POLÍTICA ADMINISTRACIÓN DEL RIESGO

DEPARTAMENTO
DE CÓRDOBA

MONTERIA

26/04/2021

1. INTRODUCCIÓN

La Gobernación de Córdoba, en su Plan de Desarrollo Territorial “Ahora le Toca a Córdoba: Oportunidades, Bienestar y Seguridad 2020– 2023”, basa su gestión en 3 ejes estratégicos: la Equidad y Bienestar, Oportunidad y Emprendimiento, Seguridad y Legalidad, integrando directrices y estrategias a desarrollar con el fin de cumplir los objetivos y metas Institucionales. Con la entrada en vigencia del Modelo de Planeación y Gestión MIPG, el cual integra los sistemas de gestión de Calidad y de Desarrollo Administrativo; se crea un único sistema de Gestión de la calidad y de Desarrollo Administrativo y a su vez se crea un sistema de Gestión Articulado con el sistema de Control Interno, el cual se actualiza y alinea con los estándares Internacionales COSO 2013 Y COSO ERM 2017, y el Modelo de líneas de defensa, el cual es adoptado y desarrollado por la Gobernación de Córdoba para tal fin.

De acuerdo con el numeral 2.2.1 del Manual Operativo del Modelo Integrado de Planeación y Gestión, “política de planeación institucional” de la dimensión “Direccionamiento estratégico y planeación” del MIPG, para responder a la pregunta ¿cuáles son las prioridades identificadas por la entidad y señaladas en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

El Departamento Administrativo de la Función Pública, La Secretaria de Transparencia de la Presidencia de la Republica, y el Ministerio de Tecnologías y Comunicaciones, diseñaron la Guía Para la Administración del Riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital, con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo, así como el control de todos los niveles de la entidad pública, brindando seguridad frente al logro de los objetivos, dentro de la cual se presenta la estructura de la política de administración del riesgo.

Se entiende por política de administración del riesgo a la declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. En este sentido, es claro que la identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos, desarrollando este en los diferentes niveles de la Gobernación, de acuerdo con su esquema de direccionamiento estratégico, gestión de procesos, procedimientos, políticas de operación y sistemas de información, los cuales son el insumos esenciales para la gestión de la administración del riesgo.

En consecuencia, la Gobernación de Córdoba, concibe organiza y aplica la siguiente política de administración del riesgo, de tal manera que la implementación de su estructura, sea implícita al desarrollo de las actividades y funciones de todos los cargos existentes en la entidad, y en particular de las asignadas a aquellos que tengan responsabilidad y liderazgo de procesos. Logrando con ello los siguientes beneficios:

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

1. Apoyo a la toma de decisiones
2. Garantizar la operación normal de la organización
3. Minimizar la probabilidad e impacto de los riesgos
4. Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
5. Fortalecimiento de la cultura de control de la organización
6. Incrementa la capacidad de la entidad para alcanzar sus objetivos
7. Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

2. OBJETIVO

La Gobernación de Córdoba, busca con el desarrollo de Política de Administración del Riesgo, establecer los elementos y el marco general de actuación para la Gestión Integral de los riesgos a los que se enfrenta la Gobernación de Córdoba, al igual que orientar para el diseño, implementación y desarrollo de las acciones necesarias que conduzcan a disminuir la vulnerabilidad en los procesos y actividades, con un enfoque preventivo frente a situaciones que puedan interferir en el desarrollo de la misionalidad y de los objetivos institucionales, preparando una respuesta oportuna a amenazas internas y externas que puedan generar eventos de riesgo.

3. ALCANCE

La alta dirección de Gobernación de Córdoba, velará por la adecuada implementación y cumplimiento de las directrices que componen la estructura de la presente Política de Administración del Riesgo, la cual es aplicable a los Objetivos Estratégicos, Procesos, Proyectos y planes de la entidad, al igual que a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones. La Gobernación de Córdoba, cuenta con sistema de gestión integrado, el cual maneja un enfoque basado en procesos, con el que se busca garantizar la satisfacción de las necesidades y cumplimiento de los derechos de los ciudadanos, mediante las accione de medición y mejora continua, conservando una estructura de procesos: Estratégicos, Misionales, de Apoyo y de Medición.

4. CONCEPTOS BÁSICOS RELACIONADOS CON LA GESTIÓN DEL RIESGO

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Nota: 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 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 de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
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.
Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
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
Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.
Control: Medida que permite reducir o mitigar un riesgo.
Causa Inmediata: Circunstancias 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 la cuales se puede presentar el riesgo.
Factores de Riesgo: Son las fuentes generadoras de riesgos.
Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Integridad: Propiedad de exactitud y completitud.
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
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.
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 * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
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 se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
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.
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.
Mapa de riesgos: es una herramienta de visualización de datos para comunicar riesgos específicos que enfrenta la entidad, ayuda a identificar los riesgos asociados a los procesos. Se trata de una representación gráfica de un número selecto de riesgos diseñado para ilustrar el impacto de los riesgos en un eje y la probabilidad o frecuencia en el otro, al igual que la definición de sus controles.

