

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

Política de administración de los riesgos de gestión, corrupción y seguridad de la información

Proceso Direccinamiento estratégico



 INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA	CODIGO	PE-PO-100-001
	SISTEMA DE GESTIÓN	VERSIÓN	2
	POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	APROBADO	10/MAR/2021

1.	MARCO NORMATIVO	4
2.	TERMINOS Y DEFINICIONES	4
3.	POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION DE INDERVALLE	8
3.1	Objetivo de la Política	8
3.2	Alcance de la Política.....	8
3.3	Niveles de tolerancia al riesgo	8
3.4	Establecimiento de la Política	8
3.5	Niveles de aceptación del riesgo	9
3.6	Tratamiento de Riesgos.....	9
4.	IDENTIFICACIÓN DE RIESGOS	9
4.1	Análisis de los objetivos estratégicos y de lo procesos.....	9
4.2	Identificación de los puntos de riesgos	9
4.3	Identificación de áreas de factores de riesgo	10
4.4	Descripción del riesgo.....	11
4.5	Clasificación del riesgo	12
5	VALORACIÓN DEL RIESGO.....	12
5.1	Análisis de Riesgos	12
5.1.1	Determinar la probabilidad	13
5.1.2	Determinar el impacto	13
5.2	Evaluación de Riesgos	14
5.2.1	Análisis preliminar (riesgo inherente)	14
5.2.2.	Valoración de controles.	14
5.3	Estrategias para combatir el riesgo.....	20
5.4	Herramientas para la gestion del riesgo.....	20
5.4.1	Gestión de eventos	20
5.4.2.	Indicadores clave de riesgo.....	21
5.5	Monitoreo y revisión.....	21
6	LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN.	22
6.1	Disposiciones generales	23
6.2	Generalidades acerca de los riesgos de corrupción	23
6.3	Identificación del riesgo de corrupción	24
6.3.1	Procesos, procedimientos o actividades susceptibles de riesgos de corrupción	24
6.3.2	Lineamientos para la identificación del riesgo de corrupción.....	25
6.4	Valoración del riesgo.....	27

 INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

6.4.1 La determinación de la probabilidad.....	27
6.4.2 La determinación del impacto	28
6.4.3 Análisis preliminar (riesgo inherente)	29
6.4.4 Valoración de controles.....	30
6.5 Seguimiento riesgos de corrupción	32
7. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACION	33
7.1 Identificación de los activos de seguridad de la información	33
7.2 Identificación del riesgo:.....	34
7.3 Valoración del riesgo.....	36
7.4 Controles asociados a la seguridad de la información.....	38

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA	CODIGO	PE-PO-100-001
	SISTEMA DE GESTIÓN	VERSIÓN	2
	POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	APROBADO	10/MAR/2021

1. MARCO NORMATIVO

- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del Control Interno: Literal a). Proteger los recursos de la organización, buscando adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
- Ley 1474 de 2011: Estatuto Anticorrupción Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
- Decreto 943 del 21 de mayo de 2014: Por el cual se actualiza el Modelo Estándar de Control Interno y se presenta el Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Componente 1.3 Administración de Riesgos y elemento 1.3.1 Políticas de Administración del riesgo.
- Guía para la administración del Riesgo y el diseño de controles en entidades públicas - Departamento Administrativo de la Función Pública- Versión 5-diciembre 2020.
- Norma Técnica Colombiana NTC-ISO 9001:2015.
- NTC ISO 31000-Gestión del Riesgo, principios y directrices-2011.
- NTC-GTC137-Gestión del Riesgo-Vocabulario-2011.

2. TERMINOS Y DEFINICIONES

- **Apetito al riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección y del órgano de gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la entidad, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en un entorno digital.
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Cadena de Valor:** Es la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios.
- **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.
- **Caracterización de los procesos:** Estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación con los demás procesos, los insumos, los

 INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

activos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos.

- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituye la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Compartir el Riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, procesos, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.
- **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.
- **Contexto Externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos que puede ser: ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, nacional, regional o local.
- **Contexto Interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos, el cual puede ser: gobierno, estructura organizacional, funciones, responsabilidades, políticas, normas, directrices adoptadas por la organización, objetivos, estrategias implementadas, recursos (capital, tiempo, personas, procesos, sistemas, tecnologías).
- **Contexto Estratégico:** Insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones internas y externas de la institución.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Controles Correctivos:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen riesgos implícitos.
- **Control Detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Controles Preventivos:** 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.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA	CODIGO	PE-PO-100-001
	SISTEMA DE GESTIÓN	VERSIÓN	2
	POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	APROBADO	10/MAR/2021

- **Establecimiento del contexto:** Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.
- **Evaluación del Riesgo:** Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Evento:** Incidente o situación potencial que puede ocurrir en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie de causas.
- **Evitar el Riesgo:** Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
- **Factores de riesgo:** Son las fuentes generadoras de riesgo.
- **Frecuencia:** Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo y proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Impacto:** Consecuencias que puede ocasionar a la entidad la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Mapa de Riesgos:** Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias y sus acciones preventivas.
- **Mapa o red de procesos:** Es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación y sus interacciones.
- **Monitorear:** Comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.
- **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.
- **Objetivo del proceso:** Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

