PRESENTACIÓN

La Política de Administración del Riesgo del Concejo de Bogotá D.C., orienta la identificación, valoración y tratamiento de los riesgos al interior de la Corporación, facilitando la toma de decisiones, garantizando la adecuada operación de los distintos procesos que permiten a la Corporación el cumplimiento de su misión, y generar valor público.

La aplicación de la metodología que se describe a continuación facilitara a los funcionarios adoptar los controles para prevenir la materialización de los riesgos, fortaleciendo la cultura del autocontrol al interior de la Corporación y establecer las acciones a desarrollar en el evento de la materialización de alguno de los riesgos identificados.

La metodología basada en la *«Guía para la administración del riesgo y el diseño de controles en entidades públicas»* del Departamento Administrativo de la Función Pública, recoge los cambios propuestos en la versión 5, y su adaptación a la realidad y dinámicas propias del Concejo de Bogotá D.C.

Para facilitar la aplicación de la política se definieron cuatro capítulos, el Capítulo I define la política y lineamientos generales, el Capítulo II la gestión del riesgo en la operación de los procesos, el Capítulo III la gestión de los riesgos de corrupción y finalmente el Capítulo IV la gestión de los riesgos de seguridad de la información, bajo el liderazgo de la Dirección Administrativa – Proceso Sistemas y Seguridad de la Información.

CONTENIDO

Capítulo I
Lineamientos Generales de la Política

1. Objetivo

Gestionar los riesgos de corrupción, de gestión y de seguridad digital en el Concejo de Bogotá D.C., a través de herramientas metodológicas para su identificación, valoración, tratamiento; monitoreo y evaluación; así mismo establecer los niveles de responsabilidad en términos de formulación, seguimiento e implementación de los mecanismos conceptuales y técnicos señalados en este documento para la gestión del riesgo, con el propósito de controlar los eventos que potencialmente puedan obstaculizar el logro de los objetivos estratégicos y de los procesos.

2. Alcance

La política de administración del riesgo aplica a todos los servidores públicos de la Corporación y dependencias del Concejo de Bogotá D.C., en la totalidad de los procesos a su cargo. La identificación de los riesgos se circunscribe a los objetivos de cada proceso y los objetivos estratégicos de la Corporación.

Aplica a todos los procesos e involucra la identificación, valoración, tratamiento, monitoreo, seguimiento, revisión, comunicación, y análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público en beneficio privado.
- Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

3. Declaración de la Política de Administración de Riesgos

El Concejo de Bogotá D.C., como Corporación pública de elección popular y en cumplimiento de sus funciones constitucionales, legales y reglamentarias garantizara la continuidad y sostenibilidad de su misionalidad frente a su entorno, ciudadanos y grupos de interés, para lo cual se compromete a enfocar sus esfuerzos institucionales a identificar,

analizar y dar tratamiento a los riesgos que puedan obstaculizar el logro de sus objetivos estratégicos y de los procesos en el cumplimiento de su misionalidad.

Para ello y de acuerdo con su naturaleza adaptara las herramientas necesarias para la administración de los riesgos, tomando como referente la «Guía para la administración del riesgo y el diseño de controles en entidades públicas» proferida por el Departamento Administrativo de la Función Pública, y demás documentos técnicos y legales que le sean aplicables.

4. Términos y Definiciones

- **Activos de seguridad de la información del proceso:** es cualquier elemento que tenga valor para la entidad, tales como aplicaciones, servicio web, redes, información física o digital, tecnologías de información TI.

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

- **Amenaza Cibernética:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

- **Análisis del Riesgo:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011)

- **Apetito al 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.

- **Arquitectura TI (Tecnología de la Información):** permite describir la estructura y las relaciones de todos los elementos de TI de la entidad. Se compone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos.

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

- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

- **Causa Inmediata:** Circunstancia bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

- **CICCI :** Comité Institucional de Coordinación del Control Interno

- **CIGD**: Comité Institucional de Gestión y Desempeño

- **Clasificación de la información:** es el ejercicio por medio de la cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea 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.

- **Control**: Medida que permite reducir o mitigar un riesgo.

- **Custodia:** es una parte designada de la entidad, un cargo, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

- **Disponibilidad**: propiedad de la información de ser accesible y utilizable a demanda por una entidad.

- **Factores de Riesgo:** Son las fuentes generadoras de riesgo.

- **Gestión del Riesgo:** proceso efectuado por los Líderes de los Procesos y sus equipos de trabajo para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos de la Corporación.

- **Identificación de los activos de seguridad de la información del proceso:** consiste en qué se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, proporcionando confianza en el uso del entorno digital.

- **Impacto**: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Información:** se refiere a un conjunto organizado de datos contenido en cualquier momento que los sujetos obligados generen, obtengan, adquieran, transformen o controles.

- **Información pública:** es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- **Información pública clasificada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014.

- **Información pública reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad como tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19º.

- **Integridad**: Propiedad de salvaguardar la exactitud y completitud (estado completo de los activos).

- **Inventario de activos:** asociados con la información y las instalaciones de procesamiento de la información y se deberá elaborar y mantener un inventario de estos activos.

- **Ley Estatutaria 1581 de 2012 (octubre 17):** por la cual se dictan disposiciones generales para la protección de datos personales. Los principios y disposiciones contenidas serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

  Según artículo 4º, se mencionan los principios para el tratamiento de datos personales como: Tratamiento de datos, finalidad, libertad, veracidad, transparencia, circulación restringida, seguridad, y confidencialidad.

- **Ley 1712 de 2014 (marzo 6):** 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. Su objetivo es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.

- **Modelo de seguridad y privacidad de la información (MSPI):** modelo que imparte lineamientos a las entidades públicas en materia de implementación y adopción de

buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación y Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del nivel del Riesgo poder ser probabilidad por impacto, sin embrago, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de probabilidad – Impacto.

- **Plan Anticorrupción y de Atención al Ciudadano**: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **Políticas de gobierno digital**: es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación ciudadano – Estado, mejorando la prestación de servicios por parte de la entidad, y generando confianza a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integral de Planeación y Gestión –MIPG- y se integra con las políticas de gestión y desempeño institucional.

- **Política de seguridad digital:** el concepto se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital, como seguridad de la información, arquitectura y servicios ciudadanos digitales.

- **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 un año.

- **Propietario de la información:** es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

- **Propiedad de los activos:** los activos mantenidos en el inventario deberían tener un propietario.
- **Riesgo**: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. *“los eventos potenciales hacen referencia a la posibilidad de incurrir en*

pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos".

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

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

- **Riesgo de 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).

- **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.

- **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.

- **Riesgo Residual**: El resultado de aplicar la efectividad de los controles al riesgo inherente.

- **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.

- **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.

- **Usuarios:** cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la dependencia, para propósitos propios de su labro y que tendrán el derecho manifiesto de uso dentro del inventario de información.

- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explorada por una o más amenazas.

5. Lineamientos Generales de la Política de Administración del Riesgo

- Para la identificación y análisis de los riesgos en los procesos, se debe tener en cuenta el contexto interno y externo identificado en el marco de la formulación del plan de acción cuatrienal.

- Para el establecimiento de los lineamientos de la administración de los riesgos en la Corporación, se fundamenta en los lineamientos y herramientas que pone a disposición de las entidades públicas el Departamento Administrativo de la Función Pública (DAFP) para la implementación del MIPG, ajustado a las dinámicas propias de la Corporación.

  Los distintos pasos de la gestión del riesgo como identificación, análisis, valoración, tratamiento, comunicación, monitoreo y revisión, seguimiento de los riesgos y la evaluación la gestión de los riesgos se realiza conforme a los lineamientos que para el efecto se adaptan para el Concejo de Bogotá D.C., en el presente documento.

- El mapa de riesgos de corrupción conforme a lo establecido por la Ley 1474 de 2011 forma parte del Plan anticorrupción y de atención al ciudadano.

- En los casos de que un riesgo se materialice, el líder de proceso deberá realizar una revisión del riesgo y efectuar los cambios pertinentes al plan de tratamiento del riesgo para mitigar su impacto y la probabilidad de repetir su ocurrencia.

- Es responsabilidad de los procesos verificar el cumplimiento de los planes de tratamiento establecidos para los riesgos identificados teniendo en cuenta los cronogramas establecidos.

6. Niveles de Aceptación del Riesgo

Para definir los niveles de aceptación del riesgo, se debe tener en cuenta el análisis frente al apetito del riesgo, se debe tener claridad frente a los siguientes conceptos:

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual los Líderes de los procesos consideran que no sería posible el logro de los objetivos de la entidad.

Gráfico Nro. 1.- Definición de apetito, tolerancia y capacidad de riesgo.

Fuente: creación propia teniendo como referente guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5

El Concejo de Bogotá D.C., determina que frente a los riesgos de corrupción no hay aceptación y siempre se deben formular acciones para evitar su materialización.

Los riesgos de seguridad de la información y de los procesos que se encuentren en zona de riesgo baja, se dejan a criterio del líder del proceso, como experto, la formulación de acciones de tratamiento de considerarlo necesario, sin embargo, se debe efectuar el monitoreo conforme a la periodicidad establecida.

En los procesos, acorde con los riesgos residuales identificados por los líderes de proceso, diferentes a la zona baja, deberán definir la estrategia de tratamiento compuesta por las acciones, responsable y tiempos para su implementación.

7. Responsabilidades en la implementación de la Política de Administración del Riesgo

Teniendo como marco de referencia lo establecido en el Manual Operativo del MIPG y con el fin de dar cumplimiento a las etapas de la metodología para la implementación de la política de administración del riesgo, a continuación, se establecen los roles y las

responsabilidades para cada una de las líneas de defensa y los demás actores involucrados.

