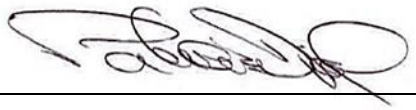
	Responsable del Proceso	Dirección de Planeación
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	Patricia Duque Cruz	Michael Andrés Ruíz Falach
Cargo:	Contralora Auxiliar	Director Técnico
Dependencia:	Despacho Contralor Auxiliar	Dirección de Planeación
R.R. Nº 031		**Fecha: 06-diciembre-2021**

1. OBJETIVO:

Establecer las actividades para la Administración de los Riesgos Institucionales en la Contraloría de Bogotá D.C., encaminadas a disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones en que se pueda ver expuesta la Contraloría de Bogotá, D.C., en cumplimiento de la misión institucional.

2. ALCANCE:

El procedimiento inicia con la elaboración de la Política de Administración de Riesgos en coordinación con los responsables de procesos del Sistema Integrado de Gestión – SIG y termina cuando el Jefe de la Oficina de Control Interna presenta el informe ejecutivo sobre el seguimiento al Mapa de Riesgos Institucional ante el Comité Institucional de Coordinación de Control Interno.

3. BASE LEGAL:

NORMA	FECHA	DESCRIPCIÓN
Constitución Política	20-jul-1991	Constitución Política de la República de Colombia. Arts. 267, 268, 272 y 274, reformados por el Acto Legislativo 04 del 2019 por medio del cual se reforma el régimen de control fiscal.
Decreto Ley 403	16-jun-2020	Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.
Ley 87	29-nov -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.

NORMA	FECHA	DESCRIPCIÓN
Ley 489	29-dic-1998	Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones, capítulo VI.
Ley 1474	12-jul-2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, artículo 73.
Ley 1712	06-mar-2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1716	14-may-2009	Por el cual se reglamenta el artículo 13 de la Ley 1285 de 2009, el artículo 75 de la Ley 446 de 1998 y del Capítulo V de la Ley 640 de 2001. (Comité de Conciliación).
Decreto 2641	17-dic-2012	Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011.
Decreto 1081	18-Ene-2015	Decreto Reglamentario Único del Sector de la Presidencia de la República, Libro 2, Parte 1, Titulo 1, Capitulo 1, Artículo 2.1.1.1.1 y s.s.
Decreto 1072	26-may-2015	Por el cual se expide el Decreto Único Reglamentarios del Sector Trabajo, Libro 2, Titulo 4, Capítulo 6, Sistema de Gestión de la Seguridad y Salud en el Trabajo.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1 - Título 9, subrogado por el Decreto 1008 de 2018.
Decreto 1069	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del sector de Justicia y del Derecho.
Decreto 1081	26-may-2015	Por medio del cual se expide el Decreto Reglamentario Único del sector Presidencia de la República.
Decreto 1083	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto 124	26-ene- 2016	Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".
Decreto 648	19-abr-2017	Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, art. 2.2.21.1.6, literal g.
Decreto 1499	11-sep-2017	Por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

NORMA	FECHA	DESCRIPCIÓN
Decreto 1008	14-jun-2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Guía Nº. 7 Gestión de Riesgos y Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
Acuerdo 658	21-dic-2016	Por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Acuerdo 664	28-mar-2017	Por el cual se modifica parcialmente el Acuerdo 658 del 21 de diciembre de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Norma NTC-ISO 27001:2013	11-dic-2013	Sistema de Gestión de la Seguridad de la Información – Requisitos.
Norma NTC-ISO 9001:2015	23-sep-2015	Sistema de Gestión de la Calidad – Fundamentos y Vocabulario.
Norma NTC - ISO 9000:2015	23-sep-2015	Sistema de Gestión de la Calidad - Requisitos.
Norma NTC-ISO 14001:2015	15-oct-2015	Sistemas de Gestión Ambiental - Requisitos con orientación para su uso.

4. DEFINICIONES:

ACCIÓN: Conjunto de actividades tomadas para eliminar la(s) causa(s) identificadas en el análisis de riesgos.

ACTIVO: Es cualquier elemento que tenga valor para la organización, sin embargo, 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.

APETITO AL RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

ÁREA DE IMPACTO: Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse el riesgo.

CADENA DE VALOR: La cadena de valor es la relación secuencial y lógica entre insumos, actividades, productos y resultados en la que se añade valor a lo largo del proceso de transformación total. (DNP, 2017, pág. 5).

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

CAUSA INMEDIATA: 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.

CLASIFICACIÓN DEL RIESGO: Permite agrupar los riesgos identificados en las siguientes categorías: Ejecución y administración de procesos, a saber:

- Fraude externo.
- Fraude interno.
- Fallas tecnológicas.
- Relaciones laborales.
- Daños a activos fijos / Eventos externos.
- Usuarios, productos y practicas

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 DE LA ORGANIZACIÓN: Combinación de factores internos y externos que pueden tener un efecto en el enfoque de la organización para el desarrollo y logro de sus objetivos:

- **Contexto Externo.** Ambiente externo en el cual la organización busca alcanzar sus objetivos, como: económicos, ambientales, políticos, sociales y culturales, tecnológicos, legales y reglamentarios, comunicación externa.

- **Contexto Interno.** Ambiente interno en el cual la organización busca alcanzar sus objetivos, como: financieros, personal, procesos, tecnología, estratégicos, comunicación interna.

