Resolución Reglamentaria Número 008
(Febrero 14 de 2019)

"Por la cual se adopta la nueva versión del Procedimiento para la Administración Integral de los Riesgos Institucionales y se dictan otras disposiciones"

EL CONTRALOR DE BOGOTÁ, D.C.
En ejercicio de sus atribuciones constitucionales y legales y en especial las conferidas en el Acuerdo 658 de 2016, modificado parcialmente por el Acuerdo 664 de 2017, expedidos por el Concejo de Bogotá D.C. y

CONSIDERANDO:

Que de conformidad con el artículo 269 de la Constitución Política de Colombia, es obligación de las autoridades públicas, diseñar y aplicar en las entidades públicas, métodos y procedimientos de control interno, según la naturaleza de sus funciones, de conformidad con lo que disponga la ley.

Que de conformidad con los literales b) y l) del artículo 4 de la Ley 87 de 1993 *"Por la cual se establecen normas para el ejercicio de control interno en las entidades y organismos del Estado y se dictan otras disposiciones",* se deben implementar como elementos del sistema de control interno institucional la definición de políticas como guías de acción y procedimientos para la ejecución de procesos, así como, la simplificación y actualización de normas y procedimientos.

Que mediante Resolución Reglamentaria No.038 del 8 de octubre de 2018, se adoptó la nueva versión del Modelo Estándar de Control Interno – MECI, en la Contraloría de Bogotá D.C., de conformidad al Decreto 1499 de 2017, modificatorio del Decreto 1083 de 2015 -Decreto Único Reglamentario del Sector de la Función Pública-, con el fin de incorporar la estructura definida en la Dimensión No. 7ª - Control Interno del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG.

Que el Concejo de Bogotá D.C. expidió el Acuerdo 658 de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., estableciendo en el artículo 6º que: *"En ejercicio de su autonomía administrativa le corresponde a la Contraloría de Bogotá, D.C., definir todos los aspectos relacionados con el cumplimiento de sus funciones en armonía con los principios consagrados en la Constitución, las leyes y en este Acuerdo".*

Que el numeral 9º del artículo 38 del precitado Acuerdo, establece como una de las funciones de la Dirección de Planeación: *"Realizar estudios, propuestas e investigaciones de carácter técnico sobre desarrollo administrativo, métodos de trabajo, simplificación, agilización y modernización de trámites y procedimientos y demás asuntos relacionados con la organización, tendientes al mejoramiento de la gestión y de los demás sistemas implementados en la Entidad."*

Que el 11 de diciembre de 2013 fue publicada la Norma NTC ISO 27001:2013, la cual establece los requisitos Sistema de Gestión de la Seguridad de la Información.

Que el 15 de diciembre de 2015 fue publicada la NTC - ISO 9000:2015, la cual establece los fundamentos y vocabulario del Sistema de Gestión de la Calidad.

Que el 23 de septiembre de 2015 fueron publicadas las normas NTC-ISO 9001:2015 y NTC-ISO 14001:2015; las cuales establecen los requisitos del Sistema de Gestión de la Calidad y del Sistema de Gestión Ambiental respectivamente.

Que mediante Decreto 1072 del 26 de mayo de 2015, se expidió el Decreto Único Reglamentario del Sector Trabajo, Libro 2, Parte 2, Titulo 4, Capítulo 6, Sistema de Gestión de la Seguridad y Salud en el Trabajo, relacionado con la Gestión de Seguridad y Salud en el Trabajo – SST Resolución 1111 del 27 de marzo de 2017, *"Por la cual se definen los Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo para empleadores y contratantes".*

Que el Presidente de la República expidió el Decreto 1499 del 11 de septiembre de 2017. *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".*

Que el artículo 2.2.22.3.4 *"Ámbito de Aplicación"* del citado decreto, establece que *"El Modelo Integrado de Planeación y Gestión – MIPG se adoptará por los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público. En el caso de las entidades descentralizadas con capital público y privado, el Modelo aplicará en aquellas en que el Estado posea el 90% o más del capital social".*

Que el artículo 2.2.23.2 del citado Decreto, determina que la actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5 de la Ley 87 de 1993".