Gráfico Nro. 2.- Líneas de Defensa

Fuente: creación propia teniendo como referente guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5 y el Modelo Integrado de Planeación y Gestión –MIPG

7.1. Línea Estratégica

Define el marco general para la gestión del riesgo y el control, supervisa su cumplimiento. Esta línea está a cargo del Comité Institucional de Coordinación de Control Interno, el cual está compuesto por el Presidente y los directivos de la Corporación.

Le compete:

- Aprobar la política de administración del riesgo del Concejo de Bogotá D.C., efectuar el seguimiento a su implementación. y analizar los resultados de las evaluaciones realizadas por la Oficina de Control Interno.

- Recomendar mejoras a la política de administración del riesgo.

- En el marco del Comité de Coordinación Institucional de Control Interno, revisar los riesgos de los procesos que en el monitoreo se evidencie la materialización de estos.

- Revisar los cambios en el Direccionamiento Estratégico y/o el entorno y cómo estos pueden generar nuevos riesgos o modificar los que se tienen identificados en cada uno

de sus procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.

- Revisar la adecuada definición y desdoblamiento de los objetivos institucionales en los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar.

7.2. Primera Línea de Defensa

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y tratamiento. Esta línea está a cargo de los líderes de los procesos y sus respectivos equipos de trabajo.

Le compete:

- Garantizar que al interior de sus equipos de trabajo se conozca la política de administración del riesgo y las actividades para su implementación.

- Identificar, valorar y evaluar los riesgos y actualizar cuando se requiera, los riesgos que puedan afectar los objetivos del proceso y objetivos estratégicos a su cargo.

- Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión.

- Efectuar seguimiento al cumplimiento de las actividades y planes de tratamiento, como resultado del ejercicio del autocontrol del proceso a su cargo.

- Reportar a la Oficina Asesora de Planeación, el monitoreo a los mapas de riesgos de los procesos a su cargo, avances y evidencias de la gestión de los riesgos a su cargo.

- Revisar y reportar a la Oficina Asesora de Planeación y la Oficina de Control Interno, los eventos de riesgos de gestión y corrupción que se han materializado en la Entidad, así como las causas que dieron origen a estos. De igual forma, tomar las medidas oportunas y eficaces para evitar en lo posible la repetición del evento no deseado.

- Revisar y reportar al proceso de Sistemas y seguridad de la Información de la Dirección Administrativa y a la Oficina de Control Interno, los eventos de riesgos de seguridad digital que se han materializado en la Entidad, así como las causas que dieron origen a estos.

7.3. Segunda Línea de Defensa

Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen eficientemente.

Esta línea de defensa está a cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: líderes de los procesos, responsables de TI, Supervisores e Interventores de contratos, coordinadores de otros sistemas de gestión.

Le compete:

- Revisar el adecuado diseño de los controles para la mitigación de riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos.

- Revisar el riesgo inherente y residual para cada proceso y consolidarlo así mismo pronunciarse sobre cualquier riesgo pueda surgir en la gestión de la entidad.

- Hacer seguimiento a las actividades de control, establecidas para mitigar los riesgos, verificando de ser pertinente, que sean documentadas e incorporadas en los procedimientos.

- Revisar los planes de tratamiento establecidos para cada uno de 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 a los objetivos.

Por su parte corresponde a la Oficina Asesora de Planeación:

- Asesorar a la línea estratégica en la definición de la política de administración de los riesgos de gestión y corrupción de la Corporación y la adaptación de la metodología de acuerdo con las dinámicas propias del Concejo de Bogotá D.C.

- Socializar a los procesos la política de administración del riesgo y brindar el acompañamiento a los procesos que así lo soliciten.

- Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos y el monitoreo periódico a los mismos.

- Orientar a la primera línea de defensa en el diseño de controles para la mitigación de los riesgos y cuando se requiera, la adecuada documentación de estos.

- Informar a la tercera línea de defensa, la materialización de los riesgos notificados por los procesos y acompañar al proceso, cuando lo requiera, en la identificación de las causas de la materialización del riesgo y el ajuste al mapa de riesgos, mediante el fortalecimiento de los controles.

Por su parte corresponde a la Dirección Administrativa- Proceso de Sistemas y Seguridad de la Información:

- Asesorar a la línea estratégica en la definición de la política de administración de los riesgos de seguridad de la información y la adaptación de la metodología de acuerdo con las dinámicas propias del Concejo de Bogotá D.C.

- Socializar a los procesos la política de administración del riesgo en lo relacionado a los riesgos de seguridad de la información y brindar el acompañamiento a los procesos que así lo soliciten.

- Apoyar a los procesos en la identificación de los riesgos de seguridad de la información para su consolidación en el mapa de riesgos institucional.

- Orientar a la primera línea de defensa en el diseño de controles para la mitigación de los riesgos de seguridad de la información y cuando se requiera, la adecuada documentación de estos.

- Informar a la tercera línea de defensa, la materialización de los riesgos de seguridad de la información notificados por los procesos y acompañar al proceso, cuando lo requiera, en la identificación de las causas de la materialización del riesgo y el ajuste al mapa de riesgos, mediante el fortalecimiento de los controles.

7.4. Tercera Línea de Defensa

Proporciona información sobre la efectividad del Sistema de Control Interno a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Esta línea de defensa está a cargo de la Oficina de Control Interno, buscando proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno.

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que se tienen identificados en cada uno de sus procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

- Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.

- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los posibles riesgos de corrupción que evidencien en los ejercicios de auditoría interna.

- En el marco del ejercicio de auditoría, revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre los aspectos susceptibles de mejora.

- Evaluar la implementación de la política de administración del riesgo y recomendar las mejoras que estime pertinentes.

- En relación con el fomento de la cultura del control en la entidad, brindar asesoría a los procesos en la identificación y valoración de riesgos y adecuado diseño de controles.

Capítulo II

Metodología para la Gestión de los Riesgos de los Procesos

Antes de iniciar la implementación de la metodología es importante que los funcionarios identifiquen el contexto interno y externo del Concejo de Bogotá D.C., el modelo de operación por procesos y el proceso al cual pertenece y su contribución a los objetivos estratégicos de la Corporación.

Gráfico Nro. 3.- Conocimiento de la Entidad

Fuente: Creación propia teniendo como referente la Guía de administración del riesgo y el diseño de controles en entidades públicas. Versión 5 – DAFP.

Para facilitar la identificación del contexto, se invita a dar respuesta a las siguientes preguntas:

1. ¿Cuál es la misión y visión del Concejo de Bogotá D.C.?

2. En el mapa de procesos adoptado por la Corporación ¿A cuál proceso pertenezco? ¿Cuál es el objetivo de mi proceso? Revisar la caracterización del Proceso.

3. Desde mi proceso ¿Cuál es mi contribución a las Apuestas Estratégicas, Objetivos Estratégicos, Líneas de Acción y Logros definidos en el Plan de Acción Cuatrienal?

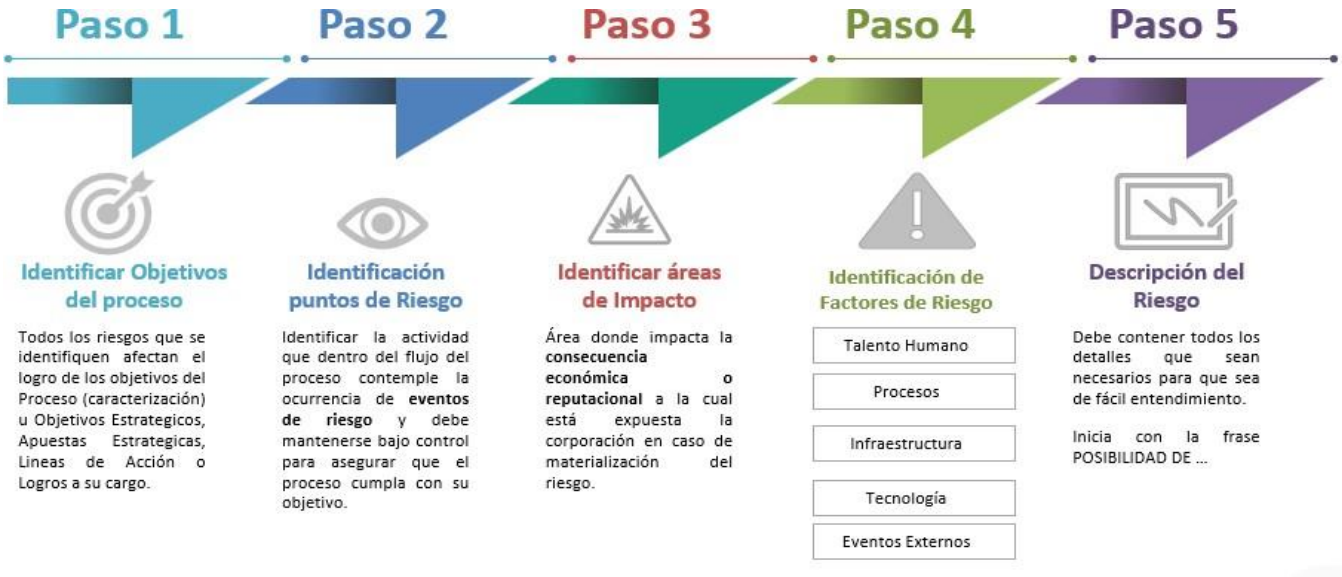
4. Las actividades que realizo a diario: ¿Se encuentran documentadas?, ¿Tienen controles identificados?

Una vez se identifique el contexto, es importante conocer la **Política Administración del Riesgo,** e Identificar los lineamientos de la política descritos en el capítulo I y los niveles de responsabilidad frente al manejo de los riesgos.

