1. OBJETIVO

Establecer una orientación metodológica que facilite la comprensión e implementación de las fases de administración del riesgo, dando lineamientos para la identificación, análisis, valoración de controles y el establecimiento de planes de tratamiento dirigidos a prevenir la ocurrencia o minimizar su impacto en caso de su materialización de los riesgos o eventos que puedan afectar negativamente el logro de los objetivos de los procesos, definiendo las responsabilidades en la administración de los mismos, los controles, su seguimiento y la pertinencia de las políticas para su tratamiento.

2. ALCANCE

Esta guía tiene como alcance la gestión del riesgo partiendo desde la identificación del contexto estratégico del Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial de Chía (IDUVI), hasta el seguimiento de los planes de manejo, se incluyen los riesgos de corrupción.

3. DEFINICIONES

- **Administración de riesgos:** Conjunto de elementos de control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La administración del riesgo contribuye a que la entidad consolide su Sistema de Control Interno y a que se genere una cultura de autocontrol y autoevaluación al interior de la misma. (DAFP, Guía de administración del riesgo).

- **Activos:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital

- **Análisis del Riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo

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

- **Gestión del Riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de objetivos.

- **Control:** cualquier medida que tome la organización y otras partes para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planificar, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzaran los objetivos y metas. (MECI 2014).

- **Control Adecuado:** es el que está presente si la dirección ha planificado y organizado (diseñado) las operaciones de tal manera que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica (MECI 2014).

- **Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y ocurrencia (DAFP, Guía de administración del riesgo, 2011 p. 13)

- **Riesgo de corrupción:** Posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular. (Secretaria de Transparencia Presidencia de la

República, Departamento Nacional de Planeación, Departamento Administrativo de la Función Pública, Oficina de las Naciones Unidas contra la Droga y el Delito, Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano, 2012, p .10)

- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos, y sociales así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos físicos relacionados con el ambiente físico, digital y las personas. (DAFP, Guía de administración del riesgo, 2018 p. 8).

- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, esta puede ser medida por términos de frecuencia o factibilidad . (DAFP, Guía de administración del riesgo, 2018 p. 8).

- **Impacto:** Se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo. (DAFP, Guía de administración del riesgo, 2018 p.8).

- **Evaluación de riesgo:** Tiene como finalidad establecer si se realiza y aplica correctamente los métodos, políticas y procedimientos establecidos para la administración de riesgo.

- **Autoseguimento al mapa de riesgo:** Consiste en el monitoreo a los riesgos identificados para asegurar la eficacia de los controles y acciones definidas para mitigar el riesgo y evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la administración del riesgo para aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

- **Riesgo Inherente:** es aquel al que se enfrenta la entidad en usencia de acciones de la dirección para modificar su probabilidad e impacto (DAFP, Guía de administración del riesgo, 2018 p.8).
- **Riesgo Residual:** Es aquel riesgo que subsiste, después de haber valorado los controles definidos para su mitigación o prevención de su ocurrencia.

4. MARCO NORMATIVO RELACIONADO

Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Directiva presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.
Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

5. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO.

5.1 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El objetivo de la política de administración del riesgo en el Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial de Chía (IDUVI), es preservar la eficacia estratégica y operativa a través de la identificación, análisis, valoración, control, monitoreo y actualización de los riesgos relacionados al desarrollo de su Misión y en cumplimiento de sus objetivos institucionales.

Esta política tiene un alcance de aplicabilidad para todos los procesos del Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial de Chía (IDUVI) sin exclusión alguna.

Para el desarrollo de la administración del riesgo se deben seguir las siguientes estrategias:

La Gestión del Riesgo está dirigida a que se establezcan acciones conducentes a reducir, evitar, transferir o compartir el riesgo con base en su evaluación.

La definición del plan de manejo del riesgo debe estar encaminada a su mitigación. No obstante, se tendrá como referencia el análisis costo/beneficio para la administración de los mismos.