Que mediante el Decreto 1008 del 14 de junio de 2018, 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"* y establece, la seguridad de la información como uno de los habilitadores transversales.

Que mediante Resolución Reglamentaria No. 018 del 7 de marzo de 2018, se adoptó la versión 4.0 del Procedimiento para elaborar el mapa de riesgos institucional, el cual debe ser actualizado, en el sentido de ajustar su denominación de *"Procedimiento para elaborar el mapa de riesgos institucional "* a *"Procedimiento para la Administración Integral de los Riesgos Institucionales",* en aplicación a los requerimientos de la Nueva Guía expedida por el Departamento Administrativo de la Función Pública

Que en cumplimiento del Decreto 1078 de 2015 subrogado con Decreto 1008 de 2018, la Contraloría de Bogotá debe implementar el Subsistema de Seguridad de la Información SGSI, en el cual se debe aplicar controles de seguridad de la información de conformidad a los lineamientos del Modelo de Seguridad y Privacidad de la Información del MINTIC basado en la Norma ISO 27001:2013.

Que teniendo en cuenta el concepto de mejora, es necesario ajustar el procedimiento para elaborar el mapa de riesgos institucional, con el fin de incorporar los cambios aprobados en cumplimiento de la normatividad vigente.

RESUELVE:

ARTÍCULO PRIMERO. Ajustar el nombre del Procedimiento para Elaborar el Mapa de Riesgos Institucional por "Procedimiento para la Administración Integral de los Riesgos Institucionales".

ARTÍCULO SEGUNDO. Adoptar la nueva versión del siguiente documento del Sistema Integrado de Gestión - SIG:

No.	Documento	Código	Versión
1	Procedimiento para la Administración Integral de los Riesgos Institucionales	PDE-07	5.0

ARTÍCULO TERCERO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes, velar por la administración y divulgación de los documentos adoptados.

ARTÍCULO CUARTO. La presente resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias, en especial el numeral 9º del artículo segundo de la Resolución Reglamentaria No. 018 del 07 de marzo de 2018.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los catorce (14) días del mes de febrero de dos mil diecinueve (2019).

JUAN CARLOS GRANADOS BECERRA
Contralor de Bogotá D.C.

	Aprobación	Revisión Técnica
Firma:		
Nombre:	MARÍA ANAYME BARÓN DURÁN	MERCEDES YUNDA MONROY
Cargo:	Contralora Auxiliar	Directora Técnica
Dependencia:	Despacho Contralora Auxiliar	Dirección Técnica de Planeación
R.R. N°	**008** **Fecha febrero 14 de 2019**	

1. OBJETIVO:

Establecer las actividades necesarias para la Administración del Riesgo en la Contraloría de Bogotá D.C., que determinan la formulación, monitoreo, revisión y seguimiento al Mapa de Riesgos Institucional, constituyéndose en una herramienta que oriente las acciones necesarias para mitigar los riesgos frente a situaciones que puedan afectar el cumplimiento de su misión, objetivos institucionales, objetivos del proceso o la satisfacción del cliente.

2. ALCANCE:

Este procedimiento inicia cuando el Contralor Auxiliar – Dirección de Planeación, elabora la Política de Administración de Riesgos en coordinación con todas las dependencias de la entidad y termina cuando el Jefe de la Oficina de Control Interno presenta al Comité Institucional de Coordinación de Control Interno el Informe Ejecutivo sobre el seguimiento al Mapa de Riesgos de Gestión y Corrupción y Mapa de Riesgos de Seguridad de la Información, según programación de reuniones de este Comité.

3. BASE LEGAL:

Tipo de norma	Fecha	Descripción
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.
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.
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 943	21-may-2014	Por medio del cual se actualiza el Modelo Estándar de Control Interno– MECI.
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 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 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.