8. Identificación del Riesgo

Desarrollar el paso a paso descrito en el siguiente gráfico:

Gráfico Nro. 4.- Identificación del Riesgo.



Fuente: Creación propia teniendo como referente la Guía de Administración del riesgo y el diseño de controles en entidades públicas. Versión 5.

La *«Guía para la Administración del Riesgo y el diseño de controles de entidades públicas»* del Departamento Administrativo de la Función Pública define los factores de riesgo como las fuentes generadoras de riesgos, y se transcribe la tabla de ejemplo propuesta, a manera de ilustración.

Tabla Nro. 01 Factores de Riesgos

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades quedeben 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
Talentohumano	Incluye seguridad y salud en eltrabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica dela entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con lainfraestructura 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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5- Departamento Administrativo de la Función Pública.

La descripción del riesgo debe contener los detalles que sean necesarios para ser entendido tanto para el líder del proceso como para personas ajenas al proceso de forma clara para lo cual se definió la siguiente estructura iniciando la frase: **POSIBILIDAD DE…**

Gráfico Nro. 5 – Descripción del Riesgo

Fuente: *creación propia teniendo como referente Guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5.*

Recomendaciones al realizar la descripción del riesgo:

- No describir como riesgos omisiones, ni desviaciones del control
- Nos describir causas como riesgos operativos
- No describir riesgos como la negación de un control
- No existen riesgos transversales, lo que pueden existir son causas transversales.

Ejemplo[1]

1 Tomado de la Guía de la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5-DAFP

9. Clasificación del Riesgo

A continuación, se presenta una tabla con la clasificación propuesta por el DAFP y la relación con el factor de riesgo:

Tabla Nro. 02 Clasificación del Riesgo y Factores de Riesgo

Clasificación	Descripción	Factor de Riesgo
1. Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Procesos
2. Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento Externo
3. 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	Talento Humano
4. Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	Tecnología
5. 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.	Varios Factores
6. 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.	Varios Factores
7. 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.	Infraestructura Evento Externo

Fuente: creación con referente Guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5

10. Valoración del riesgo

La valoración del riesgo permite establecer la probabilidad de ocurrencia del riesgo y el nivel de impacto o consecuencia, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente)

Grafica Nro. 6 Valoración del Riesgo

Fuente: *creación propia teniendo como referente Guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5.*

10.1. Análisis de riesgo

El líder de cada proceso en compañía de su equipo de trabajo establece la probabilidad de ocurrencia del riesgo y su impacto, con su experticia y conocimiento en el proceso. La probabilidad se calcula identificando la **exposición al riesgo, entendida como el número de veces que se pasa por el punto de riesgo** en el periodo de un año y se clasifica de la siguiente manera.

Grafica Nro. 7-Criterios para definir el nivel de probabilidad

Fuente: *Creación propia teniendo como referente Guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5*

Después de determinar la probabilidad del riesgo se debe determinar el impacto ya sea económico o reputacional validando los criterios en la siguiente tabla.

Tabla Nro. 3 Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 11 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, genera afectación reputacional del área o dependencia.
Moderado 60%	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la Corporación con algunos ciudadanos, afecta el logro de algunos objetivos.
Mayor 80%	Entre 101 y 500 SMLMV	El riesgo afecta la imagen de la Corporación y es publicitado a nivel distrital.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen del Concejo de Bogotá D.C. a nivel nacional, y es publicitado a nivel nacional.

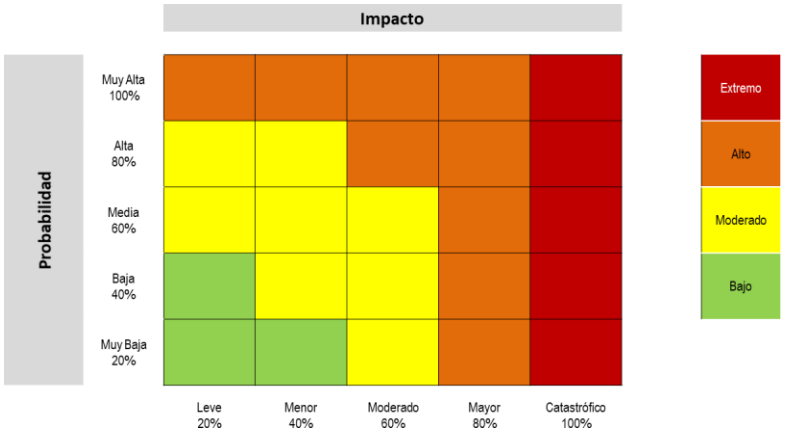
Fuente: *Tomado de la Guía de la administración del riesgo y el diseño de controles en entidades públicas. Versión 5-DAFP.*

Si se presenta ambos impactos para un riesgo, tanto económico como reputacional, con diferente nivel se debe tomar el nivel más alto.

10.2. Evaluación de riesgo

Diagnosticar la zona de riesgo inicial o preliminar antes de controles (RIESGO INHERENTE), a partir del análisis de la probabilidad de ocurrencia del riesgo e impacto. Como se evidencia en el siguiente gráfico:

Grafica Nro. 7 -Matriz de calor aplicando la probabilidad e impacto



Fuente: Tomado de la Guía de Administración del riesgo el diseño de controles en entidades públicas. Versión 5.

10.3. Valoración de controles

Ubicado en el mapa de calor la severidad del riesgo inherente, el Líder del proceso en compañía de su equipo de trabajo, identifica los controles existentes y los valora teniendo en cuenta los criterios que se describen a continuación.

La Estructura del Control que ayude a mitigar de manera adecuada el riesgo, debe considerar desde la redacción de este, las siguientes características:

Gráfico Nro. 8 Estructura descripción del control

Fuente: creación propia teniendo como referente guía de la administración del riesgo el diseño de controles en entidades públicas. Versión 5

Los responsables de implementar y monitorear los controles son los Líderes de los Procesos.

Gráfico Nro. 9 Tipologías de controles

Fuente: creación propia teniendo como referente *«Guía para la Administración del Riesgo y el diseño de controles de entidades públicas» Versión 05.*

Los controles tienen dos tipos de atributos los de **eficacia**, que permiten mitigar los riesgos y tienen una incidencia sobre el mismo, y los atributos de información o formalización, que permiten dar formalización al control, sin embargo, no tiene incidencia en su efectividad.

El líder del proceso analiza los atributos para el diseño del control, teniendo en cuenta las características como se observa en la siguiente tabla:

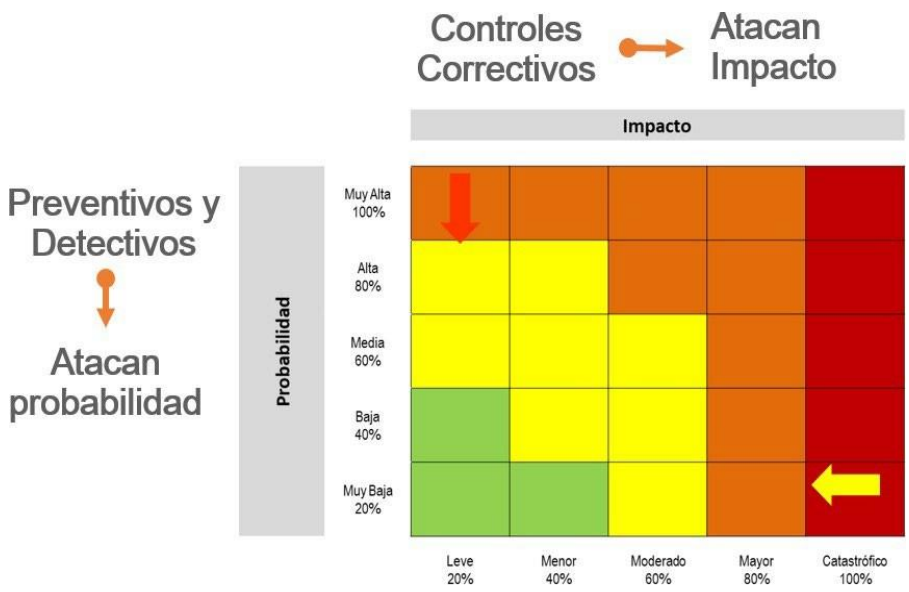
Tabla Nro. 4 Atributos para el diseño del control

Características			Descripción	Peso
Atributos de Eficacia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos Informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	0
		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.	0
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	
	Evidencia	Con Registro	El control deja un registro permite evidencia la ejecución del control.	
		Sin Registro	El control no deja registro de la ejecución del control.	

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

Teniendo en cuenta la fortaleza de los controles se puede dar movimiento, en la matriz de calor como se ilustra en la siguiente figura:

Gráfico Nro. 10 Movimiento de la matriz de calor vs Controles



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

Se debe tener en cuenta que los controles mitigan el riesgo en forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante.