Los controles y las acciones contenidas en el plan de manejo son objeto de autocontrol por parte de todos los servidores públicos y/o particulares que ejercen funciones públicas, de autoseguimiento por parte del líder de proceso, así como de evaluaciones por parte de la Oficina de Control Interno.

Los riesgos de corrupción no tendrán nivel de aceptación ya que por su naturaleza será inaceptable su ocurrencia en la entidad.

La política de administración del riesgo, se desarrollara a través de la Guía para la administración del Riesgo, como adaptación de la Guía del Departamento Administrativo de la Función Pública (DAFP) Versión 4 y en el marco de la Ley 1474 de 2011 (Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano en lo aplicable a la gestión de los riesgos de corrupción).

5.2 CONTEXTO ESTRATÉGICO ORGANIZACIONAL

Para la definición del contexto estratégico organizacional es fundamental partir de la misión, los objetivos, el plan estratégico, la naturaleza del IDUVI, así como los objetivos de los procesos estratégicos, misionales, de apoyo y de evaluación, es entonces, que el contexto estratégico es el punto de partida de una identificación eficiente de los factores tanto internos como externos, que pueden ser generadores de riesgos y que por tanto afectan negativamente en el cumplimiento de la misión y de los objetivos institucionales.

El análisis del contexto estratégico organizacional se realiza a partir del conocimiento e identificación de situaciones del entorno o externas (de carácter social, económico, cultural, de orden público, político, legal, tecnológico, ambiental, etc.) que afectan o pueden afectar al cumplimiento de los objetivos definidos en los procesos; y las particularidades internas de la institución (como la estructura organizacional, modelo de operación, asignación presupuestal, tipo de vinculación de personal, cumplimiento de los planes, sistemas de información, procesos, procedimientos, entre otros) (DAFP, Guía para la administración del riesgo, 2018, p. 20)

Para la definición del contexto se aplican varias herramientas y técnicas como por ejemplo: entrevistas con expertos en el proceso, lluvias de ideas, diagramas de flujo, herramientas de estudio “causa y efecto” y análisis por escenarios, entre otros. Estas herramientas deben ser tenidas en cuenta en cada fase de la Administración de Riesgos, ya que la participación activa de los participantes (líderes y cogestores, principalmente) permitirá una correcta identificación, análisis, valoración e implementación de los planes de tratamiento de los riesgos.

El contexto estratégico será modificado teniendo en cuenta entre otros los siguientes factores: los resultados de los ejercicios de planeación que realice el IDUVI y afecten los objetivos del mapa estratégico, actualización o cambios en los Planes y Proyectos de la Unidad, evaluaciones del Plan Estratégico, Diagnósticos Institucionales, cambios en su estructura orgánica etc.

Para lo anterior, se ha dispuesto la primera etapa para la administración de riesgos la definición del entorno estratégico para la identificación de las circunstancias y agentes generadores de riesgo provenientes del entorno o de la misma entidad, la cual será el marco de referencia la identificación de los riesgos en los procesos del IDUVI.

Entiéndase como agentes generadores todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

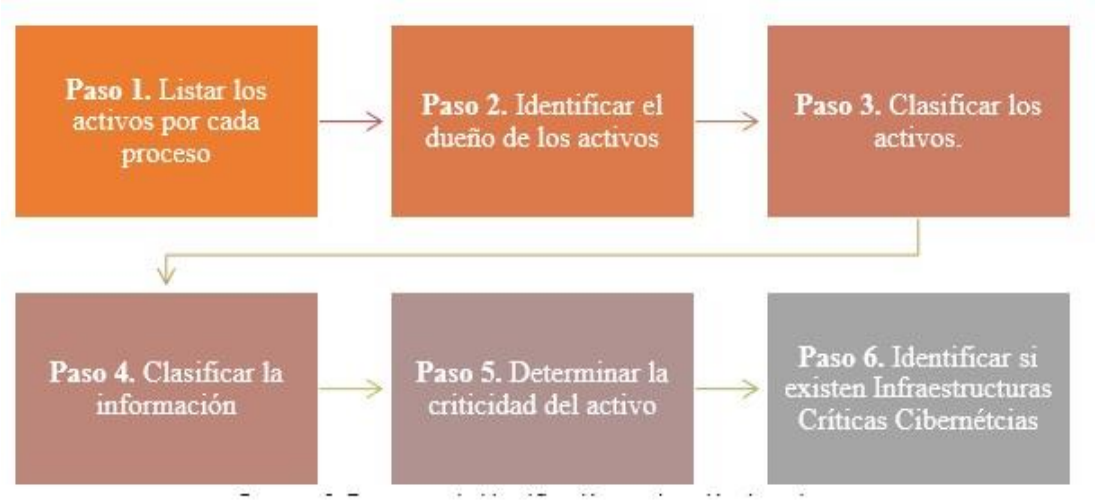
El IDUVI define el contexto estratégico organizacional para identificar los factores externos e internos que pueden ocasionar la presencia de riesgos y para aportar información que facilite y enriquezca las demás etapas de la administración del riesgo (Ver tabla 1):