Fuete: Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

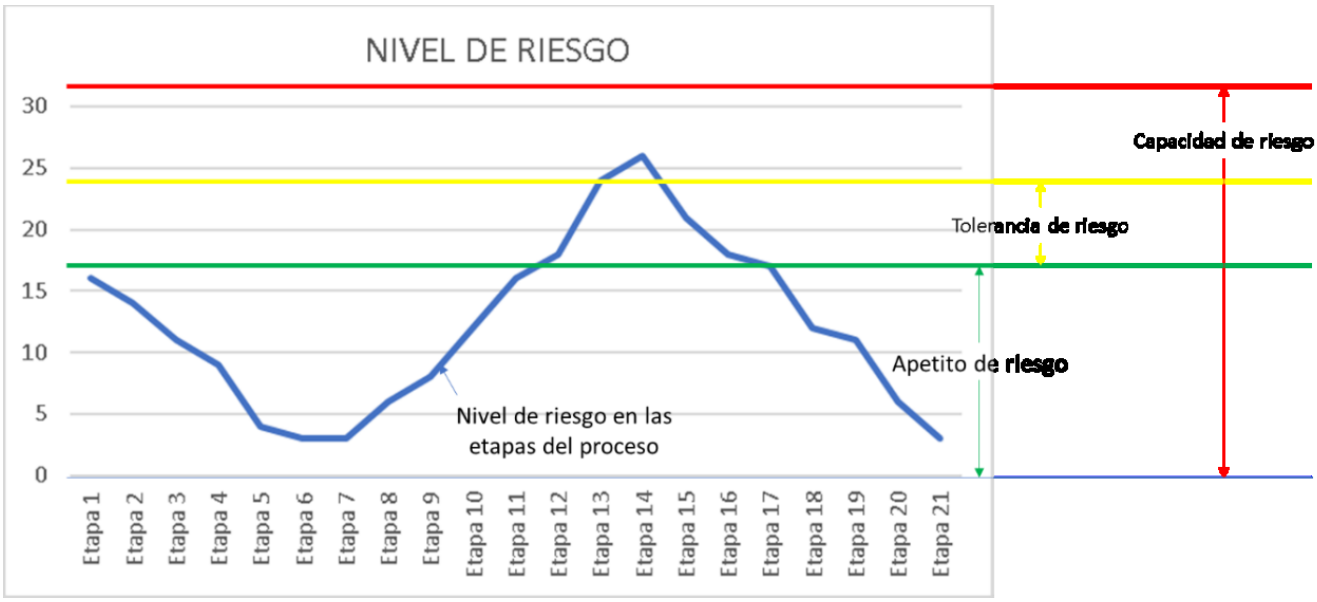
5. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

La gobernación de Córdoba desarrolla la gestión para la administración del riesgo mediante la metodología establecida por la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020, cuyos lineamientos son adoptados en la presente Política de Administración del Riesgo y aplicados a través de los procedimientos: (Administración del Riesgo) y (Formulación y Seguimiento al Plan Anticorrupción y de Atención al Ciudadano), que hacen parte integral de la estructura documental del Sistema Integrado de Gestión de la entidad.

A continuación, se describen los lineamientos desarrollados por la Gobernación de Córdoba para la Gestión de la Administración del Riesgo:

5.1 APETITO DEL RIESGO: Dentro de los lineamientos de la política de administración del riesgo se debe considerar el apetito del riesgo, por lo que se desarrolla su análisis, en relación e interacción con el **Nivel de riesgo, Tolerancia del riesgo y** la **Capacidad de riesgo**

Gráficamente los anteriores conceptos se relacionan así:



Tomado de la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

5.1.1 Determinación de la capacidad de riesgo: Para determinar la capacidad del riesgo, La Gobernación de Córdoba, aplica los valores de probabilidad e impacto contenidos en la presente Política y con base en estos la determina, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:
a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”. De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que la entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

5.1.2 Determinación del apetito de riesgo: La Gobernación de Córdoba, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, determina el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad. Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado 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.

5.1.2 Tolerancia de riesgo: Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo. El límite o valor de la tolerancia de riesgo es definido por la alta dirección en el marco del comité institucional de coordinación de control interno y no puede ser superior al valor de la capacidad de riesgo. La

determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

5.2 IDENTIFICACIÓN DEL RIESGO: Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la Gobernación de Córdoba, para ello se tiene en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, como también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

5.2.1 Análisis de objetivos estratégicos y de procesos: Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso. Para ello se analizan los objetivos estratégicos y los objetivos de los procesos que desarrolla la Gobernación de Córdoba. La entidad analiza los objetivos estratégicos y revisa que se encuentren alineados con la misión y la visión, así como su desdoble hacia los objetivos de los procesos, al igual se analiza su adecuada formulación, es decir, que contengan unos atributos mínimos, por lo que la Gobernación de Córdoba utiliza la metodología SMART (Hace referencia a las siglas en inglés que responden a: Specific (específico); Mensurable (medible); Achievable (alcanzable); Relevant; (relevante); Timely (temporal), la cual es propuesta en la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020, y cuya estructura se explica a continuación:

S: Specific (específico): el objetivo debe resolver cuestiones de: Qué, Cómo, Dónde, Cuándo, Con Qué, Quién, considerando el orden y lo necesario para el cumplimiento de su misión

M: Mensurable (medible): el objetivo debe involucra algunos números en su definición, porcentajes o cantidades exactas (Cuando aplique)

A: Achievable (alcanzable): el objetivo debe considerar lo que se ha hecho y logrado, con el fin de analizar si lo que propone este es posible o como sería mejor

R: Relevant; (relevante): el objetivo debe considerar recursos, factores externos e información de actividades previas, con el fin de contar con elementos de juicio para su determinación,

T: Timely (temporal): el objetivo debe expresar un tiempo de cumplimiento, con el fin de saber si lo que se está haciendo es optimo para llegar a la meta y así determinar el cumplimiento y mediciones finales

5.2.2 Identificación de los puntos de riesgo: Una vez analizados la estructura y formulación de los objetivos de la Gobernación de Córdoba, se realiza la identificación y determinación de los puntos de riesgos, teniendo en cuenta el flujo del proceso (Cadena de Valor), verificando donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

5.2.3 Identificación de áreas de impacto: el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la Gobernación de Córdoba en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional. Para ello la entidad debe establecer estas áreas dentro del mapa de riesgos institucional.