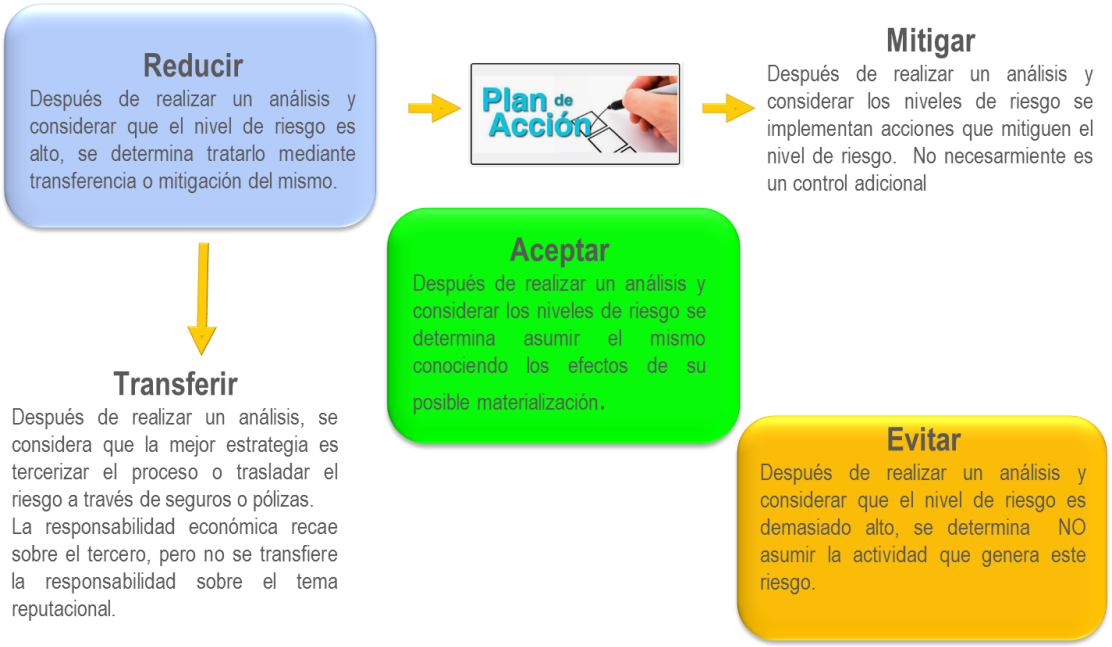
De la aplicación de la totalidad de los controles frente al riesgo, se obtiene el Riesgo Residual, frente al cual se evalúa la estrategia de tratamiento.

11. Estrategias para combatir el riesgo

El proceso debe tomar la decisión de aceptar, reducir o evitar el riesgo, analizando el riesgo residual para procesos en funcionamiento y riesgo inherente para nuevos procesos.

La tolerancia a los riesgos de proceso que el Concejo de Bogotá D.C. esta dispuesto a soportar en relación con la consecución de sus objetivos, corresponde a los riesgos que se encuentren en la Zona Residual **baja y moderada,** aquellos que se ubiquen en otra zona deberán adoptar un plan de tratamiento.

Gráfico Nro. 11-Estrategias para combatir el riesgo



Fuente: *Tomado de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 5 – DAFP*

El plan de tratamiento es una herramienta de planificación empleada para la gestión y control de tareas, donde se especifica responsable, fecha de implementación y seguimiento, que buscan evitar la materialización del riesgo.

En los eventos en que el **riesgo residual** se ubique en la zona Moderada, Alta y Muy Alta se debe definir el plan de tratamiento y monitorear su cumplimiento.

12. Aprobación y Monitoreo de la Gestión del Riesgo

Para la formulación de los riesgos de gestión y corrupción, los líderes de proceso y sus equipos de trabajo cuentan con el acompañamiento metodológico de la Oficina Asesora de Planeación cuando así lo soliciten, conforme a los lineamientos que se establecen en el presente documento. En el caso de los riesgos de seguridad de la información el acompañamiento se encuentra a cargo de la Dirección Administrativa - Proceso de Seguridad de la Información.

La aprobación de los mapas de riesgo está a cargo del directivo líder del proceso quien revisa y aprueba el mapa de riesgos del proceso de gestión y Corrupción y lo remite vía electrónica al correo de la Oficina Asesora de Planeación para su consolidación. En el caso

de los riesgos de seguridad de la información se remitirán a la Dirección Administrativa - Proceso de Seguridad de la Información para su consolidación.

Los mapas de riesgos de corrupción y de gestión de los procesos de la Corporación se mantendrán en sus versiones más recientes (tres últimas vigencias) en la carpeta de Planeación SIG de la red interna para conocimiento de los servidores y colaboradores, conforme a las aprobaciones y revisiones que hayan realizado los líderes de proceso. En el caso de los riesgos de seguridad de la información se remitirán a la Dirección Administrativa - Proceso de Seguridad de la Información para su consolidación.

Los líderes de los procesos realizaran comunicación al interior de sus equipos, los mapas de riesgos aprobados.

A continuación, se fijan los criterios para el monitoreo de la gestión de los riesgos identificados por cada uno de los procesos, conforme a las líneas de defensa definidas:

Tabla Nro. 5 Tabla de Actividades para el Monitoreo a los Riesgos

Responsable	Actividad	Periodicidad	Registro
Línea Estratégica Comité de Coordinación Institucional de Control Interno	Revisa y aprueba la Política de Administración del Riesgo.	Anual	Acta de la sesión del Comité
Primera Línea de Defensa Líderes de los procesos y sus Equipos de trabajo	Monitorea los riesgos identificados y la efectividad de loscontroles definidos	Cuatrimestral	Matriz de Monitoreo Los 03 primeros días de los meses Marzo, Julio y Noviembre
Segunda Línea de Defensa Líderes de los procesos, Responsables de TI, Supervisores e Interventores de contratos, Coordinadores de otros sistemas de gestión.	Monitorea los riesgos identificados y la efectividad de loscontroles definidos y reporta a la Oficina Asesora de Planeación	Cuatrimestral	Reporte Matriz de Monitoreo, los 03 primeros días de los meses de Enero, Mayo y Septiembre
Oficina Asesora de Planeación	Consolida el reporte del monitoreo de los riesgos de Gestión y Corrupción reportado por cada uno de los procesos.	Cuatrimestral	Consolidación de la Matriz de Monitoreo Riesgos de Gestión y Corrupción

Responsable	Actividad	Periodicidad	Registro
Tercera Línea de Defensa Oficina de Control Interno	Realiza **seguimiento** a la administración del riesgo del proceso en el desarrollo de los ejercicios de Auditoría Interna. En virtud de lo establecido en la «Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces» del DAFP de diciembre de 2018 o la que esté vigente, realiza anualmente la **evaluación** de la gestión del riesgo de la Corporación.	Anual	Informe de Auditoría a los procesos Evaluación de la Gestión del Riesgo de la Corporación

Fuente: Creación propia teniendo como referente la «Guía para la Administración del Riesgo y el diseño de controles de entidades públicas» Versión 05 – DAFP.

13. Herramientas ante la Materialización del Riesgo

Cuando se materializa un riesgo, el líder del proceso con su equipo de trabajo debe revisar si el riesgo fue identificado y valorado en el Mapa de Riesgos del Proceso y que sucedió con los controles.

En caso de un evento no deseado se debe efectuar un análisis donde se valide si es un riesgo y no se había identificado, de hallarse se debe incluir y dar tratamiento de acuerdo con la metodología.

En el evento de materialización de un riesgo, se deberán emprender acciones en el marco de sus responsabilidades, de la siguiente manera:

- Revisar el mapa de riesgos, en particular, las causas, riesgos y controles
- Fortalecer los controles existentes o formular nuevos que permitan reducir la probabilidad que el riesgo se siga presentando y actualizar el mapa de riesgos del proceso.
- Llevar a cabo un monitoreo permanente.

- En articulación con la Oficina de Control Interno, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.

Capítulo III

Metodología para la Gestión de los Riesgos de Corrupción

14. Identificación de los Riesgos de Corrupción

Para la gestión de los riesgos de corrupción, la metodología no sufrió cambios, y se mantiene la misma metodología conocida. Los riesgos de corrupción son la posibilidad de que, por acción u omisión, se use el poder para desviar la agestión de lo público hacia un beneficio privado, y deben concurrir los cuatro componentes.

Gráfico Nro. 12 Elementos para la descripción de los riesgos de Corrupción

Fuente: *Creado a partir de Secretaria de Transparencia de la Presidencia de la República*

Para la gestión de los riesgos de corrupción se debe tener en cuenta:

- La identificación de los riesgos de corrupción se realiza sobre el **proceso.**

- Anualmente el Líder del Proceso con su equipo de trabajo revisa y actualiza el Mapa de Riesgo de Corrupción de su proceso.

- La Oficina Asesora de Planeación consolida el Mapa de Riesgos de Corrupción, con la información reportada por cada uno de los procesos.

- El Mapa de Riesgos de Corrupción de la Corporación hace parte del Plan de Anticorrupción y Atención al Ciudadano, y se publica en la página web del Concejo de Bogotá D.C. **a más tardar el 31 de enero de cada año.**

- El Jefe de Control Interno desarrolla el seguimiento a la gestión de los riesgos de corrupción.

- Los riesgos de corrupción **NO** pueden aceptarse, siempre debe generar un plan de tratamiento.

15. Valoración de los riesgos de Corrupción

La valoración de los riesgos de corrupción parte de identificar la probabilidad de ocurrencia, expresada en términos de **frecuencia o factibilidad,** identificando el número de eventos materializados en un período determinado, y el impacto que la materialización pueda ocasionar.

Es necesario analizar los factores internos y externos que pueda afectar el proceso y propiciar el riesgo, toda vez que se trata de un hecho que no se ha presentado, pero es posible que suceda.

Por cada uno de los riesgos de corrupción identificados se debe valorar la probabilidad e impacto.