Tabla N°1. Ejemplo de Contexto Estratégico Institucional

FACTORES CON POSIBLES RIESGOS					
No	**FACTORES EXTERNOS**	**Descripción**	**No**	**FACTORES INTERNOS**	**Descripción**
1	**Tecnológicos**	No se realizan las actualizaciones de hardware y software	1	**Talento Humano**	* Baja ejecución de los planes de capacitación * Desconocimiento de la normatividad aplicada * Resistencia al cambio.
2	**Jurídicos**	Dinámica en las actualización de normatividad	2	**Procesos**	* Procesos en etapa de maduración * Controles débiles en los procesos
3	**Relación con otras entidades**	Demoras en la respuesta de comunicaciones enviadas a otras entidades relacionadas.	3	**Tecnología**	Número de equipos insuficiente y algunos obsoletos

5.3 IDENTIFICACIÓN DE ACTIVOS

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad el cual nombrara el Comité de Gestión de Desempeño del Insituto, para hacer la identificación se deberán seguir los siguientes pasos:



Pasos para la identificación y valoración de activos.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

En cumplimiento a lo anterior, debe tenerse en cuenta el análisis de objetivos del proceso junto con los objetivos estratégicos de tal manera que se identifique todos los activos que deben protegerse para garantizar el funcionamiento interno con el funcionamiento de cara al ciudadano.

En el caso especifico de los activos relacionados con seguridad digital se establecera el tratamiendo dado según la sección **4.1.6 del anexo 4 "**Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

1. Listar los activos por cada proceso: En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.
2. Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño designado, si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
3. Clasificar los activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.
4. Clasificar la información: Realizar la clasificación de 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. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información.
5. Determinar la criticidad del activo (Valoración 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 de cada caso.

5.3 IDENTIFICACIÓN DEL RIESGO

La fase de la identificación del riesgo, debe basarse en el resultado del análisis del contexto estratégico, y debe partir de los objetivos del IDUVI y del proceso objeto de trabajo. La identificación del riesgo debe tener en cuenta el conocimiento previo de situaciones que impiden o que pueden llegar a obstaculizar el cumplimiento de un objetivo institucional, la obtención de resultados, el cumplimiento de un requisito legal, organizacional o externo, la satisfacción de los usuarios, dificultades en el proceso, fallas en los productos y/o servicios que generados por el proceso; se pueden tomar como referencias metodologías como la espina de pescado, análisis de escenarios, entrevistas y encuestas, entre otros.
Y se usaran las siguientes preguntas:

- **QUE PUEDE SUCEDER?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- **COMO PUEDE SUCEDER?** Establecer las causas a partir de los factores determinados en el contexto.
- **CUANDO PUEDE SUCEDER?** Determinar de acuerdo con el desarrollo del proceso.
- **QUE CONSECUENCIA TENDRÍA SU MATERIALIZACIÓN**? Determinar los posibles efectos por la materialización del riesgo.

