1. INTRODUCCIÓN

La Unidad Central del Valle del Cauca, a través del Comité Institucional de Control Interno, establece y aprueba la política de administración de riesgos, tomando como referencia la *Guía para la administración del riesgo y el diseño de controles en entidades públicas – riesgos de gestión, corrupción y seguridad digital en su versión 4* de octubre de 2018, en la cual se encuentra definida la metodología a seguir para la identificación, análisis, valoración y tratamiento de riesgos, así como las responsabilidades de las diferentes líneas de defensa de acuerdo a la dimensión 7 control interno del MIPG.

Los diferentes procesos de la Institución, deberán adoptar los lineamientos definidos en esta política, identificando, analizando, valorando y tratando los riesgos de gestión, corrupción y seguridad digital que pueden afectar la misión y el cumplimiento de los objetivos institucionales a través de los diferentes planes, programas y proyectos definidos, la manera de realizarlo es mediante:

a) La identificación y documentación de riesgos de gestión, corrupción y de seguridad digital en los planes, programas, proyectos y procesos.
b) El establecimiento de acciones de control para los riesgos identificados, tomándose de esta manera medidas para asumir, reducir y mitigar los riesgos.
c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados, estableciendo planes de contingencia.

2. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

“La UCEVA se compromete a administrar los riesgos inherentes a la gestión de todos sus procesos, a los riesgos de corrupción y los riesgos de seguridad digital mediante la adopción de mecanismos de control efectivos, que contribuyan a asumir, reducir, evitar, compartir o transferir las situaciones que impacten el normal desarrollo de los procesos y procedimientos, planteando oportunamente acciones preventivas y correctivas, que permitan mantener la eficiencia, eficacia y efectividad Institucional en el cumplimiento de la misión, y el mejoramiento continuo”

3. OBJETIVO

Establecer lineamientos y criterios institucionales que orienten a la Unidad Central del Valle del Cauca, en la correcta identificación, análisis, valoración y tratamiento de los riesgos de gestión, corrupción y seguridad digital; que pueden afectar el logro de los objetivos institucionales en el marco de los procesos, proyectos y planes.

4. ALCANCE

Las políticas y directrices de administración de riesgos en la Uceva, adoptadas en el marco del proceso de implementación del Sistema de Gestión Integral, aplica para todos los procesos y procedimientos identificados y establecen las acciones para que los funcionarios de la Uceva administren los eventos que puedan afectar el cumplimiento de sus objetivos.

5. GLOSARIO

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

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

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

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

CICI: Comité Institucional de Coordinación de Control Interno**.**

CIGED: Comité Institucional de Gestión y Desempeño.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada 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 modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

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

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud.

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

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.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

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

Riesgo de gestión: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de 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 relacionados con el ambiente físico, digital y las personas.

Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

6. RESPONSABILIDAD

A continuación, se define el rol de cada una de las instancias que participan en la definición y ejecución de las acciones, métodos y procedimientos de control y de gestión del riesgo:

Tabla 1. Responsabilidades de las Líneas de Defensa frente a la Gestión del Riesgo

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
Estratégica	Alta Dirección (Rector), Comité Institucional de de Control Interno	• Elaborar un plan donde se establezcan los objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad. • Establecer y aprobar la Política de Administración del Riesgo, la cual incluye los niveles de responsabilidad y autoridad en la prevención del daño antijurídico, en colaboración con el Comité de Conciliación. • Asumir la responsabilidad primaria del Sistema de Control Interno y la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo. • Evaluar y dar línea sobre la administración de los riesgos en la entidad, específicamente el Comité Institucional de Coordinación de Control Interno. • Retroalimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles. • Definir el procedimiento para la Identificación y Valoración de Activos. • Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento). • Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos. • Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. • Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
Primera Línea	Líderes de Proceso	• Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales y actualizarlos cuando se requieran con énfasis en la prevención del daño antijurídico. • Definir y diseñar los controles a los riesgos identificados. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Consolidar y presentar al Comité Institucional de Control Interno, sobre