Tabla Nro. 6 - Criterios parar calificar la probabilidad de Riesgos de Corrupción

Nivel	Descriptor	Descriptor	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Mas 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: Tomado de la «Guía para la Administración del Riesgo y el diseño de controles de entidades públicas» Versión 05 – DAFP

Para la identificación del impacto se debe analizar las consecuencias que puede traer la materialización de un riesgo de corrupción, para lo cual se debe diligenciar las preguntas relacionadas en la siguiente tabla:

Tabla Nro. 7- Criterios para calificar el Impacto de los Riesgos de Corrupción

No.	**PREGUNTA:** **Si el riesgo de corrupción se materializa podría …**	Si	No
1	¿Afecta al grupo de funcionarios del proceso?		
2	¿Afecta el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afecta el cumplimiento de la misión de la Entidad?		
4	¿Genera interrupción en la operación de las actividades del proceso?		
5	¿Genera aumento en la carga operativa?		
6	¿Genera pérdida de confianza en la Entidad, afectando su reputación?		
7	¿Genera pérdida de recursos económicos?		
8	¿Da lugar al detrimento de calidad de vida de la comunidad?		
9	¿Genera pérdida de la información de la Entidad?		
10	¿Genera intervención de órganos de control?		
11	¿Da lugar a procesos sancionatorios?		
12	¿Da lugar a procesos disciplinarios?		
13	¿Da lugar a procesos fiscales?		
14	¿Da lugar a procesos penales?		
15	¿Ocasiona lesiones físicas?		
16	¿Afecta la imagen a nivel distrital?		
17	¿Afecta la imagen a nivel nacional?		
18	¿Genera daño ambiental?		

De acuerdo con el número de preguntas que fueron calificadas afirmativamente se califica el nivel de impacto:

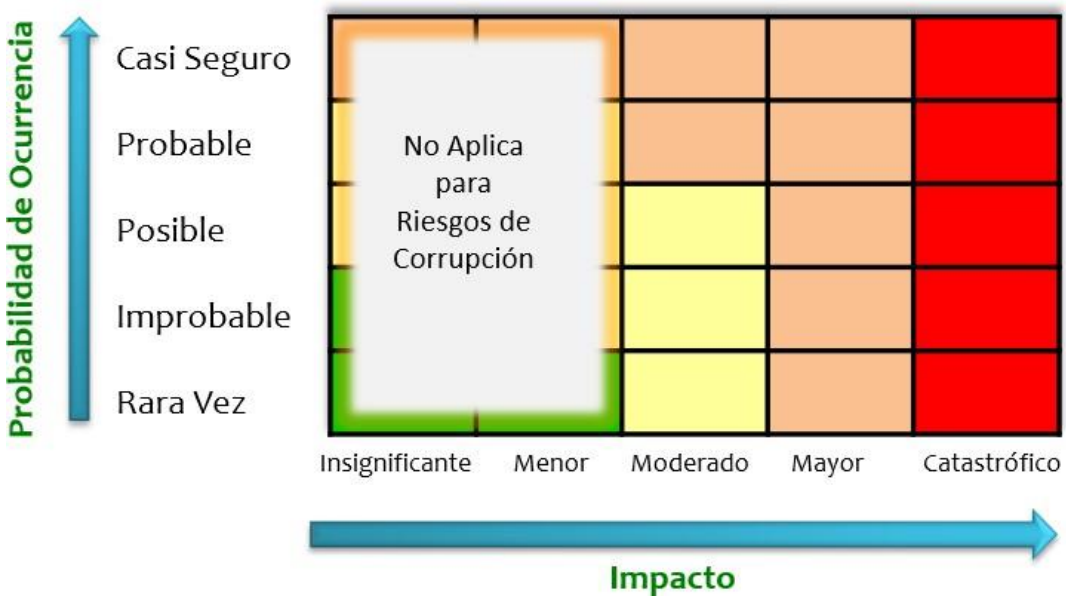
Nivel Impacto	Descriptor	Número de preguntas afirmativas
1	Insignificante	De 1 a 3
2	Menor	De 4 a 7
3	Moderado	De 8 a 11
4	Mayor	De 12 a 15
5	Catastrófico	De 16 a 18

Fuente: Cuadros adaptados de la «Guía para la Administración del Riesgo y el diseño de controles de entidades públicas» Versión 04 – DAFP

Para los riesgos de corrupción, no aplica la categoría **Insignificante o Menor,** toda vez que la materialización de un riesgo de corrupción tiene efectos negativos significativos para la Corporación.

Una vez identificada la probabilidad e impacto de los riesgos de corrupción se debe ubicar en el mapa de calor, el punto de intersección entre la probabilidad y el impacto, lo que nos permite identificar el **nivel de riesgo inherente**:

Gráfico Nro. 13 - Mapa de Calor Riesgos de Corrupción



Fuente: Construcción basada en la «Guía para la Administración del Riesgo y el diseño de controles de entidades públicas» Versión 05 – DAFP y ajustada para uniformidad de los Mapas de Calor de los riesgos de corrupción y gestión.

16. Diseño de Controles para los riesgos de Corrupción

Para el establecimiento de los controles que mitiguen de manera adecuada el riesgo, se debe considerar desde la redacción de este, las siguientes características:

Tabla Nro. 8 - Elementos para el Diseño de Controles a los Riesgos de Corrupción

Elementos para el Adecuado Diseño de Controles	
PASO 1	Debe tener definido el responsable de llevar a cabo la actividad de control
PASO 2	Debe tener en cuenta una periodicidad definida para su ejecución
PASO 3	Debe indicar cuál es el propósito del control
PASO 4	Debe establecer el cómo se realiza la actividad de control
PASO 5	Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
PASO 6	Debe dejar evidencia de la ejecución del control.

Fuente: Creación propia a partir de la «Guía para la Administración del Riesgo y el diseño de controles de entidades públicas» Versión 05 – DAFP

Los controles para que reduzcan el riesgo de corrupción, debe contar con todos los elementos, y únicamente influyen sobre la **probabilidad** de la materialización. Es decir, frente al **impacto** no genera efecto y en consecuencia no opera el desplazamiento en la matriz de calor.

El desplazamiento de un riesgo inherente en su **probabilidad** se realizará de acuerdo con la siguiente tabla:

Tabla Nro. 9 - Resultado de los Controles Riesgos de Corrupción

Control	Efecto
Ataca directamente la causa del riesgo	Desplaza 02 casillas en el eje de probabilidad
Ataca la causa del riesgo en forma indirecta	Desplaza 01 casilla en el eje de probabilidad

Los estudios y en especial la aplicación de distintos métodos de gestión de riesgos han demostrado que ningún riesgo con una medida o medidas de tratamiento se evita o elimina totalmente.

17. Tratamiento de los Riesgos de Corrupción

Una vez determinada la porción del riesgo que subsiste después de la aplicación de controles (riesgo residual) los responsables de los procesos deben evaluar las opciones de mitigación de los riesgos considerando su importancia, probabilidad e impacto. Igualmente, se debe establecer el Plan de tratamiento para los riesgos.

La metodología de gestión de riesgos contempla distintas opciones, como **aceptar, evitar, compartir,** lo cual no aplica para los riesgos de corrupción, solo es posible **reducir,** para lo cual, la primera línea de defensa debe formular un plan de tratamiento.

17.1. Plan de tratamiento de los riesgos de Corrupción

El Líder del Proceso con su equipo de trabajo, deben formular las actividades que permitan reducir la probabilidad o impacto del riesgo y efectuar el monitoreo frecuente de su cumplimiento.

- Actividad: Se debe establecer las acciones que permitirán prevenir o mitigar el riesgo. La descripción de la actividad debe iniciar con un verbo en infinitivo.
- Soporte: Se debe establecer la evidencia del desarrollo de las actividades planteadas.
- Responsable: Es la dependencia, rol o cargo encargado de desarrollar la actividad.
- Tiempo: Es la fecha máxima en la cual se realizará la actividad.

17.2. Responsabilidades en la formulación de los riesgos de corrupción

Para la formulación de los riesgos de corrupción, los líderes de proceso y sus equipos de trabajo cuentan con el acompañamiento metodológico de la Oficina Asesora de Planeación, conforme a los lineamientos que se establecen en el presente documento.

La aprobación de los mapas de riesgo está a cargo del directivo líder del proceso quien revisa y aprueba el mapa de riesgos del proceso y lo remite vía electrónica al correo de la Oficina Asesora de Planeación para su consolidación y gestión para su publicación.

Los riesgos de corrupción se someterán a consulta interna y externa teniendo en cuenta que son parte integral del Plan Anticorrupción y de Atención al Ciudadano. Estas consultas serán gestionadas por la Oficina Asesora de Planeación, con el apoyo de la Dirección Administrativa y la Oficina Asesora de Comunicaciones.

Los mapas de riesgos de los procesos de la Corporación se mantendrán en sus versiones más recientes (tres últimas vigencias) en la carpeta de Planeación SIG de la red interna para conocimiento de los servidores y colaboradores, conforme a las aprobaciones y revisiones que hayan realizado los líderes de proceso.

Los líderes de los procesos realizaran comunicación al interior de sus equipos, los mapas de riesgos aprobados.

Adicionalmente, los riesgos de corrupción como parte del Plan Anticorrupción y de atención al ciudadano – PAAC se publican en la página Web de la Corporación.

17.3. Responsabilidad en el monitoreo y revisión de los riesgos

En el desarrollo de las actividades de los procesos, los directivos líderes de proceso junto con sus equipos de trabajo realizan monitoreo y revisión del comportamiento de los riesgos y al cumplimiento de los planes de tratamiento de los riesgos de forma permanente, conforme a los principios de autocontrol, autorregulación y autogestión.

17.4. Responsabilidad en el monitoreo de los riesgos

La Oficina Asesora de Planeación solicitará el monitoreo a los riesgos de corrupción a los directivos líderes de los procesos (quienes forman parte de la primera y segunda línea de defensa), quienes en conjunto con sus equipos de trabajo realizarán la verificación de la efectividad de los controles y el estado de avance del tratamiento del riesgo, de acuerdo con los siguientes ciclos:

- **Primer Monitoreo:** Con corte al 30 de abril, se solicitará para los tres (3) primeros días del mes de mayo.