Es importante aplicar los siguientes parámetros para la identificación de los riesgos, para cada riesgo identificado, se debe determinar en primera instancia se tendrá en cuenta el análisis de **causas** que lo originan, con base en los factores Internos y/o externos analizados, seguido de una descripción de cada uno y finalmente definir los posibles efectos o consecuencias en caso de materializarse, dado que los riesgos pueden ser transversales a los procesos es importante en esta etapa, que se valide que el proceso que lo identifica, tenga la suficiente potestad para controlarlo de lo contrario se debe trasladar de forma participativa al proceso que pueda administrarlo.

Con el fin de establecer con mayor facilidad el análisis del impacto, durante el proceso de identificación del riesgo se realiza una clasificación sobre los tipos de riesgos así:

- **Riesgos estratégicos[1]:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad
- **Riesgos Gerenciales [1]:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección
- **Riesgos de imagen o Reputacional [1]:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas. Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Riesgos operativos**[1] posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad
- **Riesgos financieros**[1]**:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

[1] DAFP, Guía para la administración del riesgo, 2018 p. 28.

- **Riesgos de cumplimiento**[1]**:** posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
- **Riesgos de tecnología**[1]**:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Riesgos de Seguridad Digital**[1]**:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgos de corrupción**[1]**:** Posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

Adicionalmente, se debe realizar una identificación de las consecuencias de la materialización del riesgo, es decir, de los efectos de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental, entre otros.

Las consecuencias (efectos) asociadas a cada riesgo se pueden clasificar en:

- Pérdidas económicas
- Pérdida de imagen
- Insostenibilidad financiera
- Incumplimientos legales
- Daños a la integridad física
- Llamados de atención
- Sanciones
- Reprocesos
- Insatisfacción del usuario
- Otras adicionales que se generan con la descripción del riesgo.

Cuando se generen dudas con respecto a si se identificó un riesgo o realmente lo identificado es una causa, se sugiere aplicar la siguiente frase:

"Debido a **CAUSA** *puede ocurrir* **RIESGO** *lo que conllevaría a* **EFECTO***"*

Para nuestro ejemplo de riesgo *"Incumplimiento en la atención de las PQRS interpuestos por los usuarios grupos de interés",* se analizó que se ha presentado vencimientos en la atención a las peticiones y quejas de los usuarios, se identificaron como posibles causas las debilidades en los controles de los vencimientos de los términos dado que se realizan de forma manual sumado a ello se cuentan con equipos de cómputo insuficientes y obsoletos que dificultan su control.

IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Para los riesgos de seguridad digital se Debera tener en cuenta en la identificación del contexto todo lo relacionado a los siguientes factores del entorno digital donde los externos afectan a la entidad y los internos a los procesos :

ENTIDAD		PROCESOS
Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros		Identificación de los procesos y su respectiva caracterización
Flujos de información y los procesos de toma de decisiones		Detalle de las actividades que se llevan a cabo en el proceso
Empleados, contratistas		Flujos de información
Objetivos estratégicos y la forma de alcanzarlos		Identificación y actualización de los activos en la cadena de valor de la entidad pública
La misión, visión, valores y cultura de la organización		Recursos
Sus políticas, procesos y procedimientos		Alcance del proceso
Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros)		Relaciones con otros procesos de La entidad pública
Toda la estructura organizacional		Cantidad de ciudadanos afectados por el proceso
Roles y responsabilidades		Procesos de gestión de riesgos que se tienen actualmente implementados
Sistemas de información o servicios		Personal involucrado en la toma de decisiones

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

5.5 ANÁLISIS DEL RIESGO

La calificación del riesgo busca establecer la **probabilidad** de ocurrencia de los riesgos y su **impacto** en caso de materializarse para determinar la zona de exposición al riesgo, que depende de nivel de calificación de estos dos elementos.

La probabilidad puede ser medida con criterios de frecuencia, determinando el número de veces que un riesgo ha sucedido en un tiempo determinado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. El impacto se mide según el grado en que las consecuencias o efectos pueden perjudicar a la organización si se materializa el riesgo. [2]

[2] DAFP, Guía para la administración del riesgo, 2018, p. 39.