- **Objetivos estratégicos:** Identifican la finalidad hacia la cual deben dirigirse los recursos y esfuerzos para dar cumplimiento al mandato legal aplicable a cada entidad. Estos objetivos institucionales se materializan a través de la ejecución de la planeación anual de cada 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.
- **Plan de Manejo del Riesgo:** Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.
- **Política de administración de Riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público a lo privado.
- **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.
- **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.
- **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 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 medidas de tratamiento de riesgo.
- **Tolerancia al riesgo:** Es el valor de la máxima desviación admisible del nivel del riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Valoración del Riesgo:** Elemento de control, que determina el nivel o grado de exposición de la entidad pública al impacto del riesgo, permitiendo estimar las prioridades para su tratamiento según el Decreto 1599 de 2005.

 INDERVALLE	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

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

3. POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION DE INDERVALLE

Indervalle define su política de riesgos atendiendo los lineamientos establecidos en la Guía para la Administración del riesgo y el diseño de controles en entidades públicas DAFP¹, articulada con las normas aplicables a la Entidad y al sistema de gestión de la calidad, como mecanismo para identificar, analizar, valorar, monitorear y dar tratamiento a los riesgos que pudieran afectar el cumplimiento del logro de los objetivos institucionales.

3.1 Objetivo de la Política

Establece los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la entidad.

- Suministrar una metodología que permita a todas las entidades gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso.
- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores de la entidad (Esquema de las Líneas de Defensa) en los riesgos de gestión y en los riesgos de corrupción, así como el monitoreo y seguimiento de estos.
- Suministrar lineamientos basados en una adecuada gestión del riesgo y control a los mismos, que permitan a la alta dirección de las entidades tener una seguridad razonable en el logro de sus objetivos.

3.2 Alcance de la Política

Aplica para la gestión de riesgos de todos los procesos de INDERVALLE, proyectos de la Entidad y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones. Incluye los riesgos de gestión, corrupción y seguridad de la información.

3.3 Niveles de tolerancia al riesgo

La tolerancia de 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. El límite o valor de la tolerancia de riesgo es definido por la alta dirección y no puede ser superior al valor de la capacidad del 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.

3.4 Establecimiento de la Política

Es responsabilidad de La Alta Dirección de Indervalle con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno y el Comité Institucional de Gestión y Desempeño.

¹Guía para la Administración del riesgo y el diseño de controles en entidades públicas.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

3.5 Niveles de aceptación del riesgo

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo. Los riesgos aceptados están sujetos a monitoreo. Tenga en cuenta que los riesgos de corrupción son inaceptables.

3.6 Tratamiento de Riesgos

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

4. IDENTIFICACION DE RIESGOS

4.1 Análisis de los objetivos estratégicos y de lo procesos.

Se deben analizar los objetivos estratégicos de la entidad y asegurar que se encuentren alineados con la misión y visión. Igualmente se deben analizar los objetivos de los procesos y asegurar que estos contribuyan a los objetivos estratégicos.

Los objetivos se deben formular correctamente y contener unos atributos mínimos, para la cual se puede hacer uso de las características SMART como a continuación se presenta:



4.2 Identificación de los puntos de riesgos

Actividades dentro del flujo del proceso donde se presenta evidencia o indicio de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control y así asegurar que el proceso cumpla su objetivo.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

4.3 Identificación de áreas de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la entidad en caso de materialización de un riesgo. Los impactos que aplican son: afectación económica y reputacional.

4.4 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. A continuación, un listado de ejemplo de factores de riesgo:

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

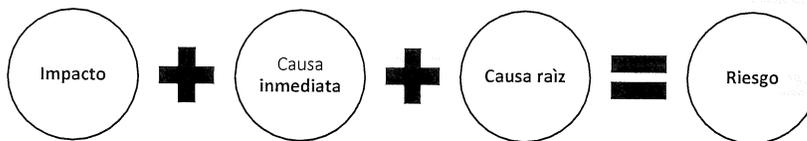
Factor	Definición		Descripción
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

Factor	Definición	Descripción	
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

4.5 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 las personas ajenas a este. Se propone la siguiente estructura que facilita su redacción y claridad que inicia con la frase **POSIBILIDAD DE:**



EJEMPLO:

Proceso: Gestión de recursos

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad.

Alcance: Inicia con el análisis de necesidades para cada uno de los procesos de la entidad y termina con la compra y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Redacción: Posibilidad de afectación económica (IMPACTO) por multa y sanción del ente regulador (CAUSA INMEDIATA) debido a adquisición de bienes y servicios fuera de los requerimientos normativos. (CAUSA RAIZ)



Premisas para una adecuada redacción del riesgo:

- No describir como riesgos OMISIONES o DESVIACIONES del control. Ejemplo: Errores en la liquidación de nómina por fallas en los procedimientos actuales.
- No describir CAUSAS COMO RIESGOS. Ejemplo: Inadecuado funcionamiento de la plataforma estratégica donde se realizar el seguimiento a planeación.
- No describir riesgos como la NEGACION DE UN CONTROL. Ejemplo: Retrasos en la prestación del servicio por no contar con digiturno.
- No existen RIESGOS TRANSVERSALES, SI CAUSAS TRANSVERSALES: Ejemplo: Pérdida de expedientes.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

4.6 Clasificación del riesgo

Permite agrupar los riesgos identificados en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en <i>hardware</i> , <i>software</i> , 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.