CONTROL: Medida que permite reducir o mitigar un riesgo según el ciclo del proceso, se tiene los siguientes **tipos de controles**:

- **Control Preventivo.** Control accionado en la **entrada** del proceso (insumos) 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 y de acuerdo con la forma como se ejecutan los riesgos tenemos:

- **Control automático.** Son ejecutados por un sistema.
- **Control manual.** Controles que son ejecutados por personas.

DAÑO ANTIJURÍDICO: Perjuicio causado con ocasión de la acción u omisión de una autoridad pública, cuando no existe un título legal que le imponga a la víctima el deber de soportar la afectación de su patrimonio.

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad

ESTRATEGIAS PARA TRATAR O COMBATIR EL RIESGO: Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar:

- **Aceptar riesgo**: Después de realizar el análisis y considerar los niveles de riesgo, se determina **asumir** el mismo conociendo los efectos de su posible materialización.
- **Evitar riesgo:** Después de realizar el análisis y considerar que el nivel de riesgo es demasiado Alto, se determina **NO asumir** la actividad que genera este riesgo.
- **Reducir el riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es Alto, se determina tratarlo mediante transferencia o mitigación del mismo:
  - **Transferir:** Después de realizar el análisis, se considera que la mejor estrategia es **tercerizar el proceso o transferir el riesgo** a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
  - **Mitigar:** Después de realizar el análisis y considerar los niveles de riesgo, se **implementan acciones** que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

EVENTO: Incidente o situación, que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

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

INDICADOR: Expresión cuantitativa observable y verificable que permite describir características, comportamientos o fenómenos de la realidad. Esto se logra a través de la medición de una variable o una relación entre variables, se expresa en los siguientes tipos:

- **Indicadores de Gestión.** Miden los dos primeros eslabones de la cadena de valor, es decir, los insumos y las actividades, dado que en estos dos eslabones es en donde mayor énfasis debe hacer una entidad para mejorar la eficiencia de su proceso productivo.

- **Indicadores de Producto.** Miden los bienes y servicios que son generados y entregados, cumpliendo los estándares de calidad definidos, como consecuencia de la transformación de los insumos a través de un proceso de producción.

- **Indicadores de Resultado**. Son aquellos que cuantifican los efectos relacionados con la intervención pública; dichos efectos pueden ser incididos por factores externos y no necesariamente se producen directamente por la intervención pública.

INFORMACIÓN: Todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración[1].

Por otra parte, la Ley 1712 de 2014, artículo 6, la define como: *"Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen".*

INFORMACIÓN PÚBLICA: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal[2]. Está disponible al ciudadano, funcionarios, contratistas, subcontratistas y demás personal que trabaja para la Contraloría de Bogotá.

INFORMACIÓN PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014[3].

[1] Tomada de http://www.iso27000.es/sgsi.html
[2] Tomado de la ley 1712 2014
[3] Tomado de la ley 1712 2014

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014[4]

INTEGRIDAD: Propiedad de exactitud y completitud.

INVENTARIO DE ACTIVOS DE INFORMACIÓN: Se identifica los activos de información importantes para la Contraloría de Bogotá, D.C. para así clasificarlos, calificarlos y darles el tratamiento adecuado para su protección

MAPA DE RIESGOS DE CORRUPCIÓN: Herramienta que le permite a la entidad identificar, analizar y controlar los posibles hechos generadores de corrupción, tanto internos como externos. A partir de la determinación de los riesgos de posibles actos de corrupción, causas y sus consecuencias se establecen las medidas orientadas a controlarlos.

MAPA DE RIESGOS INSTITUCIONAL: Documento que contiene los riesgos a los cuales está expuesta la entidad: Gestión, Corrupción y Seguridad de la Información, a los cuales se les ha formulado acciones para mitigarlos, reducirlos o eliminarlos.

MONITOREO: Actividad encaminada a comprobar, supervisar, observar o registrar la forma en que se lleva a cabo o se cumplió la acción, el cual permite determinar la necesidad de modificar, actualizar o mantener en las mismas condiciones los factores de riesgos, así como su identificación, análisis y valoración.

NIVEL DE RIESGO: 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.

PARTES INTERESADAS: Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión u actividad que realice la Entidad.

PÉRDIDA: Consecuencia negativa que trae consigo un evento.

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

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión de riesgos. La gestión o administración del riesgo establece los lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

RIESGO: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas

[4] Tomado de la ley 1712 2014

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

Se tienen los siguientes tipos de riesgos:

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

- **Riesgo de Gestión**: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de la entidad o del proceso, entre **otros:**

  - **Riesgo Antijurídico.** Se produce por la actuación incorrecta, irregular, omisiva o por la extralimitación de funciones del servidor público, pudiendo dar lugar a que un juez condene patrimonialmente a la Institución, para que repare los perjuicios ocasionados.

  - **Riesgo de Cumplimiento.** Se asocia con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

  - **Riesgo Estratégico.** Se asocia con la forma en que se administra la entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta dirección.