Tabla 3. Tabla valoración probabilidad

	PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN	FRECUENCIA
	1 Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
	2 Improbable	El evento puede ocurrir en algún momento	Al menos de 1 vez en los últimos 5 años.
para los Riesgos de corrupción solo se aplicará esta valoración	*3 Posible*	El evento podría ocurrir en algún momento	Al menos de 1 vez en los últimos 2 años.
	4 Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en el último año.
	5 Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Nota: Para la probabilidad de materialización de los ***riesgos de corrupción*** se considerarán solo los siguientes criterios[3]:

(i) **Probable:** se espera que el evento ocurra en la mayoría de las circunstancias y
(ii) **Casi seguro:** El evento probablemente ocurrirá en la mayoría de las circunstancias.

En cuanto al impacto se medirá de acuerdo a al tipo de riesgo para riesgos de gestión se aplicará la siguiente tabla :

FORMATO PARA DETERMINAR EL IMPACTO DEL RIESGO DE GESTIÓN

NOMBRE DEL RIESGO DE GESTIÓN		
Nivel	**Impacto Cuantitativo**	**Impacto Cualitativo**
CATASTROFICO	. Impacto que afecte la ejecución presupuestal en un valor ≥50% .Pérdida de cobertura en la prestación de los servicios de la entidad ≥50% .Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% . Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad	. Interrupción de las operaciones de la entidad por más de cinco (5) días .Intervención por parte de un ente de control u otro ente regulador .Pérdida de información crítica para la entidad que no se puede recuperar . Incumplimiento en las metas y objetivos institucionales afectando de forma grave

[3] Secretaria de transparencia de la Presidencia de la República .

		la ejecución presupuestal . Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados
MAYOR	Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad	Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	Impacto que afecte la ejecución presupuestal en un valor ≥ 5 % . - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de	Interrupción de las operaciones de la entidad por algunas horas.

	los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: Adaptado de Instituto de Auditores Internos COSO ERM. Agosto 2004 / DAFP Guia de administración del riesgo pag 41 - 2019

Para determinar el impacto de los riesgos de seguridad digital se empleara la información contenida en la siguiente tabla:

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGUIRDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥20% de la población. Afectación ≥20% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad
MENOR	2	Afectación ≥40% de la población. Afectación ≥40% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de 30 días de recuperación	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥60% de la población. Afectación ≥60% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de 8 semanas de recuperación	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.

MAYOR	**4**	Afectación ≥80% de la población. Afectación ≥80% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de 10 meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
CATASTROFICO	**5**	Afectación ≥100% de la población. Afectación ≥ 100% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de 2 años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Fuente: Ministerio de Tecnologias de la Infornación y Comunicaciones 2017 / DAFP Guia de administración del riesgo pag 43 - 2019

Una vez determinada la probabilidad y su impacto del riesgo, se identifica su cruce en la **Matriz de Calificación, Evaluación y Respuesta a los Riesgos** de esta forma es posible para establecer la **zona de exposición del riesgo** (Zona de riesgo baja, moderada, alta o extrema y distinguir si los riesgos son aceptables, tolerables, moderados, importantes o inaceptables, para así fijar las prioridades de las acciones requeridas para su tratamiento, este primer análisis se denomina ***RIESGO INHERENTE***[4] donde no se tienen en cuenta los controles.
Para el ejemplo en desarrollo se clasificó el impacto como “moderado”, y su probabilidad en “probable”, lo cual nos establece en una zona de exposición al riesgo como “Zona de riesgo alta”.

[4] Departamento Administrativo de la Función Pública (DAFP, Guía para la administración del riesgo, 2018, p. 8)

Ejemplo análisis del riesgo - Calificación del riesgo inherente – Riesgo*: "Incumplimiento en la atención de las PQRS interpuestos por los usuarios y grupos de interés".*

ANÁLISIS DEL RIESGO			
CALIFICACIÓN RIESGO INHERENTE			
FRECUENCIA	**PROBABILIDAD**	**IMPACTO**	**EVALUACIÓN Y MEDIDAS DE RESPUESTA**
4. El evento probablemente ocurrirá en la mayoría de las circunstancias Orientador (Al menos de 1 vez en el último año)	**4. Probable**	**3. Moderado**	**(12) ZONA DE RIESGO ALTA** Reducir, Evitar, Compartir o Transferir el Riesgo

Matriz de Calificación, Evaluación y Respuesta a los Riesgos.