A continuación, se presenta la relación entre factores de riesgo y clasificación del riesgo:



5 VALORACIÓN DEL RIESGO

5.1 Análisis de Riesgos

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

5.1.1 Determinar la probabilidad

Posibilidad de ocurrencia del riesgo, la cual 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.

A continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública con sus escalas de probabilidad:

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

A continuación, los 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%

5.1.2 Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos ECONOMICOS y REPUTACIONALES como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el más alto.

A continuación, criterios para definir el nivel de impacto:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

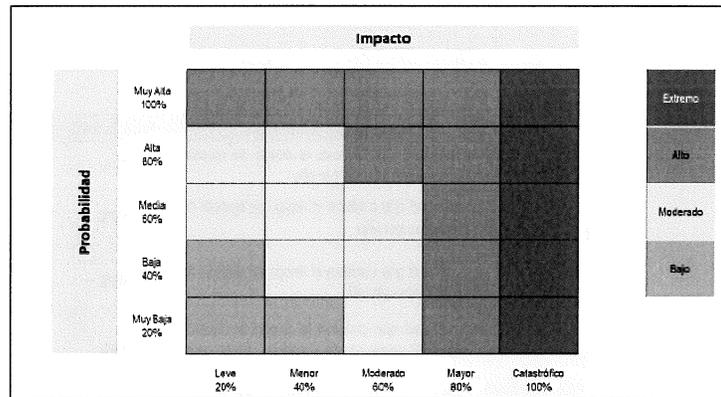
	Afección Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
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

5.2 Evaluación de Riesgos

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

5.2.1 Análisis preliminar (riesgo inherente)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



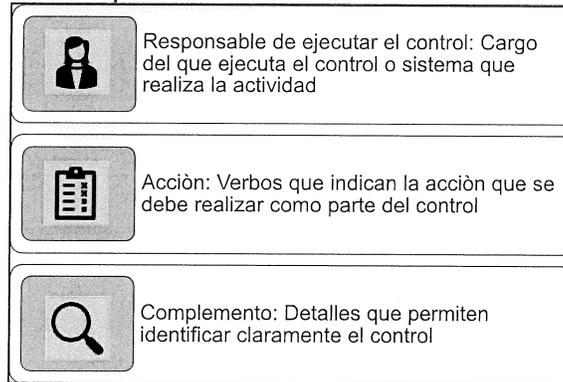
5.2.2. Valoración de controles.

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

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

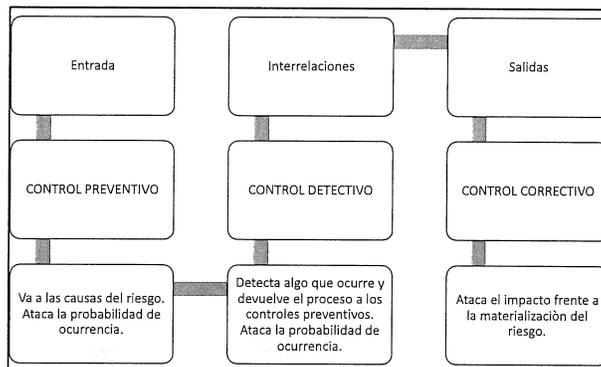
5.2.2.1 Estructura para la descripción del control:



Ejemplo: El profesional de contratación verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación a través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

5.2.2.2 Tipología de controles y los procesos

A través del ciclo de los procesos es posible establecer cuando se activa un control y por lo tanto establecer su tipología con mayor precisión como a continuación se presenta:



Igualmente se pueden tener controles manuales (personas) y automáticos (sistema).

5.2.2.3 Análisis y evaluación de controles

A continuación, se analizan los atributos para el diseño del control teniendo en cuenta características relacionada con la eficiencia y formalización.

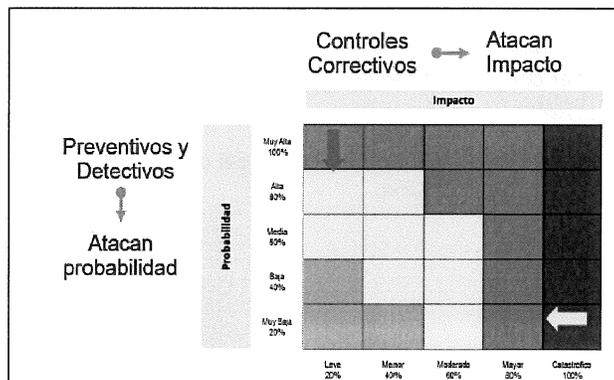
	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN	CODIGO	PE-PO-100-001
	POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	VERSIÓN	2
		APROBADO	10/MAR/2021

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	25%	

Características		Descripción	Peso	
Atributos Informativos			Intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
	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.	-

NOTA: Los atributos informativos solo dan formalidad al control y su fin es conocer el entorno del control y complementar el análisis con elementos cualitativos, sin embargo, no tienen incidencia directa en su efectividad.