Líneas de Defensa	Responsable	Responsabilidad frente al Riesgo
		los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo, y realizar el seguimiento a la eficacia de los controles implementados en cada uno de los procesos
Segunda Línea	Servidores responsables de monitoreo y evaluación de controles y gestión del riesgo	• Consolidar los mapas de riesgos de gestión, corrupción y seguridad digital enviados por los líderes de los procesos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar. • Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de éstos e informar las alertas respectivas.
Tercera Línea	Oficina de Control Interno	• Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa. • Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. • Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. • Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. • Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

7. ANÁLISIS DEL CONTEXTO

La Uceva, para la identificación de los riesgos de gestión, corrupción y de seguridad digital, iniciará con el establecimiento del contexto discriminándolo de la siguiente manera:

Contexto Externo. Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:

- ✓ **Políticos.** Cambios de gobierno, legislación, políticas públicas y regulación.
- ✓ **Económicos y Financieros.** Disponibilidad de capital, liquidez, mercados financieros, desempleo y competencia.

- ✓ **Sociales y culturales.** Demografía, responsabilidad social y orden público.
- ✓ **Tecnológicos.** Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
- ✓ **Ambientales.** Emisiones de residuos, energía, catástrofes naturales, desarrollo sostenible.
- ✓ **Legales y Reglamentarios.** Normatividad externa (leyes, decretos, ordenanzas y acuerdos).

Contexto Interno. Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como:

- ✓ **Financieros.** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- ✓ **Personal.** Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
- ✓ **Procesos.** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- ✓ **Tecnología.** Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- ✓ **Estratégicos.** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
- ✓ **Comunicación Interna.** Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

Contexto del Proceso. Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

- ✓ **Diseño del Proceso.** Claridad en la descripción del alcance y objetivo del proceso.
- ✓ **Interacciones con Otros Procesos**. Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- ✓ **Transversalidad.** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

- ✓ **Procedimientos Asociados.** Pertinencia en los procedimientos que desarrollan los procesos.
- ✓ **Responsables del Proceso.** Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- ✓ **Comunicación entre los Procesos.** Efectividad en los flujos de información determinados en la interacción de los procesos.
- ✓ **Activos de Seguridad Digital del Proceso.** Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

8. TIPOLOGÍA DE RIESGOS

- ✓ **Riesgos Estratégicos.** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
- ✓ **Riesgos Gerenciales.** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- ✓ **Riesgos Operativos.** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- ✓ **Riesgos Financieros.** 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.
- ✓ **Riesgos Tecnológicos.** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- ✓ **Riesgos de Cumplimiento.** 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.
- ✓ **Riesgo de Imagen o Reputacional.** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
- ✓ **Riesgos de Corrupción.** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- ✓ **Riesgos de Seguridad Digital.** 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.

9. PASOS A SEGUIR EN LA IDENTIFICACIÓN DE RIESGOS

a) Solicitar por parte de la Oficina de Planeación a los líderes de proceso, la actualización de los mapas de riesgos de gestión, corrupción y de seguridad digital.

b) Los líderes de registrarán el mapa de riesgos de gestión, corrupción y de seguridad digital, en el formato mapa de riesgos 1010-36.9-003-F.

c) La Oficina de Planeación realizará el acompañamiento a los líderes de proceso con respecto a la metodología a utilizar para la identificación, valoración y tratamiento de los riesgos.

d) Una vez los líderes de proceso hayan finalizado el registro de los mapas de riesgos de gestión, corrupción y seguridad digital; éstos serán enviados a la Oficina de Planeación para la revisión en cuanto al cumplimiento de la metodología indicada (redacción de riesgos, identificación de causas, calificación de probabilidad e impacto, controles establecidos, fechas y responsables asignados).

e) La Oficina de Planeación enviará los mapas de riesgos de gestión, corrupción y seguridad digital a la Oficina de Control Interno para su validación final.

f) En el Comité Institucional de Control Interno, se aprobarán los mapas de riesgos de gestión, corrupción y seguridad digital y se comunicará a los líderes de proceso que éstos han sido subidos a la Intranet y página Web para su consulta, aplicación de controles y monitoreo periódico.

g) Se hará seguimiento dos veces al año, a la eficacia de los controles implementados, en caso de desviaciones negativas, se aplicará lo establecido en la presente política de administración de riesgos.