Tipo de norma	Fecha	Descripción
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 funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Acuerdo 664	26-jun-2017	Por el cual se modifica parcialmente el acuerdo 658 del 21 de diciembre del 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 funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Norma NTC-ISO 27001:2013	11-dic-2013	Norma Internacional - Requisitos del Sistema de Gestión de la Seguridad de la Información.
Norma NTC-ISO 9001:2015	23-sep-2015	Norma Internacional - Requisitos del Sistema de Gestión de la Calidad.
Norma NTC-ISO 14001:2015	23-sep-2015	Norma Internacional - Requisitos del Sistema de Gestión de Gestión Ambiental.
Norma NTC - ISO 9000:2015	15-oct-2015	Norma Internacional, Sistema de Gestión de la Calidad – Fundamentos y Vocabulario.

4. DEFINICIONES:

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

ACTIVO DE INFORMACIÓN: Son elementos tales como aplicaciones de la organización, servicios web, redes, software, servicios, hardware, información física o digital, recurso humano, procesos, procedimientos, oficinas e instalaciones asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad. Es una pieza de información definible e identificable, almacenada en cualquier medio.
Las Características de los activos de la información: Un activo de información puede tener las siguientes características, independiente del tipo de activo:

- El activo de información es reconocido como valioso
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o combinación de los mismos.
- Forma parte de la identidad de la entidad y sin la cual la Contraloría de Bogotá puede estar en algún nivel de riesgo.

ADMINISTRACIÓN DE RIESGOS: 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación[1], teniendo en cuenta los siguientes aspectos:

- **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.

- **Establecimiento del Contexto:** definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y el establecimiento del alcance y los criterios del riesgo para la política para la gestión de riesgo

- **Contexto Externo:** ambiente externo en el cual la organización busca alcanzar sus objetivos
- **Contexto Interno:** ambiente interno en el cual la organización busca alcanzar sus objetivos (NTC-ISO 31000)

- **Identificación de Riesgos:** proceso para encontrar, reconocer y describir el riesgo (NTC-ISO 31000)

- **Análisis de Riesgo:** proceso para comprender la naturaleza del riesgo (NTC-ISO 31000)

- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo, ésta puede ser medidas con criterios de frecuencia o factibilidad (Guía DAFP)

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

- **Calificación del Riesgo.** se logra a través de la estimación de la probabilidad de su ocurrencia (número de veces que se ha presentado el riesgo) y el impacto que puede causar la materialización del riesgo (magnitud de sus efectos).

- **Control**: medida que modifica al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones)

- **Valoración del Riesgo:** proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo

AMENAZAS: causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

APETITO AL RIESGO: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

[1] Intosai: guía para las normas de control interno del sector público http://www.Intosai.org

AUTOEVALUACIÓN DEL CONTROL: elemento de Control que basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.

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

COMPARTIR EL RIESGO: se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

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**.**

CONFIDENCIALIDAD: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

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.

DOCUMENTOS DE APOYO: son una serie de documentos que se han recogido y dan apoyo con su contenido a las tareas administrativas.

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

EVALUACIÓN DEL RIESGO: Proceso de comparación de los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo, magnitud o ambos son aceptables o tolerables.

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.

EVITAR EL RIESGO: tomar las medidas encaminadas a prevenir su materialización.

FACTORES DE RIESGO: manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos.

FRECUENCIA: medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

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[2]
Por otra parte, la Ley 1712 de 2014, artículo 6, la define como: "un 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[3]. 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[4].

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[5]

INTEGRIDAD: propiedad de exactitud y completitud

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

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

GESTOR DE PROCESO: funcionario de las dependencias que conforman el equipo multidisciplinario de gestores del proceso, con el propósito de contribuir al logro de los objetivos institucionales.

MAPA DE RIESGOS: documento con la información resultante de la gestión del riesgo

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

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

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 y a los cuales se les ha formulado acciones para mitigarlos, reducirlos o eliminarlos, se toma como un solo documento los riesgos de Corrupción, de Gestión y de Seguridad de la información.

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.