A continuación, se muestra el movimiento en la matriz de calor acorde con el tipo de control:



	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

A continuación, se presenta un ejemplo de aplicación de atributos:

Controles y sus características				Peso
Control 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	X	-
Sin registro			-	
Total valoración control 1				40%
Control 2 El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-

Controles y sus características				Peso
inconsistencias, devuelve el proceso al profesional de contratos asignado.	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 2				30%

5.2.3 Nivel de riesgo (riesgo residual)

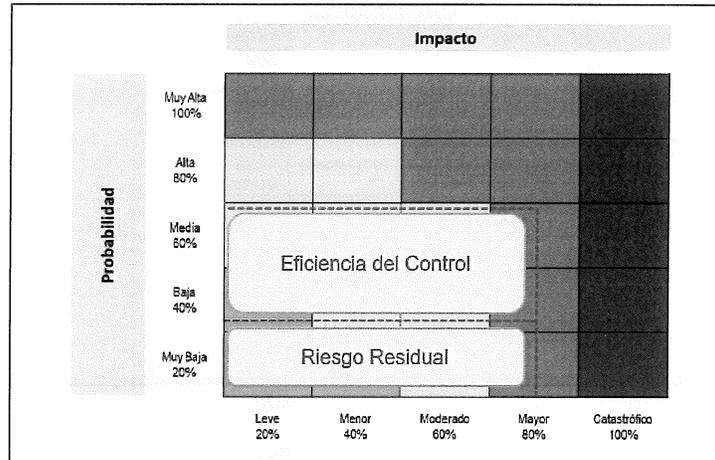
Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

A continuación, se muestra ejemplo de los cálculos requeridos para la aplicación de los controles:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Probabilidad inherente		Valoración control 1 preventivo		
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	80%		40%		$60\% * 40\% = 24\%$ $60\% - 24\% = 36\%$
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	$36\% * 30\% = 10,8\%$ $36\% - 10,8\% = 25,2\%$
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

A continuación, se muestra movimiento en la matriz de calor:



A continuación, se presenta ejemplo de mapa de riesgos:

Proceso:	Gestión de recursos										
Objetivo:	Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación										
Alcance:	Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas										
Referencia	Impacto	Causa inmediata	Causa raíz	Descripción del riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1	Afectación económica	Multa y sanción del organismo de control	Incumplimiento de los requisitos para contratación	Posibilidad de afectación económica por multa y sanciones del organismo de control debido a la adquisición de bienes y servicios fuera de los requerimientos normativos.	Ejecución y administración de procesos	120	Moderada	60%	Mayor	80%	Alta

Valoración del riesgo:

 <p>INDERVALLE INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA</p>	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN		CODIGO	PE-PO-100-001
	POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO		VERSIÓN	2
			APROBADO	10/MAR/2021

No. control	Descripción del control	Afectación		Atributos					Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento	
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia								Evidencia
1	El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación	X		Preventivo	Manual	40%	Documentado	Continua	Registro material	36%	Baja	25,2%	Mayor	80%	Alta	Reducir

No. control	Descripción del control	Afectación		Atributos					Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento	
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia								Evidencia
2	El jefe de del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	X		Detectivo	Manual	30%	Documentado	Continua	Con registro	25,2%						

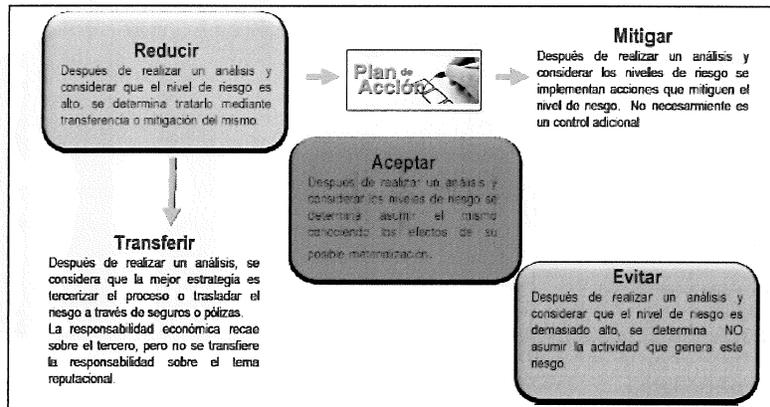
Plan de acción: OPCIONAL

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

5.3 Estrategias para combatir el riesgo

Decisión que se toma frente a un determinado nivel de riesgo, puede ser aceptar, reducir o evitar como se describe a continuación:



Frente al plan de acción referido para la opción de reducir, es importante que conceptualmente y de manera general, se trata de una herramienta de planificación 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.