- **Segundo Monitoreo:** Con corte al 31 de agosto, se solicitará para los tres (3) primeros días del mes de septiembre.

- **Tercer Monitoreo:** Con corte al 31 de diciembre, se solicitará para los tres (3) primeros días del mes de enero.

Gráfico Nro. 14 – Monitoreo Gestión de Riesgos

17.5. Acciones ante la materialización de riesgos de Corrupción

En el evento de materialización de un riesgo de Corrupción, se deberán emprender acciones en el marco de sus responsabilidades, así:

- 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 que se tomaron las acciones y se actualiza el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.
- En articulación con la Oficina de Control Interno, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.

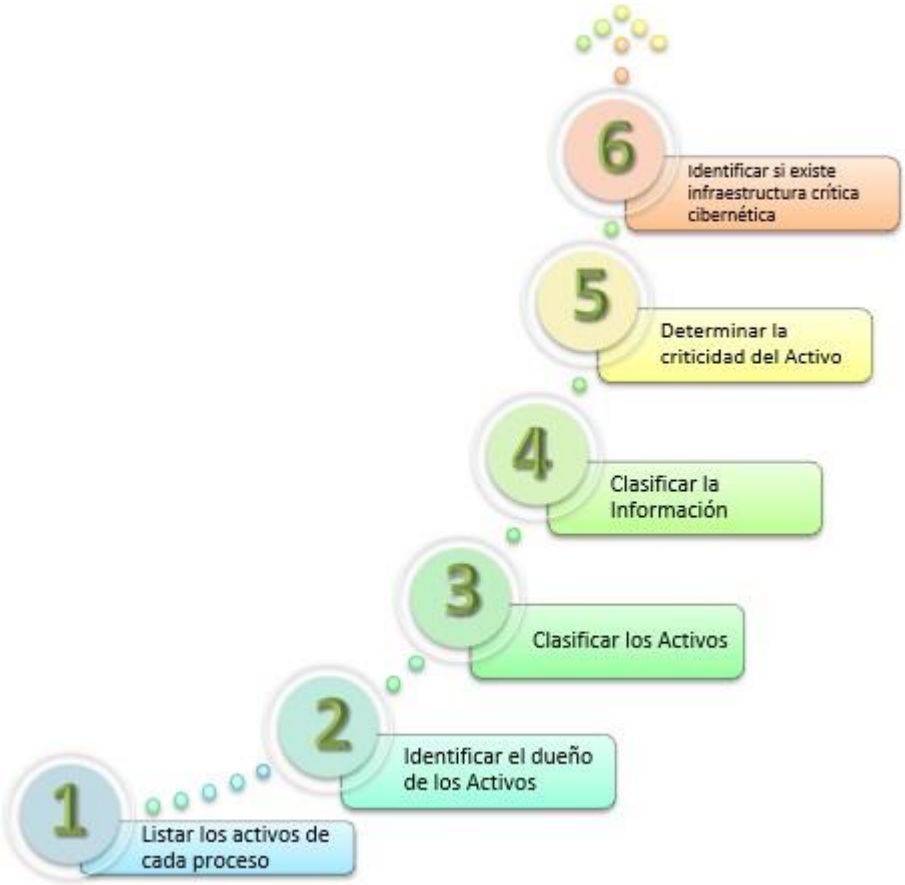
Capítulo IV

Gestión de los Riesgos de Seguridad de la Información

18. Pasos para identificar los activos de seguridad de la información del proceso

Es necesario identificar los pasos de los activos de seguridad de la información del proceso:

Gráfico Nro. 15 – Pasos para identificar los Activos de Seguridad de la Información



Fuente: Tomado a partir de la «Guía para la Administración de riesgos y el diseño de Controles en las entidades públicas» - Departamento Administrativo de la Función Pública - Versión 04

Paso 1. Listar los activos por cada proceso: en cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

PROCESO	ACTIVO	DESCRIPCIÓN
Nómina	Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 14. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Paso 2. Identificar el dueño de los activos: cada uno de los activos identificados deberá tener un dueño designado. Hay que indicar, que sí un activo no posee dueño, nadie se hará responsable ni lo protegerá debidamente.

ACTIVO	DESCRIPCIÓN	DUEÑO DEL ACTIVO
Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos	Director(a) Financiero(a)

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 14. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Paso 3. Clasificar los activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza: información, software, hardware, servicios, intangibles, componentes de red, personas, instalaciones, etc.

TIPO DE ACTIVO	DESCRIPCIÓN
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD, otros) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores). Teniendo en cuenta lo anterior, se puede distinguir como información: • Contratos, • Acuerdos de confidencialidad, • Manuales de usuario, • Procedimientos operativos o de soporte, • Planes para la continuidad del negocio, • Registros contables, • Estados financieros, • Archivos ofimáticos, • Documentos y registros del sistema integrado de gestión, • Bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) • Otros.
Software	Activo informático lógico como: Programas, Herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
Hardware	Equipos físicos de cómputo y de comunicaciones como: Servidores, Biométricos que por su criticidad son considerados activos de información.
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como:

TIPO DE ACTIVO	DESCRIPCIÓN
	Servicios WEB, Intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el '*Good Will*', entre otros
Componentes de Red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, Cableado estructurado y tarjetas de red, *Routers, Switches*, Otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: Personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la entidad.

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, pp. 15, 16. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

ACTIVO	DUEÑO DEL ACTIVO	TIPO DE ACTIVO
Aplicativo de Nómina	Director financiero	Software

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 16. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Paso 4. Clasificar la información: conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.

LEY 1581 DE 2012	LEY 1712 DE 2014
Tiene como principio rector: -Contener datos personales, -No contener datos personales.	Apunta a que la información puede ser: -Pública, -Reservada.

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 16. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf. Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981. Ley 1712 de 2014. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

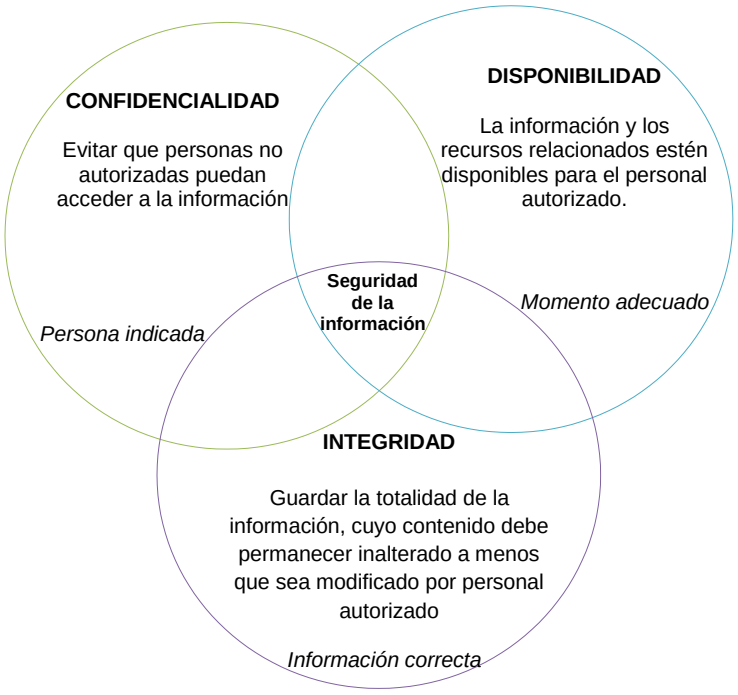
ACTIVO	TIPO DE ACTIVO	LEY 1712 DE 2014	LEY 1581 DE 2012
Aplicativo de Nómina	Software	N/A	N/A

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 16. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Paso 5. Determinar la criticidad del activo: se debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada en cada caso.

En este paso se define las escalas de criticidad ALTA, MEDIA y BAJA para valorar los activos respecto a los tres pilares principales: la confidencialidad, la integridad y la disponibilidad. Estos tres pilares son fundamentales para que haya una seguridad de la información buena.

Gráfico Nro. 16 – Criterios de la Seguridad de la Información



El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la confidencialidad, la

integridad, y la disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Para cada propiedad se deben establecer criterios específicos y lineamientos para el tratamiento adecuado del activo. Asimismo, se delinearon tres niveles que permiten determinar el valor general del activo en la entidad como se mencionó arriba: ALTA, MEDIA y BAJA con el fin de identificar qué activos deben ser tratados de manera prioritaria.