  - **Riesgo Financiero.** Se relaciona con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

  - **Riesgos Operativos.** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, definición de los procesos, estructura de la entidad y articulación entre dependencias

- **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. Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente lo otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

  En este sentido se tiene que:

  - **Activo:** En relación con la seguridad de la información, se refiere a cualquier información elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización y afecte los siguientes aspectos de seguridad de la información:

- ✓ **Confidencialidad.** Garantiza que solo las personas o entidades autorizadas tendrán acceso a la información y datos recopilados y que estos no se divulgarán sin el permiso correspondiente.

- ✓ **Integridad.** Garantiza la exactitud y completitud de la información, es decir, es decir, que la información se muestra tal y como fue concebida, sin alteraciones o manipulaciones que no hayan sido autorizadas expresamente.

- ✓ **Disponibilidad.** Garantiza que la información estará disponible en todo momento para aquellas personas o entidades autorizadas para su manejo y conocimiento.

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:

- ✓ **Amenazas.** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

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

SEGUIMIENTO: Actividad realizada por la Oficina de Control Interno en la cual se analizan las causas, los riesgos y la efectividad de los controles incorporados en el Mapa de Riesgos.

TOLERANCIA AL RIESGO: Valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

VALORACIÓN DE RIESGOS: Establece la probabilidad de ocurrencia y nivel del riesgo, se determinan en dos escenarios:

- **Análisis de Riesgos.** Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgos inicial o **INHERENTE**:

  - ➢ **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.

  - ➢ **Impacto**. Consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Evaluación de Riesgos:** Busca confrontar los resultados del análisis de riesgos inicial o Inherente frente a los controles establecidos, con el fin de determinar la zona de riesgos final o **RESIDUAL**.

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
5.1. Elaboración y aprobación de la Política de Administración de Riesgos				
1	Director Técnico de Planeación	Elabora la Política de Administración de Riesgos en coordinación con los responsables de procesos del SIG.		
2	Contralor, Contralor Auxiliar, Director, Jefe de Oficina, (Comité Coordinación de Control Interno)	Revisa, aprueba y socializa la política de administración de riesgos.	Política de Administración de Riesgos. PDE-09 Acta Comité Institucional de Coordinación de Control Interno - CICCI. PGD-02-07	**Punto de Control:** Verifica que la política de administración de riegos contenga los lineamientos establecidos en la metodología vigente diseñada por el DAFP.
5.2 Identificación de riesgos:				
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Responsable de Proceso)	Convoca a reunión al equipo de gestores para identificar los riesgos de gestión, riesgos de corrupción y riesgos de seguridad de la información que pueden afectar el logro de los objetivos del proceso.		**Observación**: El equipo de gestores debe estar conformado por funcionarios de todas las dependencias que hacen parte del proceso y en lo posible asegurar el ejercicio participativo que incluya todos los niveles de la dependencia. Los facilitadores de la Dirección de Planeación brindarán el acompañamiento respectivo.
2	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Analiza los siguientes insumos con el fin de identificar posibles situaciones generadoras de riesgo para el proceso: • Plan Estratégico Institucional. • Lineamientos de la Alta Dirección. • Política de Prevención del Daño Antijurídico. • Política de administración de riesgos.		

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		• Contexto estratégico del proceso. • Análisis de Impacto al Negocio – BIA del proceso, dispuesto en la Intranet: http://intranet.contraloriabogota.gov.co/video-tutoriales-cifrado-de-la-informaci-n, el cual busca determinar los eventos y los factores externos que pueden afectar en forma adversa a la entidad y sus instalaciones. • Nivel del riesgo residual de aquellos riesgos que tienen continuidad para la siguiente vigencia.		**Observación:** El Informe del Análisis de Impacto al Negocio – BIA para la Contraloría de Bogotá D.C.,fue elaborado dentro del contexto del dominio A 17 - Aspectos de la seguridad de la información de la gestión de continuidad de negocio - de la norma ISO/IEC 27001:2013.
3	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Analiza el objetivo y actividades claves del proceso o puntos de riesgos (Caracterización del Proceso), e identifica aquellos factores que evidencien o den indicios de que pueden ocurrir eventos de riesgos para el proceso.		**Observación:** La caracterización del proceso señala la cadena de valor del Proceso: Insumos, actividades de transformación, salidas o resultados del proceso.
4	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Diligencia la siguiente información en los campos del "Sistema de Administración de Riesgos Institucionales – SARI" de la Entidad. (Ver estructura PDE-07-01 "Mapa de Riesgos Institucional"	Acta Equipo de Gestores (PGD-02-07)	**Observación:** Previo al diligenciamiento de la información en el aplicativo de riesgos, se sugiere realizar el ejercicio en el formato PGD-07-01. Las tablas señaladas en el procedimiento se encuentran inmersas en el formato PDE-07-02.
5	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Selecciona el contexto interno y externo Interno del proceso, teniendo en cuanta las debilidades y amenazas identificadas en diagnóstico DOFA del proceso • Externo: económicos, ambientales, políticos, sociales y culturales, tecnológicos, legales y reglamentarios, comunicación externa, entre otros.		**Observación:** Los aspectos identificados en el resultado de la matriz DOFA (Debilidades y Amenazas) valoradas con 3 "Alto", deben ser llevadas al mapa de riesgos del proceso.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		• Interno: financieros, personal, procesos, tecnología, estratégicos, comunicación interna,		
6	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Diligencia las casillas de definición del riesgo señalas en la Tabla No. 1, si todas son contestadas afirmativamente, se trata de un **Riesgo de Corrupción**, de lo contrario se trata de otro tipo de riesgos.		
7	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Identifica el tipo de riesgo: • Gestión: Gestión: antijurídico, cumplimiento, estratégico, financiero y operativos, entre otros. • Corrupción. • Seguridad de la Información.		
8	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Clasifica el riesgo en las siguientes categorías, (ver Tablas 2 y 3. Clasificación de riesgos Vs Factores de riesgos), entre otros: • Ejecución y administración de procesos. • Fraude externo. • Fraude interno. • Fallas tecnológicas. • Relaciones laborales. • Usuarios, productos y prácticas. • Daños a activos fijos/eventos externos.		**Observación:** Esta actividad no aplica para Riesgos de Seguridad de la Información.
9	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Selecciona las áreas de factores de riesgo del proceso, entre ellos: procesos, talento humano, tecnología, Infraestructura, evento extorno, entre otros. Ver Tabla No. 4. Factores de riesgos.		**Observación:** Esta actividad no aplica para Riesgos de Seguridad de la Información.
10	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Señala las áreas de **impacto** o consecuencia ECONÓMICA (presupuestal) y/o REPUTACIONAL, a la cual se ve expuesto el proceso o área en caso de materializarse el riesgo.		