5.4 Herramientas para la gestión del riesgo

Aparte de los mapas de riesgos, se cuentan con las siguientes herramientas:

5.4.1 Gestión de eventos

Evento es un riesgo materializado, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. Algunas fuentes para establecer una base histórica de eventos pueden ser:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

- Mesa de ayuda
- PQRS
- Oficina jurídica

5.4.2. Indicadores clave de riesgo

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento pueda indicar una mayor o menor exposición a determinados riesgos. No indica materialización del riesgo, pero sugiere que algo no funciona adecuadamente y se debe investigar.

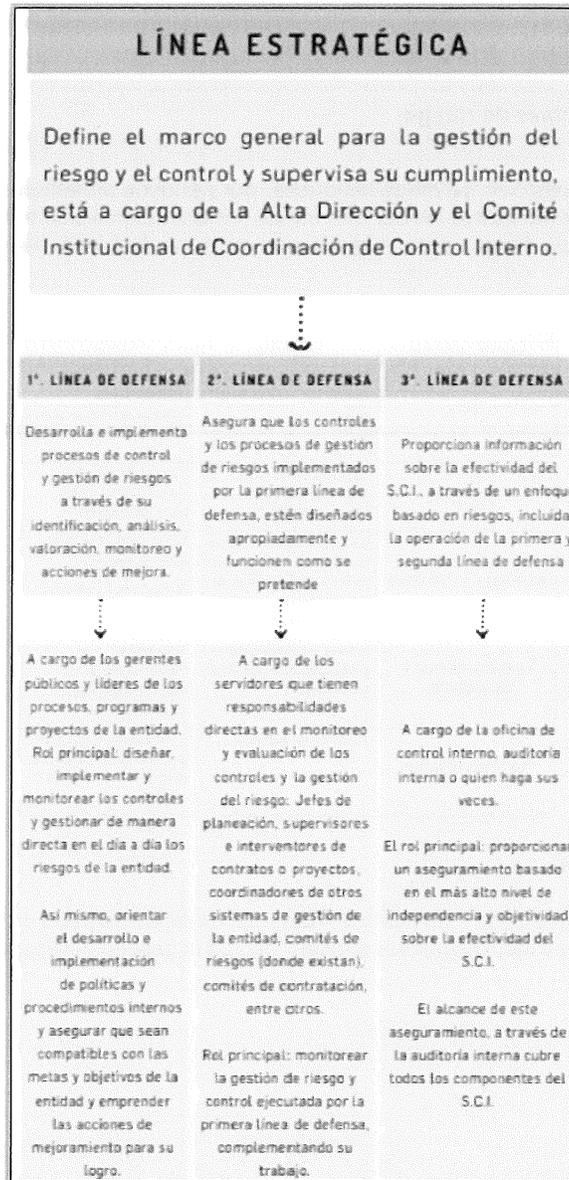
Algunos ejemplos de indicadores:

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

5.5 Monitoreo y revisión

Teniendo en cuenta la dimensión 7 de control interno del modelo integrado de planeación y gestión, las líneas de defensa permiten identificar la responsabilidad de la gestión del riesgo y control de la siguiente manera:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021



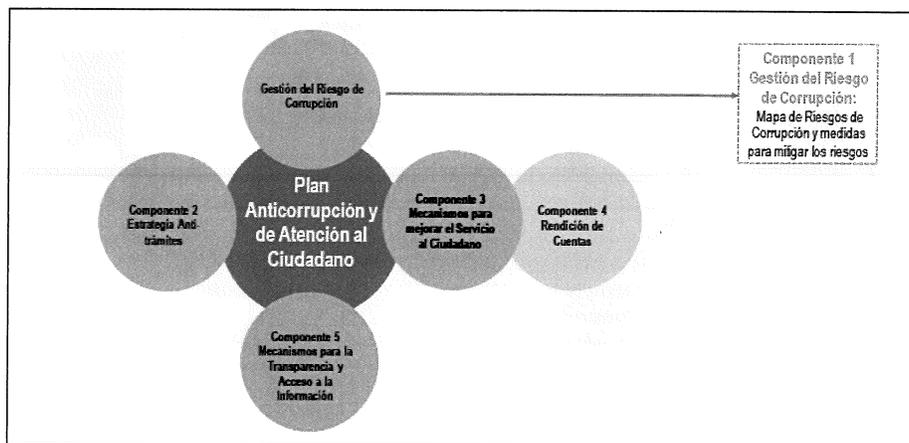
6 LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

6.1 Disposiciones generales

En el marco del Plan anticorrupción y de atención al ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción. El desarrollo de este componente se articula con los demás establecidos para el desarrollo del plan.

A continuación, se presentan los componentes del plan anticorrupción de atención al ciudadano:



En materia de riesgos asociados a posibles actos de corrupción, se deben considerar los siguientes aspectos:

- El riesgo de corrupción se define como la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de corrupción se establecen sobre procesos.
- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

6.2 Generalidades acerca de los riesgos de corrupción

- **Entidades encargadas de gestionar el riesgo:** Lo deben adelantar las entidades del orden nacional, departamental y municipal.
- Se elabora anualmente por cada responsable de los procesos al interior de las entidades, junto con su equipo.
- **Ajustes y modificaciones:** 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. Se deben dejar por escrito los ajustes, modificaciones o inclusiones realizadas.
- **Monitoreo:** Los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

- **Seguimiento:** El jefe de control interno o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. Es necesario que en sus auditorías internas analicen las causas, los riesgos de corrupción y la efectividad de los controles definidos en el mapa de riesgos de corrupción.

