad de la Información.

✓ Se deberá describir de forma clara, breve y precisa, cada control definido.

✓ Para definir un control de manera adecuada, se recomienda seguir la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP), que consta de los siguientes 6 pasos:

- Debe tener definido el responsable de llevar a cabo la actividad de control.
- Debe tener una periodicidad definida para su ejecución.
- Debe indicar cuál es el propósito del control.
- Debe establecer el cómo se realiza la actividad de control.
- Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.

● 6.3.4.5 Tipología de controles

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

- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo.

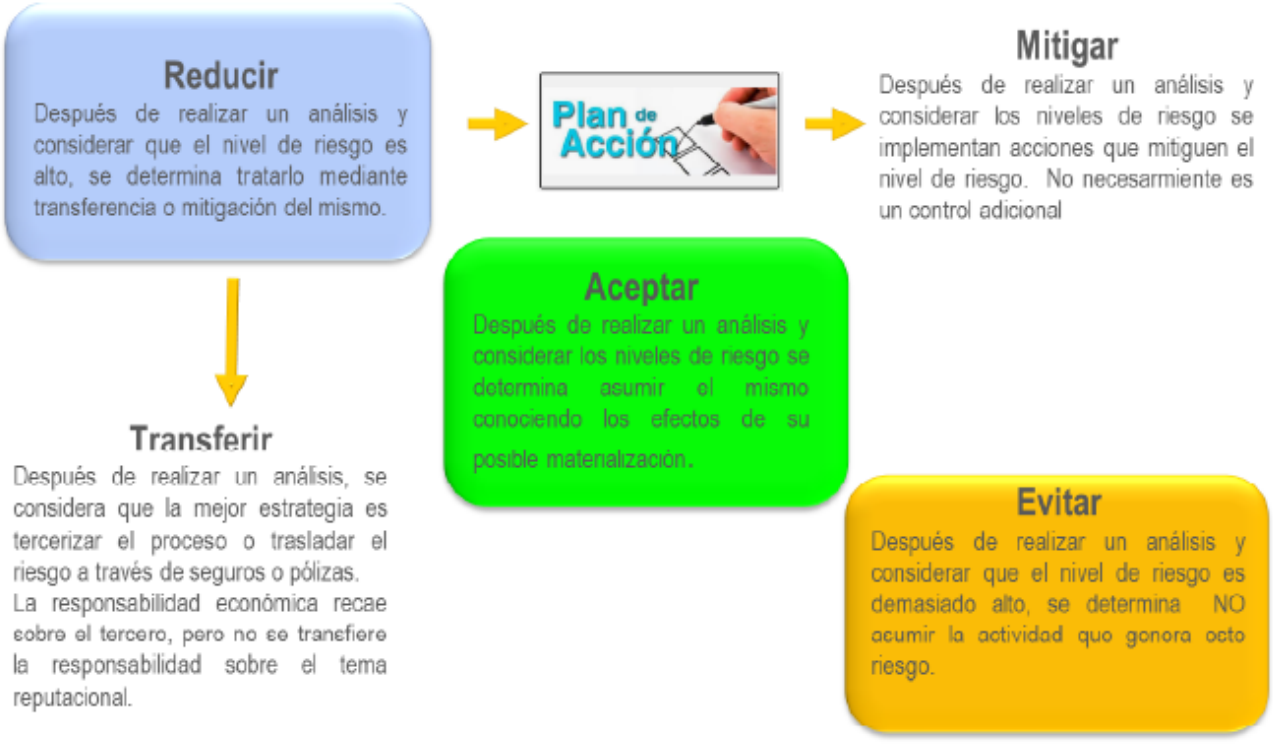
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Atacan el impacto frente a la materialización del riesgo.

6.3.4.6 Planes de tratamiento de riesgos de seguridad digital

Una vez se han identificado los riesgos residuales, el dueño o responsable del riesgo con el apoyo del Oficial de Seguridad de la Información, debe definir el plan de tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgos de seguridad digital.

El tratamiento de riesgos de seguridad digital, se enmarca en las siguientes categorías:

Ilustración. Estrategias para combatir el riesgo



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

Nota: Es importante tener en cuenta que todos los riesgos con evaluación después de controles que se encuentren en zona “Alta” y “Extrema”, se les debe definir acciones para el plan tratamiento de los riesgos, que permitan modificar la probabilidad de ocurrencia y/o impacto.

Con la finalidad de tratar o mitigar los riesgos de seguridad digital se deben tomar como referencia los controles establecidos en el Anexo A de la Norma ISO 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad digital en entidades públicas”.

6.3.5 Monitoreo y revisión

Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente el documento del Mapa de Riesgos de Corrupción y si es del caso ajustarlo.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es -por sus propias características una actividad difícil de detectar.

En esta fase se debe:

1. Garantizar que los controles son eficaces y eficientes.
2. Obtener información adicional que permita mejorar la valoración del riesgo.
3. Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
4. Detectar cambios en el contexto interno y externo.
5. Identificar riesgos emergentes.30

Nota: El Monitoreo y Revisión permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgo, así como su identificación, análisis y valoración.

Para lo anterior, se deberá identificar la presencia de hechos significativos como:

- Riesgos materializados de corrupción.
- Observaciones, investigaciones disciplinarias, penales, fiscales, o de entes reguladores, o hallazgos por parte de la Oficina de Control Interno.
- Cambios importantes en el entorno que den lugar a nuevos riesgos.

7. CONTROL DE CAMBIOS

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
29/07/2019	01	Creación del documento	MEJORA	
28/04/2021	02	Actualización de la metodología de valoración de riesgos de gestión, riesgos de seguridad digital y del contenido del manual.	MEJORA	Ajustes en lineamientos externos (DAFP).

8. CRÉDITOS

Elaboró	Revisó	Aprobó
Fernando A. Vergara García	Magda Patricia Gómez Torres	Luz Patricia Quintanilla Parra
Cargo – Rol: Contratista Oficina Asesora de Planeación	Cargo: Profesional Especializado Oficina Asesora de Planeación.	Cargo: Jefe Oficina Asesora de Planeación
Ellien Yulieth Rodríguez Rincón	Mary Rojas Muñoz	Juan Fernando Acosta Mirkow
Cargo – Rol: Contratista Oficial de Seguridad de la Información	Cargo – Rol: Contratista Líder TI	Cargo: Subdirector de Gestión Corporativa
Aprobado	Acta Comité Institucional de Gestión y Desempeño de fecha 28 de abril de 2021	