10. CRITERIOS PARA CALIFICAR LA PROBABILIDAD

Para determinar la probabilidad de ocurrencia de los riesgos de gestión, corrupción y seguridad digital, la Institución los analiza considerando la **frecuencia** o **factibilidad,** donde la frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado en la entidad o se cuenta con un historial de situaciones o

eventos asociados al riesgo; **factibilidad** implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo en la entidad, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Tabla 2. Calificación de Probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

11. CRITERIOS PARA CALIFICAR EL IMPACTO – RIESGOS DE GESTIÓN

La Unidad Central del Valle del Cauca, implementa la siguiente metodología para calificar el impacto de los riesgos de gestión:

Tabla 3. Calificación de Impacto – Riesgos de Gestión

Nivel	Impacto (consecuencias) cuantitativo	Impacto (consecuencias) cualitativo
Catastrófico	• Impacto que afecte la ejecución presupuestal en un valor ≥50%. • Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de información crítica para la entidad que no se puede recuperar. • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Nivel	Impacto (consecuencias) cuantitativo	Impacto (consecuencias) cualitativo
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 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%.	• Interrupción de las operaciones de la entidad por algunas horas. • Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.

Nivel	Impacto (consecuencias) cuantitativo	Impacto (consecuencias) cualitativo
	• 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.	
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.

12. CRITERIOS PARA CALIFICAR EL IMPACTO – RIESGOS DE SEGURIDAD DIGITAL

La Uceva implementa la siguiente metodología para calificar el impacto de los riesgos de seguridad digital:

Tabla 4. Calificación de Impacto – Riesgos de Seguridad Digital

Nivel	Valor del Impacto	Criterios de Impacto para Riesgos de Seguridad Digital	
		Impacto (consecuencias) cuantitativo	**Impacto (consecuencias) cualitativo**
Insignificante	1	• Afectación ≥0,1% de la población. • Afectación ≥0,1% 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 ≥0,2% de la población. • Afectación ≥0,2% del presupuesto anual de la entidad.	• Afectación leve de la integridad. • Afectación leve de la disponibilidad.

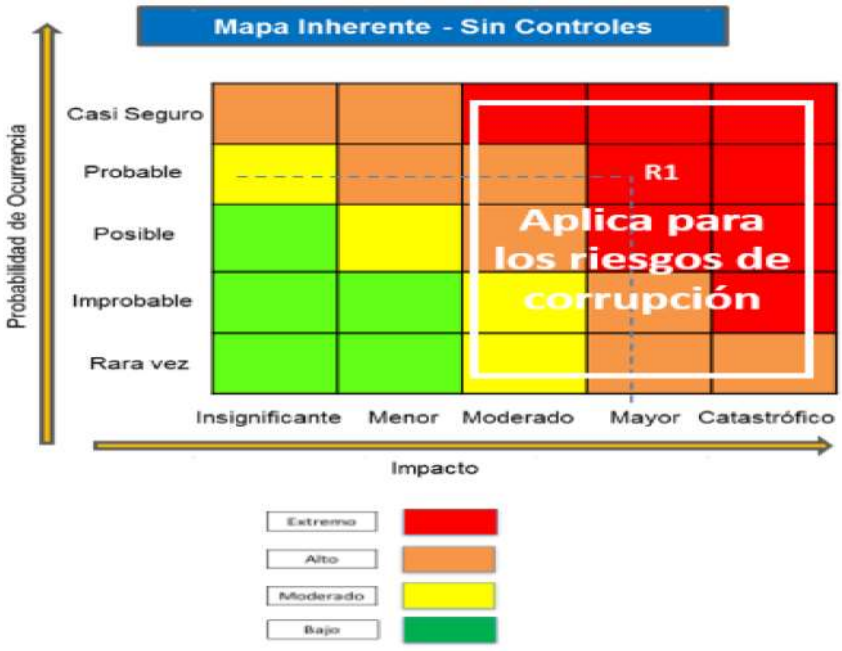
Nivel	**Valor del Impacto**	**Criterios de Impacto para Riesgos de Seguridad Digital**	
		Impacto (consecuencias) cuantitativo	**Impacto (consecuencias) cualitativo**
		• Afectación leve del medio ambiente requiere de ≥29 días de recuperación.	• Afectación leve de la confidencialidad.
Moderado	3	• Afectación ≥0,3% de la población. • Afectación ≥0,3% del presupuesto anual de la entidad. • Afectación leve del medio ambiente requiere de ≥7 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 ≥0,4% de la población. • Afectación ≥0,4% del presupuesto anual de la entidad. • Afectación importante del medio ambiente que requiere de ≥2 meses de recuperación.	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
Catastrófico	5	• Afectación ≥0,5% de la población. • Afectación ≥0,5% del presupuesto anual de la entidad. • Afectación muy grave del medio ambiente que requiere de ≥1 año 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

Nivel	**Valor del Impacto**	**Criterios de Impacto para Riesgos de Seguridad Digital**	
		Impacto (consecuencias) cuantitativo	**Impacto (consecuencias) cualitativo**
			empleados y terceros.