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
11	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Redacta las causas o circunstancias generadoras del riesgo, con base en el análisis del contexto del proceso (Externo, Interno), teniendo en cuenta que para un mismo riesgo pueden existir una o varias causas. **Nota**. Para Riesgos de Gestión y Corrupción continua actividad 17.		
12	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	**Riesgos de Seguridad de la Información:** Registra el tipo de activo de información del proceso, los cuales se encuentran publicados en la página WEB de la entidad, entre otros tenemos: • Información digital y física. • Software. • Hardware. • Servicios. • Base de datos. • Componentes de red. • Recurso Humano. • Instalaciones.		**Observación:** La identificación de los activos de información permite determinar, qué elementos son los más importantes para el proceso para la prestación del servicio.
13	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Selecciona los tipos de aspectos de seguridad de la información que pueden verse afectados en el evento de materializarse el riesgo: • Pérdida de confidencialidad. • Pérdida de la integridad. • Pérdida de la disponibilidad.		
14	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Señala la criticidad de los activos de información del proceso, clasificada en: Alta y Media.		**Observación:** Los procesos que no presentan activos de información con criticidad **ALTA** deben seleccionar activos de criticidad **MEDIA** según determinación de la importancia del activo de información.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
15	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Selecciona el tipo de Amenaza identificada, según el activo escogido para el proceso, ver Tabla No. 5, entre otros tenemos: • Daño físico. • Eventos naturales. • Perdida de los servicios esenciales. • Perturbación debida a la radiación. • Compromiso de la información • Fallas técnicas. • Acciones no autorizadas. • Compromisos de las funciones. **Nota.** Para las A**menazas Humanas:** se activan los campos de Figura, Motivación y Acciones Amenazantes. Ver Tabla No. 6. Acciones amenazantes – Amenaza Humana.		**Observación:** Verifica que para cada riesgo se debe asociar el tipo de activo(s) del proceso y analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Una amenaza puede tener varias vulnerabilidades por lo tanto se debe verificar la selección de mínimo una..
16	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Seleccione las **Vulnerabilidades** asociadas a la amenaza identificada, a partir del tipo de activo de información identificado. Ver Tabla No. 7. Guía de vulnerabilidades comunes.		**Observación;** Para que una 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. En caso de no encontrar la información requerida en las tablas 6 y 7 redacte la vulnerabilidad y amenaza.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
17	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Redacta el riesgo de seguridad de la información iniciando con la frase "Posibilidad de" e incorporando los siguientes aspectos: QUÉ, (impacto), CÓMO? y POR QUÉ (vulnerabilidades/causas). Ver Imagen Nº. 1. Estructura redacción del riesgo.		**Observación:** Para los r**iesgos de Corrupción** enfocar la redacción a: 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 seguridad digital se encuentran inmersos en los riegos de Seguridad de la Información.
5.3 Análisis del Riesgo.				
18	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Realiza el análisis de los riesgos, con el fin de determinar el riesgo I**nherente**, teniendo en cuenta los criterios para calificar la probabilidad y el impacto: **Riesgos de Gestión y Seguridad de la Información:** Determina la **Probabilidad**. según criterios definidos en la Tabla No. 8, a saber: • Muy baja = 20%. • Baja = 40%. • Media = 60%. • Alta = 80%. • Muy alta = 100%. Determina el **Impacto** (económico y/o reputacional), según criterios establecidos en la Tabla No. 9, así: • Leve = 20%. • Menor = 40%. • Moderado = 60%. • Mayor = 80%. • Catastrófico =100%.		**Observación:** La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un (1) año. Para efectos de establecer el valor del impacto se debe seleccionar el valor de la afectación económica y reputacional, entre estos valores se escoge el mayor para así determinar el valor y color del impacto. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
19	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	**Riesgos de Corrupción:** Determina la **Probabilidad,** según criterios establecidos en la Tabla Nº. 10, a saber: • Rara vez. • Improbable. • Posible. • Probable. • Casi seguro. Determina el **Impacto,** según criterios establecidos en la Tabla No. 11.		**Observación:** Para calificar el impacto, se debe dar respuesta (si/no) a 19 preguntas, posteriormente se comparan las respuestas positivas con los parámetros de referencia para obtener una calificación de cinco (5) impacto moderado, diez (10) impacto mayor y veinte (20) impacto catastrófico según el caso.
20	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Determina la Zona de Riesgo Inherente (campo calculado), a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos (Ver Tabla Nº. 12. Zona de Riesgo): • Extremo. • Alto. • Moderado. • Bajo.		**Observación.** Aunque se utilice el mismo Mapa de Calor para todos los riesgos, a los riesgos de corrupción solo les aplican las columnas de impacto moderado, mayor y catastrófico, dado que esto riesgos siempre serán significativos.
5.4 Valoración de Controles				
21	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Identifica y evalúa los controles para cada tipo de riesgo, (Ver Tabla Nº. 13), a saber: **Riesgos de Gestión:** Selecciona los controles asociados a las actividades de la cadena de valor del proceso: preventivos (insumos), detectivos (actividades claves) y/o correctivos (salidas), que ayudan a mitigar las causas que originan los riesgos. Retoma el valor residual del riesgo basado en la valoración de		**Observación:** Los controles detectivos y preventivos afectan la **probabilidad** y los controles correctivos afectan el **impacto**: Para cada causa debe existir mínimo un control, en el evento de no contar con controles preventivos o detectivos, la probabilidad residual es la misma probabilidad inherente, es importante señalar que no será posible su movimiento en