Tabla Nro. 10 – Criterios de Clasificación

Criterios de clasificación		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
INFORMACIÓN PÚBLICA RESERVADA	**ALTA (A)**	**ALTA (1)**
INFORMACIÓN PÚBLICA RESERVADA	**MEDIA (M)**	**MEDIA (2)**
INFORMACIÓN PÚBLICA	**BAJA (B)**	**BAJA (3)**
NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 7. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Tabla Nro. 11 – Niveles de Clasificación

Niveles de clasificación	
ALTA	Activos de información en los cuales la clasificación de la información en dos (02) o todas las propiedades (confidencialidad, integridad y disponibilidad) es **ALTA.**
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (01) de sus propiedades o al menos una de ellas es de nivel **MEDIO.**
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es **BAJA.**

Fuente: Tomado a partir de la guía de gestión de riesgos. Seguridad y privacidad de la información del MINTIC, pp. 6, 7. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

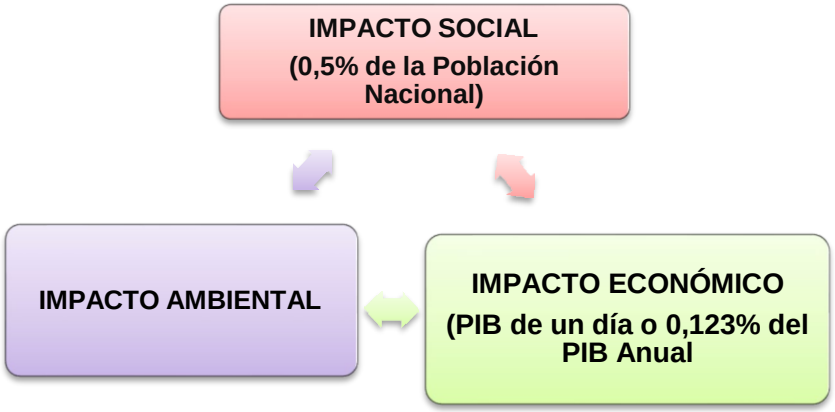
Tabla Nro. 12 – Tabla de valoración de un Activo

ACTIVO	**TIPO DE ACTIVO**	**Criticidad respecto a su confidencialidad**	**Criticidad respecto a su integridad**	**Criticidad respecto a su disponibilidad**	**Nivel de criticidad**
Aplicativo de Nómina	Software	BAJA	MEDIA	BAJA	**MEDIA**

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, p. 17. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Paso 6. Identificar si existe infraestructura crítica cibernética (ICC): la entidad debe identificar y reportar a las instancias y autoridades respectivas en el Gobierno Nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes tres criterios:

Gráfico Nro. 17 – Criterios de Impacto o Afectación ICC



Fuente: Tomado a partir de la Guía para la Administración de riesgos y diseño de controles - DAFP

Resumen pasos 1 al 6

Con base a los seis (06) pasos revisados anteriormente, la entidad podría generar un formato de referencia como el siguiente para generar tanto su procedimiento de identificación e inventario de activos como el formato para hacer su levantamiento. El formato puede variar según la necesidad y normatividad aplicable o si desea integrar otra información.

Tabla Nro. 10 – Identificación de Activos de Proceso

Identificación activos del proceso										
PROCESO	ACTIVO	DESCRIPCIÓN	DUEÑO DEL ACTIVO	TIPO DEL ACTIVO	LEY 1712 DE 2014	LEY 1581 DE 2012	CRITIFICIDAD RESPECTO A LA CONFIDENCIALIDAD	CRITIFICIDAD RESPECTO A LA INTEGRIDAD	CRITIFICIDAD RESPECTO A LA DISPONIBILIDAD	NIVEL DE CRITICIDAD
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Tomado a partir de la guía de riesgos de la Función Pública; y, Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. MINTIC, p. 18. https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+Públicas+-+Guía+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Recomendaciones adicionales para la identificación de activos

Para identificar los activos, es realizar su inventario y clasificación, la entidad pública pueden emplear los siguientes métodos:

- Revisión de flujos o diagramas del proceso
- Revisión de inventarios de activos previos o de otros procesos
- Entrevistas o lluvia de ideas dentro de cada proceso

19. Identificar los riesgos inherentes de seguridad de información

Se podrán identificar los siguientes tres (03) riesgos inherentes de seguridad de la información:

Gráfico Nro. 18 – Riesgos Inherentes de Seguridad de la Información

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización. A continuación, se mencionan un listado de posibles amenazas y vulnerabilidades que podrían materializarse los tres (03) riesgos previamente citados:

19.1. Identificación de Amenazas

Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan –entre otros, las siguientes amenazas:

Tabla Nro. 11 – Tabla de Amenazas

- ***(D)**eliberadas, **(F)**ortuitas o **(A)**mbientales:*

TIPO	AMENAZA	ORIGEN
DAÑO FÍSICO	Fuego	F,D,A
	Agua	F,D,A
	Contaminación	F,D,A
	Accidente importante	F,D,A
	Destrucción del equipo o medio	F,D,A
	Polvo, corrosión, congelamiento	F,D,A
	Fenómenos climáticos	A
EVENTOS NATURALES	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
PÉRDIDA DE LOS SERVICIOS ESENCIALES	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Pérdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D,F
PERTURBACIÓN DEBIDA A LA RADIACIÓN	Radiación electromagnética	D,F
	Radicación térmica	D,F
	Impulsos electromagnéticos	D,F
COMPROMISOS DE LA INFORMACIÓN	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D,F
	Datos provenientes de fuentes no confiables	D,F
	Manipulación de hardware	D
	Manipulación de software	D
	Detección de la posición	D,F
FALLAS TÉCNICAS	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema del software	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información	F
ACCIONES NO AUTORIZADAS	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso del software falso o copiado	D

TIPO	AMENAZA	ORIGEN
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
COMPROMISOS DE LAS FUNCIONES	Error en el uso	D,F
	Abusos de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: *Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, pp. 19,20. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf*

-Amenazas dirigidas por el hombre:

Empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla Nro. 12 – Amenazas dirigidas por el hombre

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
PIRATA INFORMÁTICO, INTRUSO ILEGAL	*Reto *Ego *Rebelión *Estatus *Dinero	*Piratería *Ingeniería social *Intrusión, accesos forzados al sistema *Acceso no autorizado
CRIMINAL DE LA COMPUTACIÓN	*Destrucción de la información *Divulgación ilegal de la información *Ganancia monetaria *Alteración no autorizada de los datos	*Crimen por computador *Acto fraudulento *Soborno de la información *Suplantación de identidad *Intrusión en el sistema
TERRORISMO	*Chantaje *Destrucción *Explotación *Venganza *Ganancia política *Cubrimiento de los medios de comunicación	*Bomba/Terrorismo *Guerra de la información *Ataque contra el sistema DOS *Penetración en el sistema *Manipulación en el sistema
ESPIONAJE INDUSTRIAL (INTELIGENCIA, EMPRESAS, GOBIERNOS EXTRANJEROS, OTROS INTERESES)	*Ventaja competitiva *Espionaje económico	*Ventaja de defensa *Ventaja política *Explotación económica *Hurto de información *Intrusión en privacidad personal *Ingeniería social *Penetración en el sistema *Acceso no autorizado al sistema

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
INTRUSOS (EMPLEADOS CON ENTRENAMIENTO DEFICIENTE, DESCONTENTOS, MALINTENCIONADOS, NEGLIGENTES, DESHONESTOS O DESPEDIDOS)	*Curiosidad *Ego *Inteligencia *Ganancia monetaria *Venganza *Errores y omisiones no intencionales (por ejemplo, error en el ingreso de datos, error de programación)	*Soborno de información *Ingreso de datos falsos o corruptos *Interceptación *Código malicioso *Venta de información personal *Errores en el sistema *Intrusión en el sistema *Sabotaje del sistema *Acceso no autorizado al sistema

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, pp. 21,22. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

19.2. Identificación de Vulnerabilidades

Puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tabla Nro. 13 – Tipos de Vulnerabilidades

TIPO	VULNERABILIDADES
HARDWARE	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o 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

TIPO	VULNERABILIDADES
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
LUGAR	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
ORGANIZACIÓN	Ausencia de procedimiento de registro / retiro de usuarios
	Ausencia de proceso para supervisión de derecho de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	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: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, pp. 21,22. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Hay que resaltar que 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 puede explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Se presenta a continuación un ejemplo de **relación entre vulnerabilidad** de acuerdo con el **tipo de activos y las amenazas:**

Tabla Nro. 14 – Relación entre Vulnerabilidades y Amenazas

TIPO	Ejemplo de VULNERABILIDADES	Ejemplo de AMENAZAS
HARDWARE	Mantenimiento insuficiente / Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía

TIPO	Ejemplo de VULNERABILIDADES	Ejemplo de AMENAZAS
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección física	Hurtos medios o documentos
	Falta de cuidado en la disposición final	Hurtos medios o documentos
	Copia no controlada	Hurtos medios o documentos
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetro	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
RED	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones

TIPO	Ejemplo de VULNERABILIDADES	Ejemplo de AMENAZAS
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
	Ubicación en área susceptible de inundación	Destrucción de equipos o medios
	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos

TIPO	Ejemplo de VULNERABILIDADES	Ejemplo de AMENAZAS
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo

TIPO	Ejemplo de VULNERABILIDADES	Ejemplo de AMENAZAS
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

Fuente: Tomado a partir del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Anexo Técnico (Anexo 4 – DAFP -) -, pp. 23 - 27. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

20. Descripción del Riesgo en Seguridad de la Información

Los riesgos de seguridad de la información se basan en la afectación de los tres criterios en un activo o un grupo de activos dentro del proceso: pérdida de confidencialidad (**PC**), pérdida de integridad (**PI**) y pérdida de disponibilidad (**PD**).

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización:

Tabla Nro. 15 – Matriz descripción riesgos en la seguridad de la información

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	VULNERABILIDADES	CONSECUENCIAS
Base de datos de Nómina	**PI**	*-Falta de políticas de seguridad.* *-Ausencia de políticas de seguridad* *-Contraseñas sin protección y mecanismos de autenticidad*	Falsificación de derechos	COMPROMISOS DE LAS FUNCIONES	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	*Posible retraso en el pago de nómina*

Fuente: Tomado a partir de la guía de riesgos de la Función Pública

21. Valoración del riesgo en la seguridad de la información

Esta se hace de forma cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo en la seguridad de la información versus el impacto del mismo, obteniendo al final la matriz denominada *Matriz de Calificación, Evaluación y Respuestas a los Riesgos* con la cual presenta la forma de calificar los riesgos con los niveles de *impacto* y *probabilidad*, así como las zonas de riesgo presentando las posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra:

Tabla Nro. 16 – Mapa de calor Riesgos en la Seguridad de la Información

PROBABILIDAD	**IMPACTO**				
	INSIGNIFICANTE (1)	**MENOR (2)**	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	B	B	M	A	A
IMPROBABLE (2)	B	B	M	A	E
POSIBLE (3)	B	M	A	E	E
PROBABLE (4)	M	A	A	E	E
CASI SEGURO (5)	A	A	E	E	E
B: ZONA DE RIESGO BAJO: *Asumir el riesgo*					
M: ZONA DE RIESGO MODERADA: *Asumir el riesgo, reducir el riesgo*					
A: ZONA DE RIESGO ALTO: *Reducir el riesgo, evitar, compartir o transferir*					
E: ZONA DE RIESGO EXTREMA: *Reducir el riesgo, evitar, compartir o transferir*					

Fuente: Tomado de la guía de gestión de riesgo MINTIC, p. 33. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

22. Controles asociados a la seguridad de la información

Le entidad pública podrá mitigar/tratar los riesgos de la seguridad de la información empelando los siguientes controles, tomados del *Anexo 4 del estándar ISO/IEC 27001:2013*, *y los dominios a los que pertenecen,* siempre y cuando se ajusten al análisis de riesgos.