13. ANÁLISIS DEL IMPACTO

Mapa de Calor

Acorde con los riesgos aprobados por el Comité Institucional de Control Interno, se define una periodicidad de seguimiento a los riesgos de gestión, corrupción y seguridad digital dos veces al año.



Es importante tener en cuenta que a los riesgos de corrupción les aplica las columnas de impacto Moderado, Mayor y Catastrófico.

14. TRATAMIENTO DE RIESGOS

Es la respuesta establecida por la primera línea de defensa (líderes de proceso) para la mitigación de los diferentes riesgos identificados, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la Uceva, la probabilidad e impacto de este y la relación beneficio – costo de las medidas de tratamiento. En caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la Gerencia 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.

Tabla 5. Tratamiento de Riesgos – Riesgos de Gestión

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Gestión (Proceso o Proyecto)	Bajo	**Aceptar.** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. La realización propia de las actividades del proceso o proyecto permiten tener controlado el riesgo.
	Moderado y Alto	**Reducir.** Se establecen controles preventivos para reducir la probabilidad o el impacto del riesgo. **Compartir.** Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Estos casos se presentan cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que no es posible transferir la responsabilidad del riesgo.
	Extremo	**Evitar el Riesgo.** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

Tabla 6. Tratamiento de Riesgos – Riesgos de Corrupción

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Corrupción	Bajo	Ningún riesgo de corrupción podrá ser aceptado.
	Moderado	Se establecen acciones de control preventivas que permitan **reducir** la probabilidad de ocurrencia del riesgo.
	Alto y Extremo	Se adoptan medidas para: **Reducir** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **Evitar,** se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. **Transferir o compartir** una parte del riesgo para reducir la probabilidad o el impacto del mismo.

15. ACCIONAR ANTE LOS RIESGOS MATERIALIZADOS

Tabla 7. Accionar ante los Riesgos Materializados

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión - Proceso o Proyecto (zona extrema, alta y moderada)	Líder de proceso	1. Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el plan de mejoramiento. 2. Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. 3. Analizar y actualizar el mapa de riesgos. 4. Informar al Proceso de Gestión Estratégica sobre el hallazgo y las acciones tomadas.
Riesgos de Gestión - Proceso o Proyecto (zona baja)	Líder de proceso	Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión - Proceso o Proyecto (zona extrema, alta y moderada)	Jefe de Oficina de Control Interno	1. Informar al líder del proceso sobre el hecho encontrado. 2. Informar a la segunda línea de defensa (Oficina de Planeación – líder de la gestión del riesgo) con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. 3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. 4. Verificar que se tomaron las acciones y se haya actualizado el mapa de riesgos correspondiente.
Riesgos de Gestión - Proceso o Proyecto (zona baja)	Jefe de Oficina de Control Interno	1. Informar al líder del proceso sobre el hecho. 2. Informar a la segunda línea de defensa (Oficina de Planeación – líder de la gestión del riesgo) con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. 3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. 4. Verificar que se tomaron las acciones y se haya actualizado el mapa de riesgos correspondiente.
Riesgos de Corrupción	Líder de Proceso	1. Informar al Proceso de Planeación sobre el hecho encontrado. 2. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. 3. Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento 4. Efectuar el análisis de causas y determinar las acciones preventivas y de mejora. 5. Actualizar el mapa de riesgos.
Riesgos de Corrupción	Jefe de Oficina de Control Interno	1. Informar al líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. 2. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. 3. Informar a la segunda línea de defensa (Oficina de Planeación) con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.

16. BIBLIOGRAFÍA

- ✓ Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 04. Función Pública – Octubre de 2018.
- ✓ Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. Ministerio de Tecnologías de la Información y las Comunicaciones. 2018.