			IMPACTO				
			INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
			1	2	3	4	5
PROBABILIDAD	Raro	1	(1) ZONA DE RIESGO BAJA Asumir el riesgo	(2) ZONA DE RIESGO BAJA Asumir el riesgo	(3) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(4) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(5) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo
	Improbable	2	(2) ZONA DE RIESGO BAJA Asumir el riesgo	(4) ZONA DE RIESGO BAJA Asumir el riesgo	(6) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(8) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(10) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo
	Posible	3	(3) ZONA DE RIESGO BAJA Asumir el riesgo	(6) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(9) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(12) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(15) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo
	Probable	4	(4) ZONA DE RIESGO MODERADA Asumir o Reducir el Riesgo	(8) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(12) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(16) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(20) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo
	Casi seguro	5	(5) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(10) ZONA DE RIESGO ALTA Reducir, Evitar, Compartir o Transferir el Riesgo	(15) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(20) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo	(25) ZONA DE RIESGO EXTREMA Reducir, Evitar, Compartir o Transferir el Riesgo

No aplica para riesgos de corrupción

Fuente: DAFP Guia de administración del riesgo pag 47 - 2019

5.5 VALORACIÓN DE LOS CONTROLES

Los controles se definen como mecanismos, políticas, prácticas u otras acciones existentes que actúan para minimizar el riesgo negativo o potenciar oportunidades positivas en la gestión del riesgo, con el fin de garantizar el desarrollo y cumplimiento de las actividades acorde a los requisitos institucionales.

Los controles se pueden clasificar en:

- Preventivos: aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- Correctivos: aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

La clasificación de los controles puede estar asociada a:

- Controles de Gestión: Son aquellos orientados a garantizar el cumplimiento de las estrategias, políticas y objetivos institucionales, dentro de los cuales se encuentran: los indicadores, evaluaciones, auditorías, informes, comités etc.
- Controles Operativos: Son aquellos enfocados a garantizar la ejecución de las actividades, se encuentran soportados en los manuales, procedimientos, guías o instructivos definidos para desarrollar dicha actividad; también hacen parte las funciones y responsabilidades determinadas al personal, la infraestructura y todos los recursos dispuestos para la realización de dichas actividades.
- Controles Legales: Son aquellos en los cuales hacen parte la normatividad interna y externa aplicable a la entidad. Por ejemplo, acuerdos, resoluciones etc.

Calificación de los Controles

Los controles deberán calificarse con el fin de garantizar que son los adecuados para mitigar los riesgos y su calificación se hará de acuerdo a la siguiente tabla:

TIPO DE CONTROL		
PARÁMETROS	**CRITERIOS**	**PUNTAJE**
asiganción de responsable	Asignado	15
	No asignado	0
segregación y autoriad del responsable	adecuado	15
	No adecuado	0
periocidad	oportuna	15
	Inoportuna	0
proposito	prevenir	15
	detectar	10
	No es un control	0
como se realiza la actividad de control	confiable	15
	No confiable	0

que pasa con las observaciones o desviaciones	se investigan y resuelven oportunamente	15
	No se investigan ni se resulven	0
evidencia de la ejecución del control	completa	10
	incompleta	5
	no existe	0

Fuente: DAFP Guia de administración del riesgo pag 61 - 2019

Se debe calificar el diseño de los controles respondiendo a cada una de las preguntas y de acuerdo al puntaje se clasificaran en los rangos como lo indica la tabla

RANGO DE CALIFICACIÓN DEL DISEÑO	RANGOS DE CALIFICACIÓN DE LOS CONTROLES
Débil	Entre 0-85
Moderado	Entre 86-95
Fuerte	Entre 96 y 100