Teniendo en cuenta la criticidad del tema y que se requiere su publicación en la página web, las entidades podrán anonimizar la información relacionada con los controles establecidos que pueden tener relación con información clasificada o reservada como se muestra a continuación:

Información anonimizada

N.º	Riesgo	Clasificación	Causa	Probabilidad	Impacto	Riesgo Residual	Opción de Manejo	Actividad de Control
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros...	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evitar	[Redacted]

Información anonimizada

¡IMPORTANTE:
 Tenga en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.
 Una resolución no puede calificar la información como clasificada o reservada.

6.3 Identificación del riesgo de corrupción

6.3.1 Procesos, procedimientos o actividades susceptibles de riesgos de corrupción

A continuación, se presentan algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción, a partir de los cuales la entidad podrá adelantar el análisis de contexto interno para la identificación de los riesgos:

Direccionamiento estratégico (alta dirección)	<ul style="list-style-type: none"> ● Concentración de autoridad o exceso de poder. Extralimitación de funciones. ● Ausencia de canales de comunicación. ● Amiguismo y clientelismo.
--	--

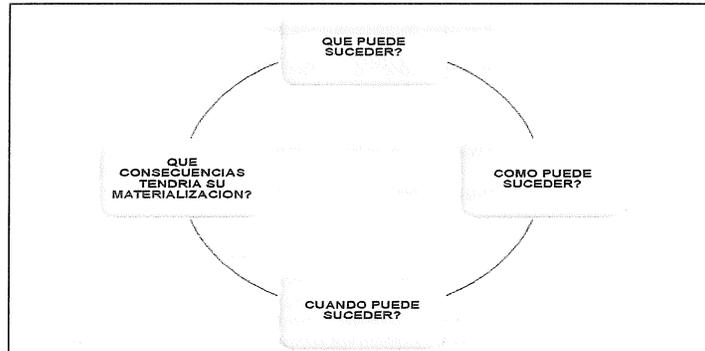
 <p>INDERVALLE INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA</p>	<p>INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA</p> <p>SISTEMA DE GESTIÓN</p> <p>POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION</p> <p>PROCESO DIRECCIONAMIENTO ESTRATÉGICO</p>	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

<p>Financiero (está relacionado con áreas de planeación y presupuesto)</p>	<ul style="list-style-type: none"> ● 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.
<p>De contratación (como proceso o bien los procedimientos ligados a este)</p>	<ul style="list-style-type: none"> ● 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.
<p>De información y documentación</p>	<ul style="list-style-type: none"> ● 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
<p>De Investigación y Sanción</p>	<ul style="list-style-type: none"> ● 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.
<p>De trámites y/o servicios internos y externos</p>	<ul style="list-style-type: none"> ● Cobros asociados al trámite. ● Influencia de tramitadores. ● Tráfico de influencias: (amiguismo, persona influyente).
<p>De reconocimiento de un derecho (expedición de licencias y/o permisos)</p>	<ul style="list-style-type: none"> ● Falta de procedimientos claros para el trámite ● Imposibilitar el otorgamiento de una licencia o permiso. ● Tráfico de influencias: (amiguismo, persona influyente).

6.3.2 Lineamientos para la identificación del riesgo de corrupción

Las preguntas claves son:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021



La descripción del riesgo de corrupción es:

RIESGO DE CORRUPCIÓN
<p>Definición de riesgo de corrupción:</p> <p>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.</p> <p><i>"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).</i></p> <p>Es necesario que en la descripción del riesgo concurren los componentes de su definición, así:</p> <p>ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.</p>

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

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

A continuación, se presenta un ejemplo de riesgo de corrupción:

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
*Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación, pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad, repercutiendo en la continuidad de su operación.	Operativo	Carencia de controles en el procedimiento de contratación Insuficiente capacitación del personal de contratos Desconocimiento de los cambios en la regulación contractual Inadecuadas políticas de operación	1. Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor 3. Demandas y demás acciones jurídicas 4. Detrimiento de la imagen de la entidad ante sus grupos de valor 5. Investigaciones disciplinarias

Fuente: Departamento Administrativo de la Función Pública.

IMPORTANTE:
 La descripción del riesgo consolida los pasos vistos en la metodología de gestión del riesgo y facilita su análisis.

6.4 Valoración del riesgo

6.4.1 La determinación de la probabilidad

La determinación de la probabilidad (posibilidad de ocurrencia del riesgo) se debe llevar a cabo de acuerdo con lo definido en los riesgos de gestión.

Se retoma la siguiente tabla:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

	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%

6.4.2 La determinación del impacto

Para la determinación del impacto frente a posibles materializaciones de riesgos de corrupción se analizarán únicamente los niveles: Moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos, por lo tanto, no aplica el nivel insignificante ni menor que aplican para los demás tipos de riesgos.