5.2.4 Identificación de áreas de factores de riesgo: los factores de riesgo son las fuentes generadoras de riesgos, por lo que la Gobernación de Córdoba establece los siguientes, con el fin de identificar las áreas que contengan estos:

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procesos y procedimientos o procesos y procedimientos desactualizados
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, en temas relacionados con el personal
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	Hurto de activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Incendios
		Daños a activos fijos
		Daño de documentos y archivos por humedad
		Daño en la infraestructura por vendavales y fuertes vientos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad y ataques cibernéticos
		Atentados, vandalismo, orden público

Nota: Para la definición de los factores de riesgos se tomó como base la tabla factores de riesgos propuesta en la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020, sin embargo, estos factores pueden ser actualizados por los líderes de procesos, considerando aspectos que puedan llegar a ser pertinentes para el análisis del contexto al momento de la identificación del riesgo

5.2.5: Identificación Riesgos de corrupción: Los riesgos de corrupción se describen como " *La posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público, hacia un beneficio privado",* "Esto Implica que Las prácticas corruptas son realizadas por actores

públicos y/o por privados con poder e incidencia en la toma de decisiones y la administración de los vienes públicos" – (Compes N° 167 de 2013).

Para la identificación de los riesgos de corrupción se pueden utilizar fuentes de datos internos y externos como lo son:

Externas. el Instituto de Auditores de España (IIA Global) indica que entre este tipo de fuentes están los organismos reguladores (Contraloría General de la República, Superintendencias, etc.) y del propio sector, instancias que cuentan con información global sobre situaciones irregulares que pueden llegar a ser comunes en las entidades públicas y que sirven de referente para los análisis que le son propios a cada organización.

Es el caso de la plataforma OCEANO de la Contraloría General de la República, que hace una labor de depuración y analítica de datos enfocado en la gestión contractual del Estado, tema transversal frente al análisis de riesgos de corrupción. De igual forma, podrán consultarse otras fuentes similares en temas sectoriales aplicables a cada entidad.

Internas. Frente a las fuentes internas, se incluyen entrevistas con el personal adecuado, la revisión de las denuncias interpuestas a través de los mecanismos implantados (canales de denuncia) y otros procedimientos analíticos. De igual forma, es pertinente incluir la evaluación de incentivos, las presiones, la potencial eliminación de controles por parte de la dirección, así como el análisis de aquellas áreas donde los controles son débiles o no existe una adecuada segregación de funciones.

Otro factor interno es la tecnología, por lo que se deben considerar los accesos a los sistemas, las amenazas internas y externas a la integridad de los datos, la seguridad de los sistemas y el posible robo de información confidencial o sensible (Instituto de Auditores de España, IIA Global).

Para la identificación de los riesgos de corrupción se deben considerar las siguientes preguntas claves.

¿Qué puede suceder?
¿Cómo puede suceder?
¿Cuándo puede suceder?
¿Qué consecuencias tendría su materialización?

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

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

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

Tomado de la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

Los riesgos de corrupción se establecen sobre procesos y se deben elaborar o actualizar anualmente por cada responsable de los procesos al interior de la entidad, junto con el equipo o personal que en ellos interviene. Después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción. En este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

Direccionamiento estratégico (alta dirección)	✓ Concentración de autoridad o exceso de poder. ✓ Extralimitación de funciones. ✓ Ausencia de canales de comunicación. ✓ Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto)	✓ Inclusión de gastos no autorizados. ✓ Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración. ✓ Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. ✓ Inexistencia de archivos contables. ✓ Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este)	✓ Estudios previos o de factibilidad deficientes. ✓ Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). ✓ Pliegos de condiciones hechos a la medida de una firma en particular. ✓ Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica). ✓ Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación. ✓ Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. ✓ Urgencia manifiesta inexistente.

	✓ Concentrar las labores de supervisión en poco personal. ✓ Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	✓ Ausencia o debilidad de medidas y/o políticas de conflictos de interés. Concentración de información de determinadas actividades o procesos en una persona. ✓ Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración. ✓ Ocultar la información considerada pública para los usuarios. ✓ Ausencia o debilidad de canales de comunicación
De Investigación y Sanción	✓ Inexistencia de canales de denuncia interna o externa. ✓ Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este. ✓ Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. ✓ Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	✓ Cobros asociados al trámite. ✓ Influencia de tramitadores. ✓ Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos)	✓ Falta de procedimientos claros para el trámite ✓ Imposibilitar el otorgamiento de una licencia o permiso. ✓ Tráfico de influencias: (amiguismo, persona influyente).

Fuete: Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

5.2.6 Identificación de riesgos de seguridad de la información: como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso y para ello se establecen las siguientes definiciones

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

Tomado de la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

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 Director de Sistemas de la Gobernación de Córdoba.
Para la identificación de los activos de seguridad de la información, se deben realizar los siguientes pasos:

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. Para ello se utiliza la tabla de Tipologías de Activos, tomada de los *LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS "MODELO NACIONAL DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PÚBLICAS" – 2018*

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) 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) entre 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: 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, el cableado estructurado y tarjetas de red, routers, switches, entre 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 empresa

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 en el siguiente Paso 5.

5- **Determinar la Criticidad del activo:** 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. En este paso se debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso.

CRITERIOS DE CLASIFICACIÓN		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

NIVELES DE CLASIFICACIÓN

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) 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 (1) 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.

Tomado de la Guía para la Gestión y Clasificación de Activos de Información – V1 2016 - MINTIC

Una vez se ejecute la identificación de los activos, se debe definir si se gestionarán los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica – Alta dirección en el marco del comité institucional de coordinación de control interno.

6- **Identificar si existe infraestructura física cibernética:** Se debe identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si se poseen Infraestructura Crítica Cibernética. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Una vez identificados los activos de la información se pueden identificar los siguientes 3 riesgos inherentes de seguridad de la información:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

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. Para este efecto, es necesario consultar el Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis: Tabla de amenazas comunes, Tabla de amenazas dirigida por el hombre, Tabla de vulnerabilidades comunes

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 las siguientes amenazas: Deliberadas (D), fortuito (F) o ambientales (A).