NATURALEZA DE LOS CONTROLES: según la naturaleza de los controles, se clasifican en:

- ***Preventivos.*** Se orientan a eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- ***Detectivos.*** Aquellos que registran un evento después de presentado; sirven para descubrir resultados no previstos y alertar la presencia de un riesgo.
- ***Correctivos.*** Aquellos que permiten, después de ser detectado el evento no deseado, el restablecimiento de la actividad.

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 del riesgo, (NTC ISO31000 Numeral 2.4). La gestión o Administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos**.**

PROCESO DE ADMINISTRACIÓN DE RIESGO: aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la Administración del Riesgo.

REDUCCIÓN DEL RIESGO: aplicación de controles para reducir las probabilidades de ocurrencia de un evento.

RIESGO: Efecto de la incertidumbre sobre los objetivos, se clasifica en los siguientes tipos

1). Estratégico.

2). Imagen.
3). Operativos.
4). Financieros.
5). Cumplimiento.
6). Tecnología.
7). Antijurídico.
8). Corrupción.
9). Seguridad de la información
10). Otros riesgos.

Estos riesgos se definen a continuación:

- **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

- **Riesgos de Imagen.** están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

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

- **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.

- **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 de Tecnología.** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad

- **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 Corrupción.** "La posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular"[6]. Es necesario que en la descripción del riesgo concurran los siguientes componentes:

[6] Presidencia de la República, Departamento Nacional de Planeación, Departamento Administrativo de la Función Pública. Estrategias para la construcción del plan anticorrupción y de atención al ciudadano. Bogotá. 2012. P.9

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado

- **Riesgo de Seguridad de la información**: combinación de amenazas y vulnerabilidades en el entorno seguridad de la información. Puede debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

RIESGO 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. Estos riesgos agrupan los enunciados en la tipología excepto los de corrupción y Seguridad de la información.

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 del riesgo.

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

TRATAMIENTO DEL RIESGO

Aceptar riesgo: No se adopta ninguna medida o control.
Evitar riesgo: Se abandonan las actividades que dan lugar al riesgo, y se decide no iniciar o no continuar con la actividad que causa el riesgo.
Compartir riesgo: Se transfiere o comparte el riesgo.
Reducir/mitigar/tratar el riesgo: Esto conlleva a la implementación de controles.

VULNERABILIDAD: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
5.1. Elaboración y aprobación de la Política administración de riesgos				
1	Contralor Auxiliar Dirección de planeación (Proceso de Direccionamiento Estratégico)	Elabora la Política de Administración de riesgos en coordinación con todas las dependencias de la entidad.		**Punto de Control:** La política de administración de riegos debe contener los lineamientos establecidos en la metodología vigente diseñada por el DAFP que incluye la gestión de riesgos de seguridad de la información.
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. Acta de aprobación de comité institucional de coordinación de control interno. Registros de socialización.	
5.2 Identificación del riesgo				
1	Contralor, Contralor Auxiliar, Director, Subdirector, Jefe de Oficina (Responsable de procesos)	Convoca a reunión al equipo de gestores y facilitadores del proceso 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

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
				proceso.
2	Director, Subdirector, Gerente, Asesor o profesional, (Gestores de procesos)	**Identificación riesgos de Gestión y Corrupción.** Diligencia Anexo 1 Mapa de Riesgos de Gestión y Corrupción teniendo en cuenta los siguientes insumos: ➢ Plan Estratégico de la entidad. ➢ Política de administración del riesgo definida por la Alta Dirección. ➢ Caracterización del proceso. ➢ Contexto interno, externo y del proceso. (Diagnostico DOFA que principalmente analiza los factores generadores de riesgos como son las debilidades y amenazas). ➢ Lineamientos de los riesgos antijurídicos determinados por el Comité de Conciliación de la entidad. Establece las causas o las circunstancias generadoras del riesgo, con base en el análisis del contexto estratégico de la organización y sus procesos (Externo,	Anexo 1: Mapa de Riesgos de Gestión y Corrupción	**Punto de Control.** Los componentes identificados en el resultado de la matriz DOFA (Debilidades y Amenazas) ponderadas como alta se deben llevar al mapa de riesgos. En la Divulgación del Plan Anticorrupción preliminar el componente 1 riesgos de corrupción estará disponible para que los contratistas, funcionarios o partes interesadas conozcan, debatan y formulen sus apreciaciones. Para la identificación del riesgo Antijurídico tener en cuenta los lineamientos vigentes de la Agencia Nacional de Defensa Jurídica del Estado. **Observación** Se debe asegurar el ejercicio participativo