Para establecer el nivel de impacto se deben aplicar las siguientes preguntas frente al riesgo identificado:

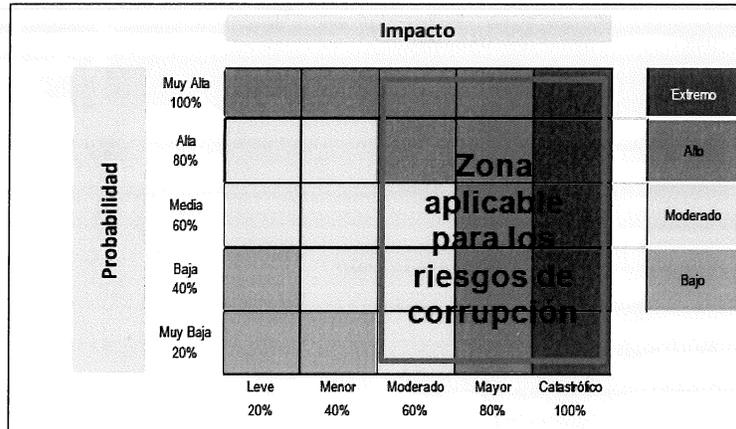
	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	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, X 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.			
CATASTRÓFICO: Genera consecuencias desastrosas para la entidad			

6.4.3 Análisis preliminar (riesgo inherente)

En esta etapa se define el nivel de severidad para el riesgo de corrupción identificado. A continuación, se muestra matriz de calor para riesgos de corrupción:

 <p>INDERVALLE</p>	<p>INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA</p> <p>SISTEMA DE GESTIÓN</p> <p>POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION</p> <p>PROCESO DIRECCIONAMIENTO ESTRATÉGICO</p>	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021



6.4.4 Valoración de controles

Aplica la valoración de controles que se manejan en los riesgos de gestión. A continuación, un ejemplo:

Gestión de la contratación								
Ejecutar las etapas precontractual y contractual en las diferentes modalidades en esta materia, acorde con el plan anual de adquisiciones aprobado para cada vigencia.								
Inicia con el análisis de las contrataciones aprobadas en el plan anual de adquisiciones y termina con las compras, contrataciones requeridas y la asignación de supervisores o interventores (según aplique).								
Referencia	Riesgo de corrupción	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Ejecución y administración de procesos	240	media	60%	mayor	80%	alta

Valoración del riesgo

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

N.º Control	Descripción del control	Afectación		Atributos							Probabilidad residual (2 controles)	Probabilidad residual Final	%	Impacto residual Final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia								
1	Para la etapa precontractual, el (la) secretario(a) general, en el marco del comité de contratación, valida los estudios previos presentados por los líderes de proceso responsables de acuerdo con la modalidad de contratación en cada caso, las decisiones tomadas son registradas en las actas del comité, firmadas por los miembros de este, lo que permite continuar con las etapas subsiguientes de los	X		Preventivo	Manual	40%	Documentado	Continua	Con registro		36%	muy baja	25,2%	mayor	80%	alta	Reducir

N.º Control	Descripción del control	Afectación		Atributos							Probabilidad residual (2 controles)	Probabilidad residual Final	%	Impacto residual Final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia								
	procesos contractuales correspondientes.																
2	Para la etapa contractual, el jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto (secretario(a) general). En el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	X		Defectivo	Manual	30%	Documentado	Continua	Con registro		25,2%						

Planes de acción (opcional-opción reducir)

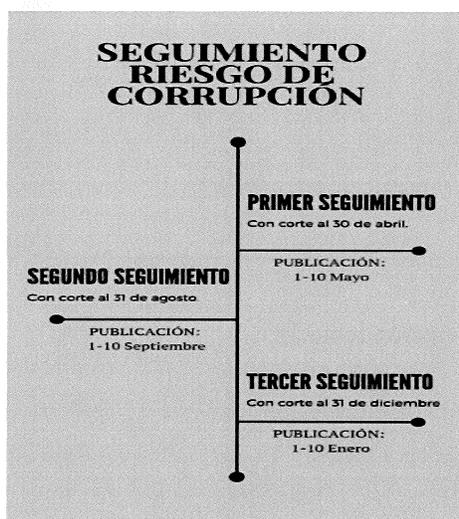
	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

Plan de Acción	Responsable	Fecha implementación	Fecha seguimiento	Seguimiento	Estado
El jefe del área de contratos, como 2ª línea de defensa, mensualmente adelanta un análisis por modalidad de contratación sobre el avance y resultados con base en los informes de supervisión e interventoría y genera las alertas ante el Comité Institucional de Coordinación de Control Interno los retrasos o incumplimientos de los contratistas, así como sobre posibles riesgos asociados a situaciones irregulares.	Coordinador área de contratación	30/10/2020	30/11/2020	Mensualmente el jefe del área de contratos debe presentar reporte ante el Comité Institucional de Coordinación de Control Interno.	En curso

6.5 Seguimiento riesgos de corrupción

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.