Fuente: DAFP Guia de administración del riesgo pag 62 - 2019

Si el resultado de las calificaciones del control es inferior a 86% el control deberá replantearse si luego de esto el control esta por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Posterior a la evaluación del diseño del control se deberá evaluar si la ejecución del control es la adecuada de acuerdo a la siguiente tabla

Rango de Calificación de la Ejecución	Peso en la Ejecución del Control
Fuerte	El control se ejecuta de manera consistente por parte del Responsable
Moderado	El control se ejecuta algunas veces por parte del Responsable
Débil	El control no se ejecuta por parte del Responsable

Fuente: DAFP Guia de administración del riesgo pag 62 - 2019

Luego de calificar cada control se cruzara de acuerdo a la siguiente matriz

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DÉBIL:0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
fuerte: calificación entre 96 y 100”	fuerte (siempre se ejecuta	fuerte + fuerte = fuerte	NO
	moderado (algunas veces)	fuerte + moderado = moderado	SI
	débil (no se ejecuta)	fuerte + débil = débil	SI
fuerte: calificación entre 96 y 100”	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	SI
	moderado (algunas veces)	moderado + moderado = moderado	SI
	débil (no se ejecuta)	moderado + débil = débil	SI
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	SI
	moderado (algunas veces	débil + moderado = débi	SI
	débil (no se ejecuta)	débil + débil = débil	SI

Fuente: DAFP Guia de administración del riesgo pag 63 - 2019

Con el resultado de la calificación se podrá definir que grado de solidez tiene el control

Disminución de probabilidad e impacto

Se debe aplicar la siguiente Tabla de Valoración de los Controles teniendo en cuenta las características citadas, para saber con exactitud el número de casillas dentro de la Matriz que se desplaza la valoración del riesgo a fin de disminuir su nivel.

Solidez del conjunto de controles	Los controles ayudan a disminuir la probabilidad	Los controles ayudan a disminuir el impacto	# De columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# De columnas en la matriz de riesgo que se desplaza en el eje de impacto
Fuerte	directamente	directamente	2	2
Fuerte	directamente	indirectamente	2	1
Fuerte	directamente	no disminuye	2	0
Fuerte	no disminuye	directamente	0	2

Moderado	directamente	directamente	1	1
Moderado	directamente	indirectamente	1	0
Moderado	directamente	no disminuye	1	0
Moderado	no disminuye	directamente	0	1

Fuente: DAFP Guia de administración del riesgo pag 66 - 2019

La evaluación de los controles permiten definir el número de columnas o filas a disminuir en el eje de la ***PROBABILIDAD*** o de ***IMPACTO*** en caso de ser efectivo, es importante que el líder del proceso determine si es pertinente o si requiere del establecimiento de controles adicionales o complementarios, con el fin de evitar o prevenir el riesgo.

Los tipos de controles determinados para disminuir en su ***PROBABILIDAD*** son los controles operativos como la aplicación de lineamientos contenidos en documentos, formatos, normas u otros que se empleen de manera permanente.

Los tipos de controles determinados para disminuir en su ***IMPACTO*** son aquellos controles enfocados a evaluar como auditorías, indicadores u otros relacionados.

Después de evaluar los controles y desplazar las casillas de probabilidad o impacto de acuerdo a los resultados obtenidos de la calificación de los controles, se determina la nueva zona de exposición al riesgo, que en esta etapa se denomina **RIESGO RESIDUAL**. [5]

5.6 TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:[6]

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

[5] DAFP, Guía para la administración del riesgo, 2011, p. 36

[6] DAFP, Guía para la administración del riesgo, 2018, p. 68

acciones emprendidas. Por ejemplo: el control de calidad, optimización de recursos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

- **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

- **Compartir o transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

- **Asumir un riesgo:** Cuando el riesgo ha sido reducido o transferido puede quedar un riesgo residual, en este caso simplemente se acepta la probable pérdida residual, dependiendo de su impacto y probabilidad se pueden formular acciones de contingencia para su manejo.