TABLA DE AMENAZAS COMUNES		
Tipo	**Amenaza**	**Origen**
Daño físico	Fuego	F, D, A
Daño físico	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
Eventos naturales	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
Pérdidas de los servicios esenciales	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
Perturbación debida a la radiación	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
Compromiso de la información	Espionaje remoto	D

Fallas técnicas	Fallas del equipo	D, F
Fallas técnicas	Mal funcionamiento del equipo	D, F
Fallas técnicas	Saturación del sistema de información	D, F
Fallas técnicas	Mal funcionamiento del software	D, F
Fallas técnicas	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
Acciones no autorizadas	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
Compromiso de las funciones	Falsificación de derechos	D

Fuente: Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas "Modelo Nacional De Gestión De Riesgo De Seguridad De La Información En Entidades Públicas" – 2018

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

Fuente: Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas "Modelo Nacional De Gestión De Riesgo De Seguridad De La Información En Entidades Públicas" – 2018

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

Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos 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: Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas “Modelo Nacional De Gestión De Riesgo De Seguridad De La Información En Entidades Públicas” – 2018

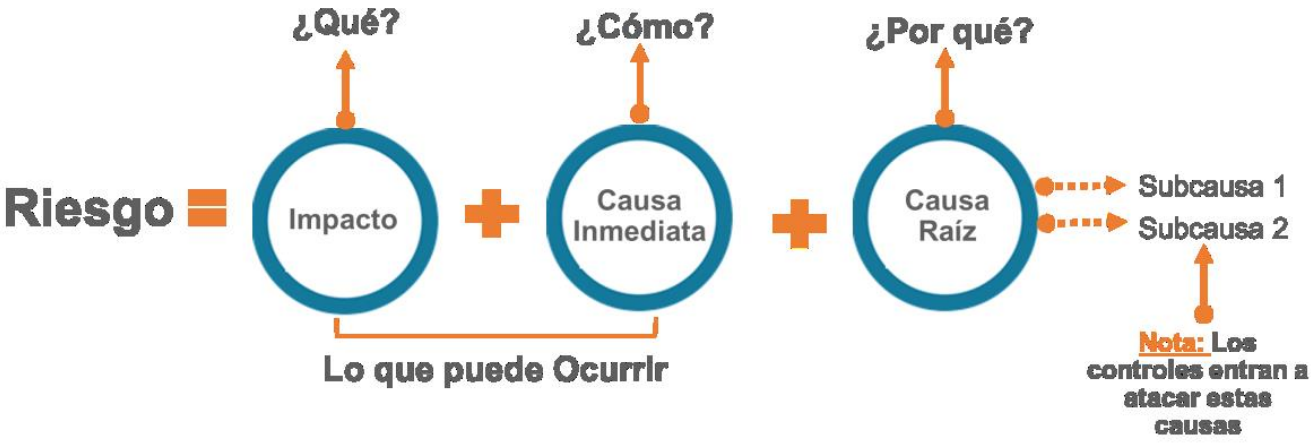
La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir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

AMENAZAS Y VULNERABILIDADES DE ACUERDO CON EL TIPO DE ACTIVO		
Tipo de activo	**Ejemplos de vulnerabilidades**	**Ejemplos de amenazas**
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Personal	Personal
Falta de capacitación en las herramientas	Falta de capacitación en las herramientas	Falta de capacitación en las herramientas

Fuente: Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

5.2.7 Descripción del riesgo: la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Estructura para la redacción del riesgo: tomada de la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020



Esta estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo. Desglosando la estructura propuesta tenemos:

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

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Premisas para una adecuada redacción del riesgo:
No describir como riesgos omisiones ni desviaciones del control.
No describir causas como riesgos
No describir riesgos como la negación de un control.
No existen riesgos transversales, lo que pueden existir son causas transversales.

5.2.8 Clasificación del riesgo: La Gobernación de Córdoba**,** toma para la clasificación de los riesgos, la tabla de clasificación de riesgos, de la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020. Mediante la clasificación del riesgo se agrupan los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

CLASIFICACIÓN	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Teniendo en cuenta que se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

RELACIÓN ENTE FACTORES DE RIESGO Y CLASIFICACIÓN DEL RIESGO	
CLASIFICACIÓN	**FACTORES DE RIESGO**
Ejecución y administración de procesos	Procesos
Fraude externo	Eventos externos
Fraude interno	Talento Humano
Fallas tecnológicas	Tecnología
Relaciones laborales	Puede asociarse a varios Factores
Usuarios, productos y prácticas	Puede asociarse a varios Factores
Daños a activos fijos/ eventos externos	Eventos externos / Infraestructura

Tomado de: Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

5.3 VALORACIÓN DEL RIESGO: La Gobernación de Córdoba, realiza la valoración del riesgo, con el fin de establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto de este, para así poder estimar la zona del riesgo inicial, lo cual se describe en el riesgo INHERENTE y la zona de riesgo final, después de la aplicación de los controles, lo cual se describe en el riesgo RESIDUAL. Para realizar una valoración del Riesgo adecuada, se deben desarrollar el Análisis y la evaluación del riesgo y controles existentes.

5.3.1 Análisis del Riesgo: Con esta acción se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, y así estimar la zona del riesgo inicial, lo cual se describe en el riesgo INHERENTE.

Para determinar la probabilidad de ocurrencia del riesgo, se establecerá la **Exposición al Riesgo**, del proceso o actividad que se está analizando**,** quedando la probabilidad inherente como el número de veces que se pasa por el punto de riesgo en un año o la frecuencia con que se lleva a cabo una actividad o desarrolla un proceso.