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		los controles, los cuales pueden verse afectados según lo tipología de los controles. Redacta la descripción del control siguiente la siguiente estructura: responsable + acción + complemento.		la matriz para la probabilidad. **Observación:** Ejemplo redacción del control: 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.
22	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	**Riesgos de Seguridad de la Información:** Selecciona los controles de Seguridad de la Información de la lista desplegable de los 114 del Anexo "A" de la Norma ISO/IEC 27001:2013 anexo "A", los cuales se encuentran en el anexo 4 "*Modelo Nacional de Gestión de riesgos de seguridad de la información en entidades públicas*", relacionados en la tabla Nº. 14.		
23	Director, Subdirector, Jefe de Oficina Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	**Riesgos de Gestión y seguridad de la Información:** Evalúa los atributos del control: eficiencia e informativos (Ver tabla Nº. 15), así: • **Atributos de eficiencia**: Compuesto por los campos de: **Tipo.** Lista desplegable con los siguientes ítems y valores: ➢ Preventivo – 25% - control asociado a las entradas del proceso (insumos). Afecta la probabilidad. ➢ Detectivo – 15% - control		**Observación:** Un control puede ser tan eficiente que ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa especifica. Sí el resultado de la calificación del control está por debajo de 96 %, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		asociado durante la ejecución del proceso. Afecta la probabilidad. ➢ Correctivo – 10% - Control asociado a la salida del proceso. Afecta el impacto. **Implementación**: Lista desplegable con los siguientes ítems: ➢ Automático - 25%. ➢ Manual - 15%. • **Atributos Informativos.** Compuesto por los campos de: **Documentación** Lista desplegable con los siguientes ítems: ➢ Documentado - 0%. ➢ Sin documentar - 0%. **Frecuencia**. Lista desplegable con los siguientes ítems: ➢ Continua - 0%. ➢ Aleatoria - 0%. **Evidencia**: Lista desplegable con los siguientes ítems: ➢ Con registro - 0%. ➢ Sin registro - 0%. Obtiene la valoración total del control (campo calculado), a través de la sumatoria de los porcentajes seleccionados de los campos de tipo e implementación. (Ver ejemplo Tabla 16).		Para cada amenaza identificada en los riesgos de seguridad de la información, debe existir un control.
24	Director, Subdirector, Jefe de Oficina Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	**Riesgos de Corrupción:** Selecciona los controles asociados a las actividades de la cadena de valor del proceso: preventivas (insumos) y detectivas (actividades claves) que ayudan a mitigar las causas		**Observación:** Para los riesgos de corrupción únicamente disminuya la **probabilidad.** No aplica para **impacto**

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		que originan los riesgos. Evalúa y califique el diseño del control de acuerdo con los puntajes establecidos en las Tabla Nº. 17 *"Peso o participación de cada variable en el diseño del control para mitigación del riesgo* y Tabla No. 18 "*Calificación del diseño del control"* (aplica para todos los riesgos). Califique según puntaje de referencia. Evalúa y califique la ejecución del control, según tabla Nº. 19. *Calificación de ejecución del control.* Evalúa la solidez individual de cada control, tabla No 20 *"calificación solidez individual del control".* Evalúa y califique la solidez del conjunto de controles, agrupe los controles por cada riesgo, calcule el promedio aritmético simple de la solidez individual de los controles y localice el puntaje en tabla No 21. *"Calificación de la solidez del conjunto de controles*". Determina la nueva calificación de probabilidad o impacto de acuerdo con el puntaje total de los controles y atendiendo lo establecido en la tabla Nº. 22. *"Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos".*		**Observación:** Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.
5.5. Plan de Tratamiento de Riesgos				
25	Director, Subdirector, Jefe de Oficina Gerente, Asesor, Profesional o	Determina el nivel o zona de riesgo Residual (campo calculado), producto del resultado de aplicar la		**Observación.** En todos los casos para los riesgos de corrupción