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		Interno y del Proceso). Redacta el riesgo orientado a la posibilidad de ocurrencia de un evento que pueda afectar el logro de los objetivos y el desarrollo de las funciones de la entidad a partir del levantamiento de causas o las circunstancias generadoras del riesgo. Diligencia el anexo 1.1 Matriz de Definición de Riesgos de Corrupción, si todas las casillas son contestadas afirmativamente, se trata de un riesgo de corrupción el cual tendrá un tratamiento especial para su valoración y publicación. Identifica el tipo de riesgo y determina las consecuencias potenciales de los riesgos en el evento de producirse.		que incluya todos los niveles de la dependencia. Para los riesgos generales de Seguridad y salud en el trabajo se tendrán en cuenta el procedimiento para la identificación de peligros, valoración de riesgos y determinación de controles. Preguntas clave para la identificación del riesgo: ¿Qué, Cómo, Cuándo puede suceder? ¿Qué consecuencias tendría su materialización? Evitar iniciar con palabras negativas como: “No…” “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en…”

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
3	Director, Subdirector, Gerente, Asesor o profesional, (Gestores de procesos)	**Identificación riesgos de Seguridad de la información** Diligencia anexo 2 Riesgos de Seguridad de la información teniendo en cuenta los siguientes insumos: Política de administración del riesgo definida por la Alta Dirección. ➢ Contexto interno, externo y del proceso. (Diagnostico DOFA que principalmente analiza los factores generadores de riesgos como son las debilidades y amenazas). ➢ *Registro de activos de información del proceso* Identifica en el formato "PGD-08-01 *Registro de Activos de Información"* publicado en la página WEB de la entidad, los activos de información del proceso que se encuentran con criticidad **ALTA** (campos 4,6, 20). Agrupa activos de información del mismo tipo (Campo 6), y analiza conjuntamente las amenazas y vulnerabilidades que sean comunes y que podrían causar su materialización. Identifica la criticidad en cuanto a integridad, disponibilidad o confidencialidad (campos 17,	Anexo No 2 Mapa de Riesgos de Seguridad de la Información.	**Punto de control** 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 para el proceso. **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.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		18,19) de los activos de información seleccionados. Redacta el riesgo orientado a la posibilidad de ocurrencia de un evento teniendo en cuenta la selección anterior: ✓ Pérdida de confidencialidad ✓ Pérdida de la integridad ✓ Pérdida de la disponibilidad ✓ Establece la amenaza que pueden materializar el riesgo, Tabla 1 - Guía de amenazas comunes, según la criticidad identificada. Establece las vulnerabilidades asociadas a la amenaza identificada, a partir del tipo de activo de información. Tabla 2 Guía de vulnerabilidades comunes. En caso de no encontrar la información requerida en las tablas 1 y 2 redacte la vulnerabilidad y amenaza. Determina las consecuencias que puedan enfrentar la entidad o el proceso a causa de la materialización del riesgo.		