El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

7. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACION

Indervalle cuenta con la política general de seguridad de la información, así como el plan estratégico de tecnología de la información-PETI, los cuales complementan los lineamientos definidos en este capítulo.

7.1 Identificación de los activos de seguridad de la información

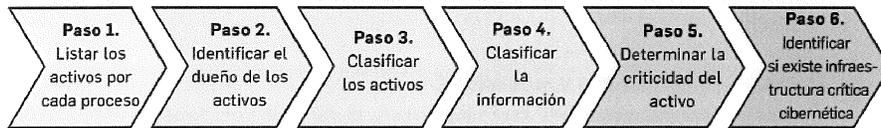
Para el inicio de la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

¿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).
¿Qué son los activos?	¿Por qué identificar los activos?
-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.

Los activos se identifican así:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



A continuación, un ejemplo de identificación de activos del proceso:

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el front office de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

7.2 Identificación del riesgo:

Se podrán identificar los siguientes tres (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 esto es necesario consultar el * Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas * donde se encuentran las siguientes tablas para el análisis:

- Tabla de amenazas comunes
- Tabla de amenazas dirigidas por el hombre
- Tabla de vulnerabilidades comunes

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

A continuación, se presenta tabla de amenazas y vulnerabilidad de acuerdo con el tipo de activo:

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

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

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

A continuación, se presenta un ejemplo de descripción del riesgo de seguridad de la información:

Seleccionar las vulnerabilidades asociadas a la amenaza identificada



RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital Ausencia de políticas de control de acceso Contraseñas sin protección Autenticación débil	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

IMPORTANTE

- * Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- * Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas"**, el cual hace parte de la presente guía.
- * **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- * **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

7.3 Valoración del riesgo

Para esta parte se utilizarán las tablas de probabilidad e impacto definidas para los riesgos de gestión al inicio de este documento.

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%

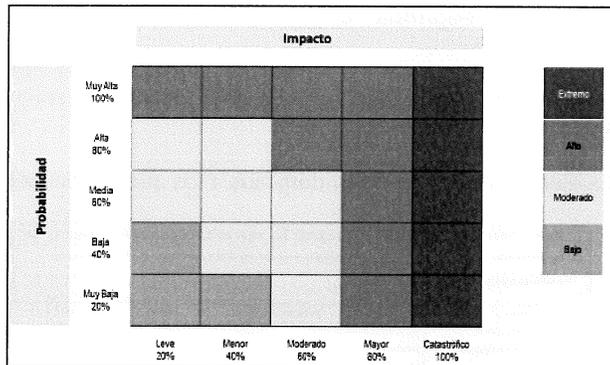
La determinación del impacto se debe llevar a cabo entendiendo el impacto como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

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

Para el análisis preliminar (riesgo inherente) en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello se aplica la matriz de calor que se manejó para los riesgos de gestión:



IMPORTANTE
 Cada entidad deberá adaptar los criterios a su realidad. El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4- Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos COISO ERM Agosto 2004

Extremo	
Alto	
Moderado	
Bajo	

IMPORTANTE:
 La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

7.4 Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando los controles del * Modelo nacional de gestión del riesgo de la información en entidades públicas * siempre y cuando se ajusten al análisis de riesgos.

A continuación, algunos ejemplos de controles y dominios a los que pertenecen:

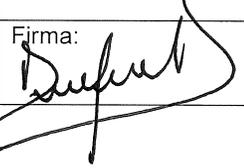
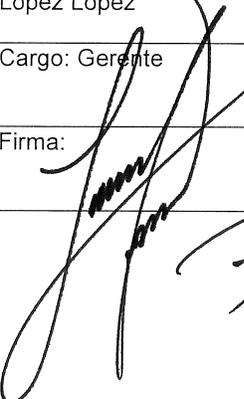
Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios 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 pérdida 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.

	INSTITUTO DEL DEPORTE, LA EDUCACIÓN FÍSICA Y LA RECREACIÓN DEL VALLE DEL CAUCA SISTEMA DE GESTIÓN POLÍTICA DE ADMINISTRACION DE LOS RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DE LA INFORMACION PROCESO DIRECCIONAMIENTO ESTRATÉGICO	CODIGO	PE-PO-100-001
		VERSIÓN	2
		APROBADO	10/MAR/2021

Ejemplo mapa de riesgos seguridad de la información:

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
10	Pérdida de la integridad	Base de datos de nómina	Seguridad digital	Multificación no autorizada	Ausencia de políticas de control de acceso	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	EFICACIA: Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 EFFECTIVIDAD: Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Reducir				A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018		
					Reducir				A.9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018		
					Reducir				A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018		

*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Elaboró:	Revisó:	Aprobó	Incorporó SGI
Nombre: Sabina Collazos Ramírez	Nombre: Dayra Faisury Borado	Nombre: Carlos Felipe López López	Nombre: Dayra Faisury Borado Gómez
Cargo: Contratista Profesional-Subgerencia de Planeación	Cargo: Subgerente de Planeación	Cargo: Gerente	Cargo: Subgerente de Planeación
Firma: 	Firma: 	Firma: 	Firma: 