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
	Técnico. (Equipo de Gestores del Proceso)	efectividad de los controles al riesgo inherente y el desplazamiento de la probabilidad o del impacto de los riesgos. Ver tabla Nº. 23, así: • Extremo. • Alto. • Moderado. • Bajo. Seleccione la medida de tratamiento del riesgo, así: • **Reducir el riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es Extremo, Alto o Moderado, se determina tratarlo mediante transferencia o mitigación del mismo, es decir, **Se adoptan medidas** para reducir la probabilidad o el impacto del riesgo o ambos. • **Aceptar riesgo**: Después de realizar el análisis y considerar el nivel de riesgo es Bajo, se determina asumir el riesgo, conociendo los efectos de su posible materialización, es decir. **NO se adopta** ninguna medida que afecte la probabilidad o el impacto del riesgo. No Aplica para los riesgos de corrupción. • **Evitar riesgo:** Después de realizar el análisis y considerar que el nivel de riesgo es demasiado **Extremo,** se determina **NO asumir** la actividad que genera este riesgo, es decir, se abandonan las actividades que dan lugar al riesgo.		la respuesta será evitar, compartir o reducir el riesgo. La opción compartir o transferir, se encuentra inmersa dentro de la posibilidad de **Reducir** el riesgo.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
26	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Establece la(s) acción(es) encaminadas a mitigar, reducir o eliminar el riesgo. Diseña el indicador que permite medir el cumplimiento de la acción propuesta.		**Observación:** La implementación de acciones aplica únicamente para la acción **REDUCIR.**
27	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Responsable de Proceso)	Aprueba el Mapa de Riesgos del Proceso, y solicita las modificaciones respectivas, en el evento de ser necesario. Remite a la Dirección de Planeación el Mapa de riesgos aprobado a través del Sistema "SARI"	Acta Equipo de gestores (PGD-02-07)	**Punto de control:** Verifica que se hayan surtido las diferentes etapas descritas para la identificación, análisis, y valoración del riesgo, señaladas en el procedimiento vigente. Verifica que las acciones formuladas estén orientadas a mitigar, reducir, o eliminar las causas que origina el riesgo.
28	Profesional Dirección de Planeación (Facilitador)	Revisa técnicamente la gestión de riesgos realizada por el proceso en el Sistema "SARI". Presenta al Director de Planeación las observaciones, en caso de ser necesario, quien informará al responsable de proceso para los ajustes correspondientes.	Nota de revisión	**Observaciones:** El Mapa de Riesgos de Corrupción hace parte del Plan Anticorrupción y de Atención al Ciudadano. El responsable de proceso realiza las modificaciones respectivas.
29	Profesional Dirección de Planeación (Facilitador)	Consolida el Mapa de Riesgos de Institucional, con base en el reporte de riesgos alimentado en el aplicativo por los responsables de procesos.		
30	Director Técnico de Planeación	Presenta ante el Comité Directivo el Mapa de Riesgos Institucional para su conocimiento y aprobación.		
31	Contralor (Comité Directivo)	Aprueba el Mapa de Riesgos Institucional para la siguiente vigencia.	Acta de Comité Directivo (PGD-02-07)	**Punto de Control:** Verifica que en la identificación, análisis y valoración de riesgos se haya tenido en cuenta lo señalado en el Procedimiento para la Administración Integral de