Tabla Nro. 16 – Controles de Referencia para la Mitigación de Riesgos de Seguridad de la Información (Tomado de la Norma Técnica ISO 27000:2003

El contenido de la tabla se puede interpretar de la siguiente manera:

A.X = DOMINIO
A.X.X = OBJETIVO DE CONTROL
A.X.X.X = CONTROLES

CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (Tomado de la Norma Técnica ISO 27000:2003)		
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información	**Control:** Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes
A.5.1.2	Revisión de las políticas para seguridad de la información	**Control:** Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	**Organización interna.**	**Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**
A.6.1.1	Roles y responsabilidades para la seguridad de información	**Control**: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	**Control**: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	**Control**: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	**Control**: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	**Control**: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.

A.6.2	**Dispositivos móviles y teletrabajo**	**Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.**
A.6.2.1	Política para dispositivos móviles	**Control**: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	**Control:** Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1	**Antes de asumir el empleo**	**Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.**
A.7.1.1	Selección	**Control**: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	**Control**: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**	**Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.**
A.7.2.1	Responsabilidades de la dirección	**Control**: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**Control:** Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	**Control:** Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Terminación o cambio de empleo**	**Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**Control**: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se

		deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8 GESTIÓN DE ACTIVOS		
A.8.1	**Responsabilidad por los activos**	**Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**
A.8.1.1	Inventario de activos	**Control**: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	**Control**: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos	**Control**: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	**Control**: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	**Clasificación de la información**	**Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.**
A.8.2.1	Clasificación de la información	**Control**: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	**Control**: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	**Control**: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3	**Manejo de Medios**	**Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.**
A.8.3.1	Gestión de medios removibles	**Control**: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización
A.8.3.2	Disposición de los medios	**Control**: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	**Control**: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte

A.9 CONTROL DE ACCESO		
A.9.1	**Requisitos del negocio para control de acceso**	**Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.**
A.9.1.1	Política de control de acceso	**Control:** Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red	**Control**: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	**Gestión de acceso de usuarios**	**Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**
A.9.2.1	Registro y cancelación del registro de usuarios	**Control**: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	**Control:** Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	**Control**: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	**Control:** La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	**Control:** Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	**Control**: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	**Responsabilidades de los usuarios**	**Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**
A.9.3.1	Uso de la información de autenticación secreta	**Control:** Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**	**Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.**
A.9.4.1	Restricción de acceso Información	**Control:** El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

A.9.4.2	Procedimiento de ingreso seguro	**Control**: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	**Control:** Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	**Control:** Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	**Control:** Se debería restringir el acceso a los códigos fuente de los programas.
A.10 CRIPTOGRAFÍA		
A.10.1	**Controles criptográficos**	**Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**
A.10.1.1	Política sobre el uso de controles criptográficos	**Control**: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	**Control:** Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1	**Áreas seguras**	**Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**
A.11.1.1	Perímetro de seguridad física	**Control**: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	**Control:** Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**Control:** Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	**Control**: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	**Control:** Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	**Control:** Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros

		puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	**Equipos**	**Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**
A.11.2.1	Ubicación y protección	**Control**: Los equipos deberían estar ubicados y protegidos para reducir los de los equipos riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	**Control**: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	**Control**: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	**Control**: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas
A.11.2.5	Retiro de activos	**Control**: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**Control**: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	**Control**: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	**Control**: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	**Control**: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1	**Procedimientos operacionales y responsabilidades**	**Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**
A.12.1.1	Procedimientos de operación documentados	**Control**: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	**Control:** Se deberían controlar los cambios en la organización, en los procesos de negocio, en las

		instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	**Control:** Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	**Control**: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	**Protección contra códigos maliciosos**	**Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**
A.12.2.1	Controles contra códigos maliciosos	**Control:** Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	**Copias de respaldo**	**Objetivo: Proteger contra la perdida de datos.**
A.12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	**Registro y seguimiento**	**Objetivo: Registrar eventos y generar evidencia.**
A.12.4.1	Registro de eventos	**Control:** Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	**Control**: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	**Control:** Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	**Control:** Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	**Control de software operacional**	**Objetivo: Asegurar la integridad de los sistemas operacionales.**
A.12.5.1	Instalación de software en sistemas operativos	**Control:** Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	**Gestión de la vulnerabilidad técnica**	**Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.**
A.12.6.1	Gestión de las vulnerabilidades técnicas	**Control:** Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la

		organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	**Control:** Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	**Consideraciones sobre auditorias de sistemas de información**	**Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**
A.12.7.1		
A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1	**Gestión de la seguridad de las redes**	**Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**
A.13.1.1	Controles de redes	**Control**: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	**Control:** Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	**Control:** Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	**Transferencia de información**	**Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**
A.13.2.1	Políticas y procedimientos de transferencia de información	**Control**: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	**Control:** Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	**Control:** Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**Control:** Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
A.14.1	**Requisitos de seguridad de los sistemas de información**	**Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto**

		incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	**Control**: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	**Control:** La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	**Control:** La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**	**Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**
A.14.2.1	Política de desarrollo seguro	**Control:** Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	**Control:** Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**Control:** Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	**Control:** Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros	**Control:** Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información
A.14.2.6	Ambiente de desarrollo seguro	**Control:** Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	**Control:** La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

A.14.2.8	Pruebas de seguridad de sistemas	**Control**: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	**Control**: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	**Datos de prueba**	**Objetivo: Asegurar la protección de los datos usados para pruebas.**
A.14.3.1	Protección de datos de prueba	**Control**: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15 RELACIÓN CON LOS PROVEEDORES		
A.15.1	**Seguridad de la información en las relaciones con los proveedores**	**Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.**
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**Control:** Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	**Control**: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de Infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	**Control:** Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	**Gestión de la prestación de servicios con los proveedores**	**Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.**
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**Control:** Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	**Control:** Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		

A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	**Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**
A.16.1.1	Responsabilidad y procedimientos	**Control**: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	**Control**: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	**Control:** Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**Control:** Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	**Control**: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**Control**: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	**Control:** La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
A.17.1	**Continuidad de seguridad de la información**	**Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.**
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**Control:** La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**Control**: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Control:** La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	**Redundancias**	**Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.**
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	**Control:** Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18 CUMPLIMIENTO		
A.18.1	**Cumplimiento de requisitos legales y contractuales**	**Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	**Control**: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	**Control:** Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	**Control:** Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	**Control:** Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	**Control**: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	**Revisiones de seguridad de la información**	**Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.**
A.18.2.1	Revisión independiente de la seguridad de la información	**Control:** El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar

		independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**Control**: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	**Control:** Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: Tomado del Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, p. 29-38.

https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+Públicas+-+Guía+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

23. Formato Mapa Riesgo Seguridad de la Información

RIESGO	ACTIVO	TIPO	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR	
Base de datos de Nómina	PI	COMPROMISOS DE LAS FUNCIONES	Falsificación de derechos	POSIBLE (3)	MENOR (2)	M (Cruce matriz: posible versus menor)	*Asumir el riesgo, reducir el riesgo*	A.9.1.1 A.9.4.2 A.9.4.3	Política de control de acceso Procedimiento de ingreso seguro Sistema de gestión de contraseñas	Sistemas	Tercer semestre del año en curso	EFICACIA (*)	EFECTIVIDAD (**)

*=

Índice de cumplimiento actividades = (# de actividades cumplidas / # de actividades programadas) * 100

** =

Efectividad del Plan de Manejo de Riesgo = (# de modificaciones no autorizadas)

24. CONTROL DE CAMBIOS

Versión	Descripción	Fecha
01	Se elabora la Política de Administración del riesgo, teniendo como base la metodología planteada por la Dirección de Gestión y Desempeño Institucional del Departamento Administrativo de la Función Pública en la *«Guía para la administración del riesgo y el diseño de controles en entidades públicas»* Versión 05, Diciembre 2020. El documento se presentó y aprobó en Comité Institucional de Coordinación del Control Interno realizado el 01 de diciembre del 2022.	20-Dic-2022

26. RUTA DE APROBACIÓN

ELABORÓ O ACTUALIZÓ:	REVISIÓN METODOLÓGICA OAP:	APROBÓ:
NELSON GUTIERREZ SILVA Jefe Oficina Asesora de Planeación		
Firmado digitalmente por Francisco Javier Bernal García FRANCISCO JAVIER BERNAL GARCÍA Profesional Especializado 222-04 Dirección Administrativa-Proceso Sistemas		
WILLIAM DARÍO AVILA DIAZ Profesional Especializado 222-04 Dirección Administrativa-Proceso Sistemas	DIANA CAROLINA ÁVILA PINZÓN Profesional Universitario 219-03	SAMIR JOSÉ ABISAMBRA VESGA Presidente Concejo de Bogotá D.C.
Carolina Parra M. CAROLINA PARRA MARTÍNEZ Profesional Especializado 222-05 Oficina Asesora de Planeación		