La Gobernación de Córdoba, para el desarrollo del análisis de los riesgos, toma como base y guía, la tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad, la cual se muestra en la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

ACTIVIDADES RELACIONADAS CON LA GESTIÓN EN ENTIDADES PÚBLICAS		
Actividad	**Frecuencia de la Actividad**	**Probabilidad frente al Riesgo**
Planeación estratégica	1 vez al año	Muy baja

Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
***Tecnología (incluye disponibilidad de aplicativos), tesorería ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.	Diaria	Muy alta

Teniendo en cuenta Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la **exposición al riesgo** estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la siguiente tabla se establecen los criterios para definir el nivel de probabilidad. Tomada de la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Para determinar las consecuencias o el impacto del riesgo, la Gobernación de Córdoba toma lo establecido en la Guía de administración de riesgo y el diseño de controles en entidades públicas,

Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020, la cual define que los criterios para definir los impactos, mediante la siguiente tabla:

Nota: Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado. Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

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 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

IMPORTANTE: Frente al análisis de probabilidad e impacto **no se utiliza criterio experto**, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para
la definición de los controles.

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado

que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.

Con el fin de establecer los niveles de impacto, se deberán aplicar las siguientes preguntas frente al riesgo identificado:

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

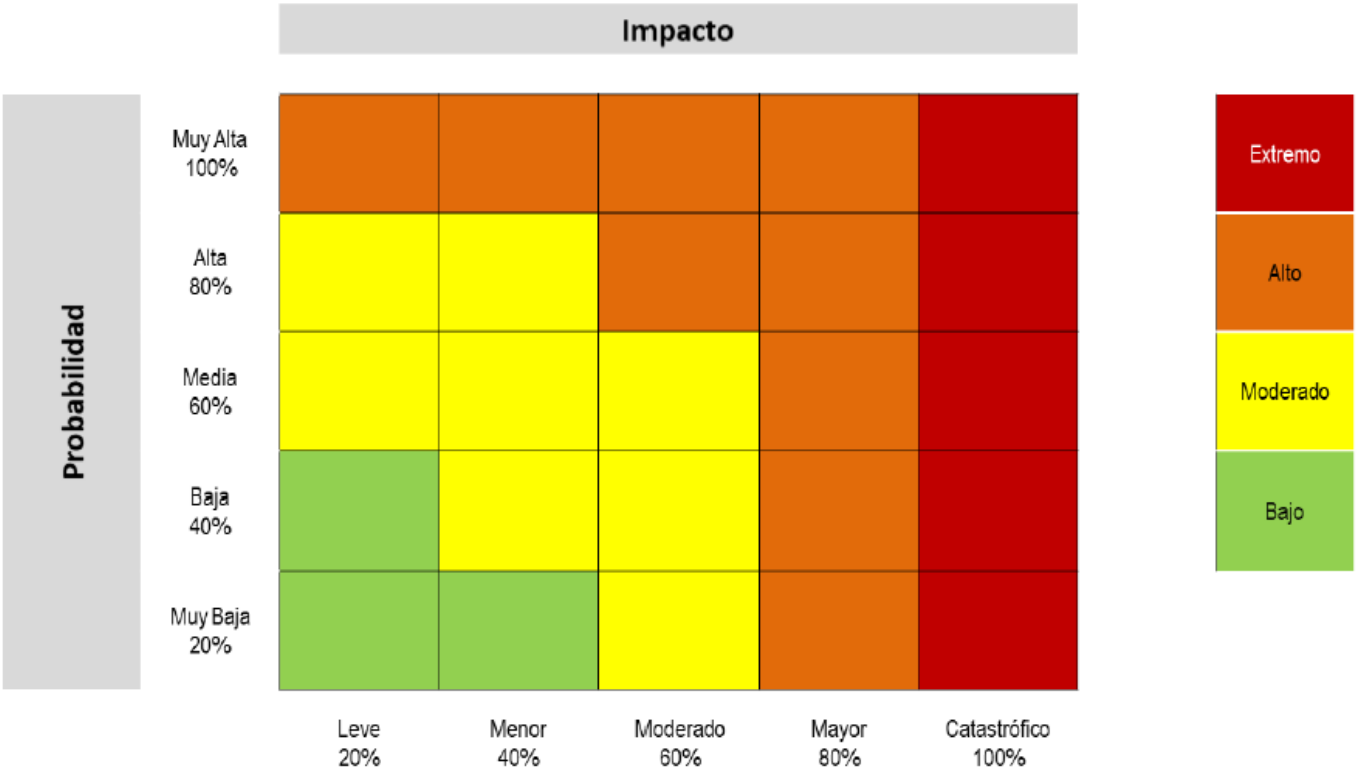
Nivel de impacto MAYOR

Fuente: Secretaría de Transparencia de la Presidencia de la República.

Tomado de: Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

5.3.2 Evaluación del Riesgo: Para realizar la evaluación del riesgo**,** la Gobernación de Córdoba parte del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, con lo cual se busca determinar la zona de riesgo inicial (RIESGO INHERENTE), y para ello se realiza el análisis preliminar del riesgo inherente, con el que se busca determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, utilizando la matriz de calor, en la cual se definen 4 zonas de severidad.

Matriz de calor (niveles de severidad del riesgo)



Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

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

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

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

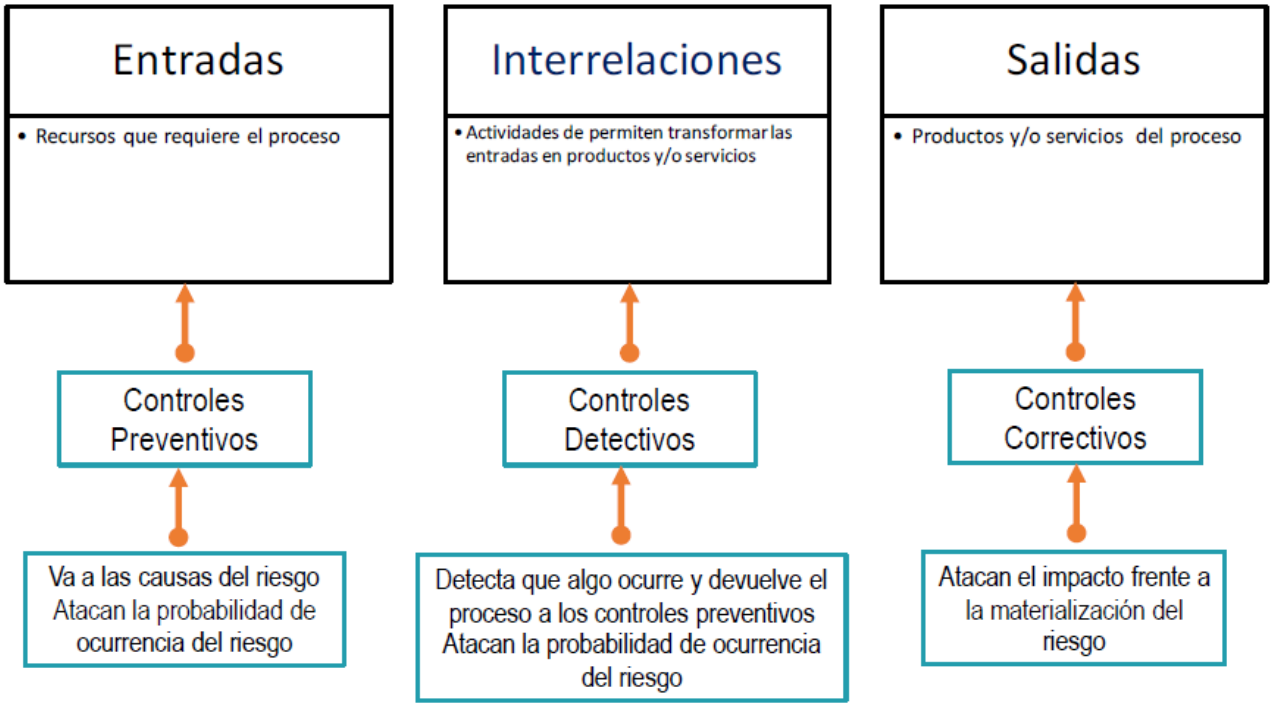
5.3.3.1 Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

5.3.3.2 Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, se consideran 3 fases globales del ciclo de un proceso así:



Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

5.3.3.3 Análisis y evaluación de los controles – Atributos: Se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. se puede observar la descripción y peso asociados a cada uno de la siguiente manera:

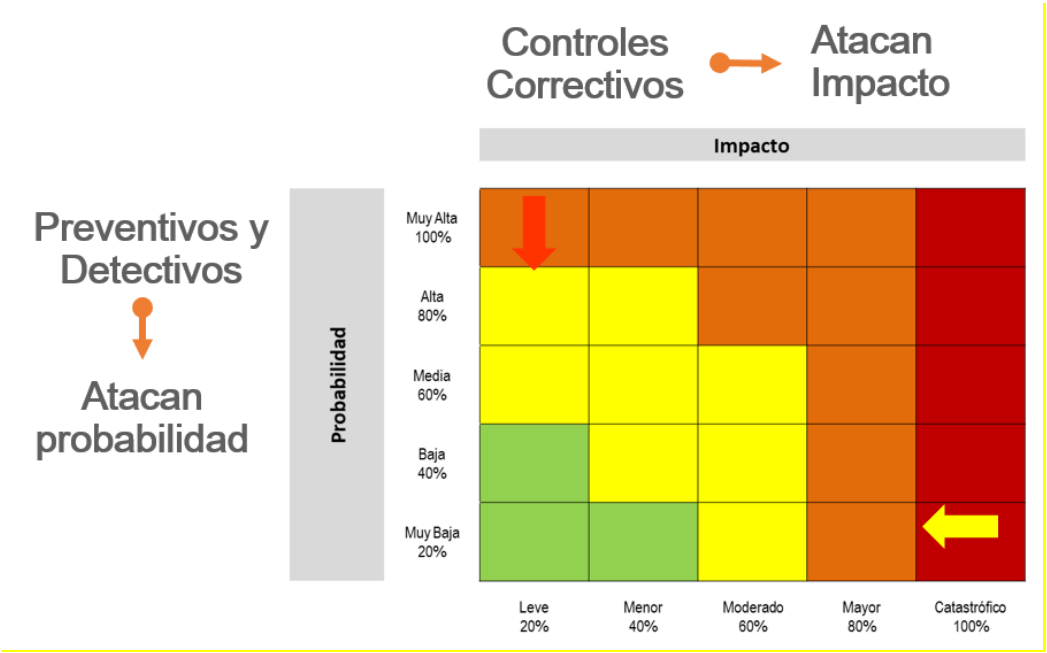
CARACTERÍSTICAS			DESCRIPCIÓN	PESO
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten 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.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el	-

			proceso no se encuentran documentados en ningún documento propio del proceso.	
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

5.3.4 Controles asociados a la Seguridad de la Información: La Gobernación de Córdoba podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de riesgos. Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	**Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información**
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
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.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
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.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020

5.3.5 Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de 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 luego de la aplicación del primer control.