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
				los Riesgos Institucionales. **Observación:** El acta debe evidenciar la aprobación de los riesgos de gestión, corrupción y seguridad de la información.
32	Profesional, Técnico Dirección de Planeación	Extrae del Sistema "SARI" los riesgos de corrupción, como componente del Plan Anticorrupción y Atención al Ciudadano.		
33	Profesional, Técnico Dirección de Planeación	Publica el Mapa de Riesgos Institucional en la Intranet y página WEB de la Entidad, a más tardar el 31 de enero de cada vigencia.	Mapa de Riesgos Institucional PGD-07-01	
5.6. Modificación Mapa de Riesgos Institucional				
34	Contralor Auxiliar, Director, Subdirector, Jefe Oficina (Responsable de Proceso)	Identifica la necesidad de modificar el Mapa de Riesgos del proceso: • Creación. • Actualización. • Eliminación) Diligencia y remite a la Dirección de Planeación, a través del Sistema "SARI", la solicitud de modificación debidamente sustentada, junto con la actualización de los campos respectivos.	Solicitud de creación, actualización o eliminación de información documentada del SIG. PGD-02-01	**Observación** La solicitud de "**Actualización**", aplica para el plan de tratamiento de riesgos: Acciones, indicadores, fechas y responsables. Las solicitudes de modificación deben efectuarse previo al vencimiento de las acciones. Si la modificación es en la identificación, análisis y valoración del riesgo, se debe solicitar la eliminación del riesgo y la creación de un nuevo riesgo.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
35	Profesional Dirección de Planeación	Revisa técnicamente la solicitud de modificación al Mapa de Riesgos Institucional. Presenta al Director de Planeación las observaciones, en caso de ser necesario, quien informará al responsable de proceso para los ajustes correspondientes.		
36	Director Técnico de Planeación	Presenta al Contralor Auxiliar y a través del Sistema "SARI", .la solicitud de modificación del Mapa de Riesgos Institucional para su aprobación.		
37	Contralor Auxiliar	Analiza y aprueba las solicitudes de modificación y las remite a la Dirección de Planeación, a través del Sistema "SARI".		**Punto de Control:** Verifica que las modificaciones a los riesgos contemplen los parámetros establecidos en de este procedimiento.
38	Profesional, Técnico Dirección de Planeación	Actualiza la versión del Mapa de Riesgos Institucional, con las solicitudes de modificación aprobadas, en el evento de no ser aprobada se comunica al proceso respectivo.	Mapa de Riesgos Institucional PGD-07-01	
5.7. Monitoreo Mapa de Riesgos Institucional				
39	Director, Subdirector, Jefe de Oficina, Gerente, Asesor, Profesional o Técnico. (Equipo de Gestores del Proceso)	Realiza en el Sistema "SARI" el monitoreo al Mapa de Riesgos del proceso.		**Observación** El monitoreo se realiza según los tiempos establecidos por la entidad, después de haber finalizado el tiempo no se permite el ingreso de información.
40	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Responsable de Proceso)	Remite a la Oficina de Control Interno, a través del Sistema "SARI", el monitoreo al Mapa de Riesgos del proceso, dentro de los términos establecidos en la Circular de reporte de información vigente.	Mapa de Riesgos Institucional PGD-07-01 (Campos de Monitoreo)	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
5.8 Seguimiento Mapa de Riesgos Institucional				
41	Jefe Oficina de Control Interno	Planifica el seguimiento al Mapa de Riesgos Institucional, de conformidad con las fechas definas en la Circular de periodicidad de reporte de información.		**Observación** El seguimiento a los riesgos de corrupción se debe publicar dentro de los diez (10) primeros días hábiles de mayo, septiembre y enero.
42	Jefe Oficina de Control Interno	Comisiona los auditores de la Oficina de Control Interno para realizar seguimiento al Mapa de Riesgos Institucional.		
43	Jefe Oficina de Control Interno	Remite comunicación oficial interna a los responsables de procesos, informando sobre el auditor de la Oficina de Control Interno, asignado para adelantar el seguimiento a los riesgos del proceso	Memorando designación auditores PGD–07-02	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
44	Profesional Oficina de Control Interno	Realiza el seguimiento al Mapa de Riesgos de los procesos y lo registra el Sistema "SARI", señalando el estado de las acciones: • Abierto: El riesgo continúa para seguimiento. • Mitigado: el riesgo se estudia para determinar si este se sigue administrando o se retira del mapa de riesgos. • Materializado: el riesgo se lleva al Plan de Mejoramiento para la formulación de acciones correctivas.		**Observación:** El cumplimiento de las acciones debe estar soportado en los documentos que evidencien su ejecución y que se hayan realizado dentro de los términos establecidos. Para el seguimiento de los riesgos antijurídicos la Oficina de Control Interno tendrá en cuenta la Política de Prevención del Daño antijurídico actualizada por el Comité de Conciliación. La evaluación de los riesgos de seguridad de la información debe contemplarse como una unidad auditable más dentro del programa anual de auditorías internas de la entidad. Para el caso de la materialización de los riesgos de corrupción, la OCI deberá informar a las autoridades competentes de la ocurrencia de un hecho de corrupción.
45	Profesional Oficina de Control Interno	Elabora informe de seguimiento al Mapa de Riesgos de Gestión, Corrupción y de Seguridad de la linformación y presenta para aprobación al Jefe de la Oficina de Control Interno.		**Observación**: El Informe debe incluir además tres (3) capítulos independientes: uno para los riesgos de corrupción, otro para los riesgos de seguridad y otro para los riesgos antijurídicos.
46	Jefe Oficina de Control Interno	Aprueba el Informe de Seguimiento al Mapa de Riesgos Institucional.	Informe de Seguimiento al Mapa de Riesgos Institucional	**Punto de control.** Verifica que las políticas de prevención del daño antijurídico se encuentren reflejadas en el Mapa de riesgos a cargo de las dependencias competentes.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
47	Jefe Oficina de Control Interno	Remite a los responsables de proceso el informe de seguimiento al Mapa de Riesgos Institucional.	Memorando remisorio Informe de Seguimiento Mapa de Riesgos Institucional. PGD–07-02	
48	Jefe Oficina de Control Interno	Envía seguimiento al Mapa de Riesgos Institucional (copia magnética) a la Dirección de Tecnologías de la Información y las Comunicaciones para la publicación en la Intranet y página WEB.		**Observación** La publicación del seguimiento a los riesgos de corrupción se debe realizar (cuatrimestral) dentro de los diez (10) primeros días de los meses de mayo, septiembre y enero.
49	Responsables de procesos y Equipo de Gestores	Analiza el informe toma decisiones así: • Cuando se mitiga el riesgo el proceso del responsable determinará su inclusión o no en el siguiente período. • Cuando se materialicen los riesgos de gestión y seguridad de la información, el proceso debe realizar análisis de las causas que dieron origen a esos eventos y definir las acciones que se incluirán en plan de mejoramiento, con el fin de que se tomen las medidas oportunas y eficaces para evitar la posible repetición del evento. Socializa informe a las dependencias que hacen parte del proceso.	Acta de Equipo de Gestores (PGD-07)	**Observación:** El acta deberá remitirse a la OCI.
50	Profesional Oficina Asesora Jurídica (Secretario del Comité de Conciliación)	Revisa el informe de seguimiento al Mapa de Riesgos que elabora la oficina de Control Interno y lo toma como insumo para el estudio que realiza el Comité de Conciliación sobre las políticas del daño antijurídico de la entidad.		**Observación:** Las directrices del Comité de Conciliación se comunican a través de la Oficina Asesora Jurídica.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		Revisa el seguimiento al Mapa de Riesgos Institucional (riesgo antijurídico) y verifica que las políticas de prevención del daño antijurídico se encuentren reflejadas en el mapa de riesgos a cargo de las dependencias competentes. Presenta los resultados junto con el informe y su anexo ante el Comité de Conciliación para que imparta las instrucciones a que haya lugar.		
51	Director de Tecnologías de la Información y las Comunicaciones y/o responsable de seguridad de la información.	Revisa el seguimiento al Mapa de Riesgos Institucional (Riesgos de Seguridad de la Información). Presenta los resultados del seguimiento ante el Comité SIGEL o la instancia que haga sus veces, para que imparta las instrucciones a las que haya lugar.		
52	Jefe Oficina de Control Interno (Secretario de Comité Institucional de Coordinación de Control Interno)	Vigila que la atención prestada por la Dirección de Apoyo de la entidad respecto de las peticiones, quejas y reclamos estén acordes con la normativa vigente y rendirá un informe semestral sobre el asunto. Presenta el Informe Ejecutivo sobre el Seguimiento al Mapa de Riesgos Institucional, ante el Comité Institucional de Coordinación de Control Interno.	Acta Comité Institucional de Coordinación de Control Interno (PGD-07)	**Observación:** La Oficina de Control Interno en desarrollo del artículo 76 de la ley 1474 y el artículo 2.1.4.6 del Decreto 124 de 2016, deberá realizar el seguimiento cuatrimestral al Plan Anticorrupción y de Atención al Ciudadano.