Nota: Para el caso de los riesgos de corrupción las acciones que se debe tener en cuenta para su administración son únicamente: **Evitar el riesgo** y **Reducir el riesgo**[7]**.**

- **Plan de manejo:**

Los planes de manejo son el conjunto de actividades (acciones) encaminadas a prevenir y/o mitigar el riesgo, las cuales comprenden:

  - *Acciones a desarrollar*: Describe las actividades a implementar para mitigar el riesgo. Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios en la infraestructura, entre otros. La selección de las acciones más conveniente debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica, realizando el balance entre el costo de la implementación de cada acción contra el beneficio de la misma para determinar su viabilidad.
  - *Identificar los responsables de llevar a cabo las acciones*,
  - *Determinar las fechas de ejecución* (tiempo máximo para la implementación de las actividades)
  - *Implementar indicadores* para medir la eficacia de los controles y la evaluación de si se ha materializado el riesgo o no.

5.7 VERIFICACIÓN Y AUTOSEGUIMENTO

Una vez diseñado y validado el plan para administrar los riesgos en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la entidad, la verificación y monitoreo está a cargo de los líderes de los procesos y la Oficina de Control Interno.
La verificación de su implementación se realiza por medio de mecanismos como autoseguimientos por parte de los líderes de los procesos con los siguientes cortes: ***abril 30, agosto 31 y diciembre 31*** y de evaluaciones por parte de la Oficina de Control Interno de acuerdo a la programación definida, con el fin

[7] Secretaria de Transparencia Presidencia de la República, Departamento Nacional de Planeación, Departamento Administrativo de la Función Pública, Oficina de las Naciones Unidad contra la Droga y el Delito, Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano, 2012, p . 12-13

de asegurar el mantenimiento de los mismos y/o necesidad de cambio de éstos. No obstante, en el formato de mapa de riesgos debe describirse el estado actual de la implementación de las acciones teniendo en cuenta los plazos establecidos en el plan de manejo.

Los riesgos y la efectividad de las medidas de control necesitan ser revisadas constantemente para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos o la detección de nuevos riesgos, es importante tener en cuenta que pocos riesgos permanecen estáticos.

La finalidad principal de estas verificaciones es la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

6. ACTUALIZACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos debe ser actualizado como mínimo una vez al año[8] o cuando se identifican nuevos factores externos que afecten el objetivo del proceso, cuando el proceso evaluado presente cambios organizacionales, como objetivo, alcance y/o actividades, o como resultado de las observaciones del seguimiento realizado por la oficina de Control Interno.

En consecuencia, la actualización del mapa de riesgos es una actividad permanente y es recomendable que se realice una vez se obtengan resultados tanto del autoseguimiento como de los seguimientos realizados por la Oficina de Control Interno.

Los plazos de ejecución de las acciones del plan de manejo de riesgos deben ser actualizados en los cambios de vigencias y deben ser publicados a más tardar el 31 de enero de cada año.

7. MATERIALIZACIÓN DE RIESGOS

Si como resultado de la autoevaluación o auto seguimiento por parte del líder del proceso y/o del seguimiento por parte de la OCI un riesgo se materializa, es fuente para la realización de una acción correctiva y debe ser incluida en el plan de mejoramiento, de acuerdo con los lineamientos contenidos en procedimiento Acciones correctivas preventivas y de mejora para evitar o disminuir la probabilidad de que vuelva a suceder[9].

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
1	**30-11-2015**	Creación del Documento acorde con los lineamientos para el Sistema de gestión de la calidad.
2	**30/09/2016**	Modificación de calificación y valoración de los controles, se incluye el tratamiento de riesgos de seguridad digital e identificación de activos,
3	**11-02-2019**	Modificación de calificación y valoración de los controles, se incluye el tratamiento de riesgos de seguridad digital e identificación de activos,

[8] DAFP, Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano, 2014, p.62

[9] DAFP, Guía de administración del riesgo, 2011 p. 12

9. APROBACIÓN

PROYECTO Y REVISO	APROBÓ
Cargo: Profesional Universitario – Encargado del SGC	**Cargo:** Jefe Oficina Asesora de Planeación
Firma: Original firmado	**Firma: Original firmado**