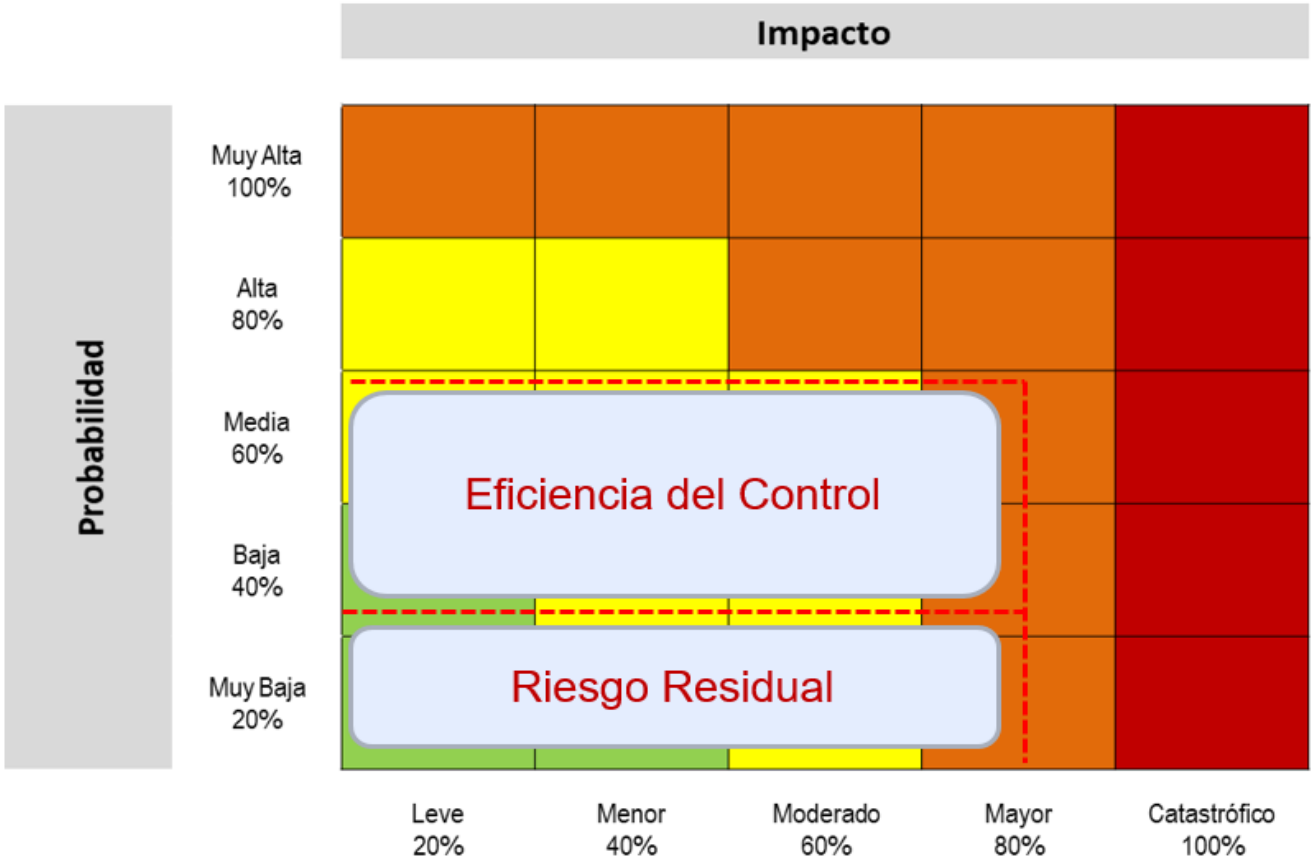
Para mayor claridad, se realizan los cálculos requeridos para la aplicación de los controles.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
R1	Probabilidad inherente	PI%	Valoración control 1 preventivo	VP%	PI% x VP%= PV% PI% - PV% = PV2%
	Valor probabilidad para aplicar 2o control	VP2%	Valoración control 2 detectivo	VD%	VP2% x VD%=VV% VP2% -VV% = PR%
	Probabilidad Residual	PR%			
	Impacto Inherente	II%	Valoración control 1 preventivo	VP%	II% x VP%= IV% II% - IV% = VI2%
	Valor Impacto para aplicar 2o control	VI2%	Valoración control 2 detectivo	VD%	VI2% xVD%= VV2% VI2% -VV2% = IR%
	Impacto Residual	IR%			

Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

Movimiento en la matriz de calor

Una vez aplicado el control dependiendo del resultado de la probabilidad y el impacto, se recalcula la zona de riesgo residual dentro de la matriz de calor



Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

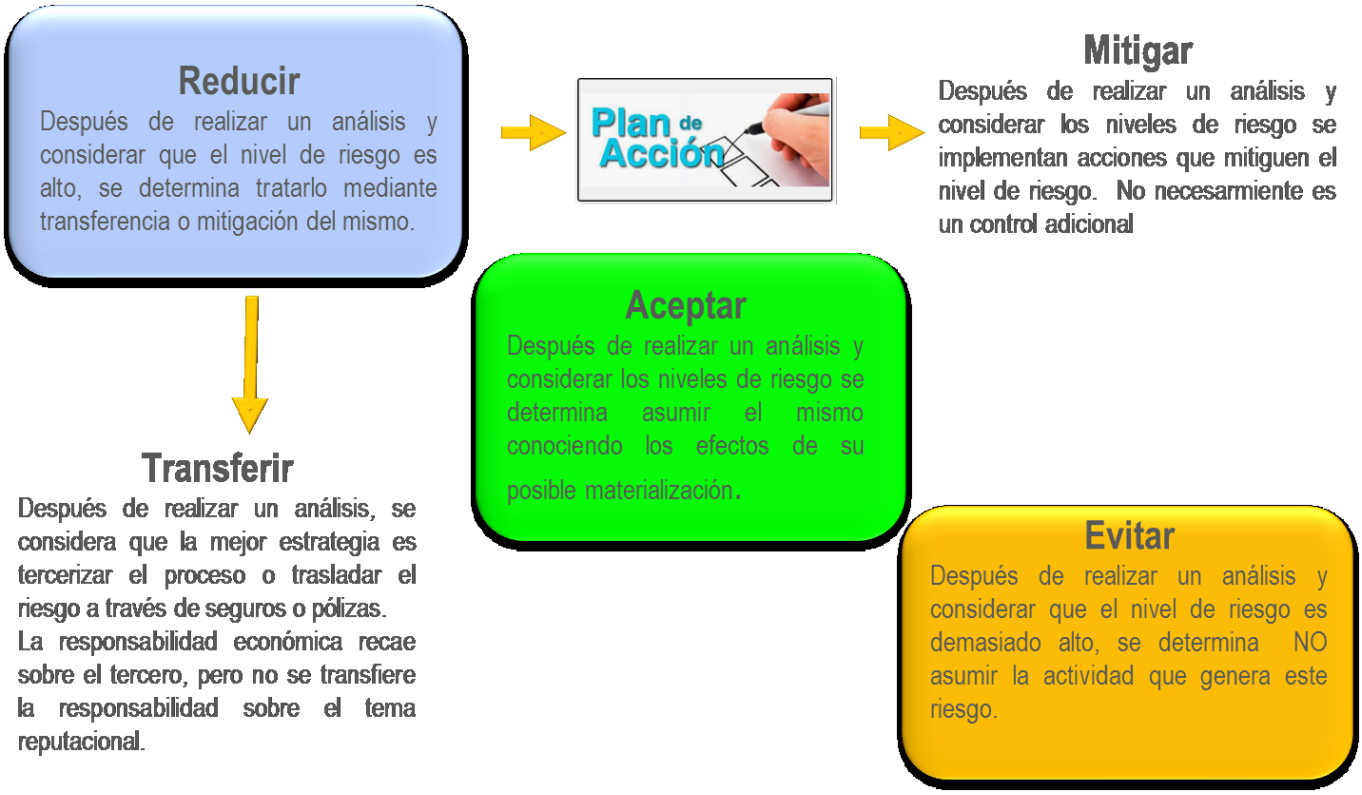
Nota 1: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto

5.4 ESTRATEGIAS PARA COMBATIR EL RIESGO:

Es la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

A continuación, se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Estrategias para combatir el riesgo



Tomada de: la Guía de administración de riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital Versión 05 del 2020.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Una vez identificado y valorado el riesgo, de acuerdo a los criterios ERCA (Evitar, Reducir, Compartir o Transferir y Aceptar), se establecen los siguientes niveles de aceptación o tolerancia de los riesgos, según su valoración.

1. **Nivel BAJO:** Se aceptará el riesgo y administrará por medio de las actividades propias del proceso asociado y su control y registro de avance se realizará semestralmente por medio del informe de desempeño.

- **Aceptar el Riesgo,** Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo. No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero

también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

2. **Nivel MODERADO:** Se deberá incluir este riesgo en el Mapa de Riesgos Institucional, se establecerán acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento trimestral y se registrarán sus avances en los informes de desempeño.

- **Reducir el Riesgo**, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La Reducción de 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, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

3. **Nivel ALTO:** Se deberá incluir el riesgo en el Mapa de Riesgos Institucional y se establecerán acciones de control preventivas que permitan EVITAR la materialización del riesgo. La administración de estos riesgos será con periodicidad trimestral y su adecuado control se registrará en los informes de desempeño.

- **Evitar el Riesgo**, Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades y tomar las medidas encaminadas a prevenir su materialización. Siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de la calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc. Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

4. **Nivel EXTREMO:** se incluirá el riesgo en el Mapa de Riesgos Institucional, se establecerán acciones de control preventivas y correctivas que permitan EVITAR la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual y su adecuado control se registrará en informes presentados a la Dirección.

- **Evitar el Riesgo**, Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades y tomar las medidas encaminadas a prevenir su materialización. Siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación,

resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de la calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc. Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

Nota: Los riesgos de corrupción son inaceptables.

- **Compartir o transferir el riesgo,** 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, reduce su efecto a través del traspaso a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permitan distribuir una porción de riesgo con otra entidad como con 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 lugar, la tercerización. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

- **Eliminación riesgos identificados,** Los riesgos que después de aplicación de sus controles, y en seguimiento, su valoración se encuentre en nivel de aceptación bajo, que soporten documentación de sus controles en sus procedimientos y evidencien implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser considerados para su eliminación.

5.5 MONITOREO Y REVISIÓN

El modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

Considerando que la Gobernación de Córdoba, debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad, establece los roles y responsabilidades de todos los actores del riesgo y control a través de las líneas de defensa:

LÍNEA ESTRATÉGICA: Define el marco general para la gestión del riesgo y el control, y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno, los cuales tienen el compromiso de realizar seguimiento al Mapa de Riesgo institucional. La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente:

- Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
- Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas.
- Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

1ra LINEA DE DEFENSA: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Los responsables de procesos realizaran el seguimiento a los controles de los riesgos de acuerdo con la periodicidad establecida y actualizaran el Mapa de riesgo institucional, cuando en la realización de los seguimientos encuentren situaciones que requieran ser ajustadas y lo remitan para su revisión y aprobación la Oficina de Control Interno.

Los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el

cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

2da LINEA DE DEFENSA: Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.
El responsable de la planeación y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a 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.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar los planes de acción 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.

3ra LINEA DE DEFENSA: Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea de defensa está conformada por el responsable de Control Interno, la cual dentro de su función de evaluación independiente presentara al Director los resultados de la evaluación de los mapas de riesgo, con las recomendaciones para la mejora continua.

El responsable de Control Interno, monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a 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.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas, para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

6. INFORMACIÓN, COMUNICACIÓN Y REPORTE

Responsabilidades por línea de defensa para la Información, comunicación y reporte de la gestión del riesgo desarrollada por la Gobernación de Córdoba.

❖ LÍNEA ESTRATÉGICA

Corresponde al Comité de institucional de coordinación de control interno, establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la entidad, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

❖ PRIMERA LINEA DE DEFENSA

Corresponde a los líderes o responsables de procesos asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.

❖ SEGUNDA LINEA DE DEFENSA

Corresponde a la persona encargada de la planeación y de la gestión del riesgo, la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

- **TERCERA LINEA DE DEFENSA**

Le corresponde al responsable del control interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Por tanto, se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de Indeportes Córdoba.

Nota: Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas. Adicionalmente, los riesgos de seguridad digital deberán ser reportados a las autoridades o instancias respectivas que el gobierno disponga.