6. FORMATOS Y OTROS DOCUMENTOS RELACIONADOS AL PROCEDIMIENTO

PDE-07-01. Mapa de Riesgos Institucional.

PDE-07-02. Identificación, análisis y valoración de los riesgos institucionales.

7. CONTROL DE CAMBIOS:

Versión	R.R. No. y Fecha	Descripción de la Modificación[5]
1.0	R.R. 02 09 mayo 2013	Si requiere ver la trazabilidad consultar la Resolución Reglamentaria.
2.0	R.R. 011 25 abril 2016	Si requiere ver la trazabilidad consultar la Resolución Reglamentaria.
3.0	R.R. 038 19 diciembre 2017	El procedimiento cambia de versión 3.0 a 4.0. En la descripción de procedimiento se ajustaron las actividades, con el fin de crear el enlace entre el contexto de la organización - DOFA. Así mismo, se modificaron las observaciones y puntos de control. Así mismo se parametrizó la forma de determinar el riesgos residual, luego de tomar medidas de control, a través de la implementación de un punto de control que asegure el cálculo para el riesgo residual, el cual se tomará en valores absolutos, es decir no puede generar valores negativos ni cero, tal como lo establece la Metodología del DAFP.
4.0	R.R 018 07 marzo 2018	Se ajusta todo el procedimiento teniendo en cuenta la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas expedida por el Departamento Administrativo de la Función Pública – DAFP, se aclara que los términos de seguridad digital y activos de seguridad digital utilizados en la mencionada guía, son sustituidos en el actual procedimiento por las palabras de *seguridad de la información y activos de información* respectivamente, con el objeto de unificar terminología en la entidad con respecto al Subsistema de Gestión de Seguridad de la Información.

[5] Mantener la descripción de las ultimas 2 versiones y registrar la nueva de manera resumida, si existen más de tres (3) versiones indicar que puede consultar el acto administrativo por el cual se aprobó.

Versión	R.R. No. y Fecha	Descripción de la Modificación[5]
5.0	R.R.008 14 febrero 2019	El procedimiento se modificó en los siguientes aspectos: Se ajustó la base legal, incorporando la Constitución Política de Colombia, Decreto Ley 403 de 2020, Ley 1715 de 2014, Decreto 1081 de 2015, Decreto 1083 de 2015, Decreto 648 de 2017, Decreto 1499 de 2017 y se eliminó el Decreto 943 de 2014. [6] Se ajustaron las definiciones básicas referentes a términos relacionados con temas de administración del riesgo. En la descripción del procedimiento se ajustaron las actividades relacionadas con la identificación, análisis, evaluación y valoración de los riesgos institucionales (Gestión, Corrupción y Seguridad de la Información), puntos de control y observaciones, de conformidad con los nuevos lineamientos establecidos en la Guía para la administración del riesgos y diseño de controles en entidades públicas del DAFP, versión 5.0, emitidos por el Departamento Administrativo de la Función Pública – DAFP. Así mismo, se integraron y ajustaron los elementos de los anexos 1 y 2 en el formato PDE-07-01 “Mapa de Riesgos Institucional y se modificó el nombre y contenido del Anexo No. 2 por PDE-07-02 “*Identificación, Análisis y Valoración de los Riesgos Institucionales”.*
6.0	R.R. 031 06 diciembre 2021	

[6] Derogado por el Decreto 1083 de 2015, Sector de Función Pública.