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
5.3 Valoración del Riesgo:				
1	Director, Subdirector, Gerente, Asesor o profesional, (Gestores de procesos)	**Análisis de riesgos** Realiza el análisis de los riesgos, con el fin de determinar el riesgo inherente, teniendo en cuenta las orientaciones dadas en las tablas para calificar la probabilidad y el impacto. • **Probabilidad**. Califique según parámetros establecidos en la Tabla No.3 criterios para calificar la probabilidad. El nivel de probabilidad oscila entre 1 y 5. (Aplica para todo tipo de riesgo). • **Impacto.** Califique según parámetros establecidos en: RIESGOS DE GESTIÓN: Tabla No. 4 criterios para calificar el impacto. El nivel va desde insignificante con un valor de impacto 1 hasta catastrófico con un valor de impacto 5. RIESGOS DE CORRUPCIÓN: Tabla No 5 criterios para calificar el impacto, en la cual 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	Anexo 1: Mapa de Riesgos de Gestión y Corrupción Anexo 2: Mapa de Riesgos de Seguridad de la Información.	**Punto de Control** Asegura que el cálculo para el riesgo residual se tome en valores absolutos, es decir no puede generar valores negativos ni cero.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		catastrófico según el caso, si la respuesta a la pregunta 16 es afirmativa el riesgo se considera catastrófico. <u>RIESGOS DE SEGURIDAD DE LA INFORMACIÓN:</u> Tabla No. 6 criterios para calificar el impacto Riesgos de seguridad de la información. La calificación de los riesgos de Seguridad de la información va desde insignificante con un valor de impacto 1 hasta catastrófico con un valor de impacto 5. Relacione la calificación de probabilidad e impacto para cada riesgo en el mapa de riesgo correspondiente. La zona de riesgo se calcula automáticamente de acuerdo con la calificación de probabilidad e impacto establecidos.		Para los riesgos de seguridad de la información, la probabilidad y el impacto se determinan con base a la amenaza, no en la vulnerabilidad. Para calificar el impacto de los riesgos de seguridad de la información según los criterios de la tabla No. 6 califíquelo de acuerdo al mayor grado de afectación en cuanto a integridad, disponibilidad y confiabilidad.
2	Director, Subdirector, Gerente, Asesor o profesional, (Gestores de procesos)	**Evaluación de riesgos** Realice la Evaluación de riesgos con el fin de determinar el riesgo residual, comparando los resultados del análisis de riesgos inherentes con los controles establecidos, así: ➢ Determine el tipo de control según parámetros establecidos en: <u>RIESGOS DE GESTIÓN Y CORRUPCIÓN</u>*:* Tabla No 8 tipos de control.		**Punto de control** Seleccione actividades de control preventivas y detectivas que ayuden a la mitigación de las causas que originan los riesgos. Para cada causa debe existir un control, un control puede ser tan eficiente que me ayude a mitigar

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Tabla No. 9 Controles Seguridad de información, si presenta controles diferentes a los relacionados en esta tabla agréguelo siempre y cuando sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo. PARA TODOS LOS RIESGOS ➢ Evalúe y califique el diseño del control de acuerdo con los puntajes establecidos en las Tabla No. 10 *"Peso o participación de cada variable en el diseño del control para mitigación del riesgo* y Tabla No. 11 "*Calificación del diseño del control"* (aplica para todos los riesgos). Califique según puntaje de referencia. ➢ Evalué y califique la ejecución del control. Según tabla No 12. *calificación de ejecución del control.* ➢ Evalué la solidez individual de cada control, tabla No 13 *"calificación solidez individual del control".* ➢ Evalué 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		varias causas, en estos casos se repite el control, asociado de manera independiente a la causa especifica. Las causas se deben trabajar de manera separada (en diferente renglón). Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo. 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 Para determinar el riesgo residual en los riesgos de corrupción únicamente disminuye en probabilidad. **Observaciones** La redacción del propósito del control debe tener verbos rectores como (verificar, validar,

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		puntaje en tabla No 14. *"Calificación de la solidez del conjunto de controles*". ➢ Determine la nueva calificación de probabilidad o impacto de acuerdo con el puntaje total de los controles y atendiendo lo establecido en la Tabla No. 15. *"Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos".* Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, se procede a la elaboración del riesgo residual. La zona de riesgo residual se calcula automáticamente de acuerdo con los resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos. Determine la medida de tratamiento para aplicar al riesgo según tabla No. 7 ✓ Aceptar riesgo, (no aplica para riesgos de corrupción) ✓ Evitar riesgo ✓ Compartir riesgo (para riesgos de corrupción, se pueden compartir pero no se puede transferir su responsabilidad). ✓ Reducir riesgo		conciliar, comparar, revisar, cotejar, etc). La columna correspondiente a la zona de riesgo residual se calcula automáticamente.
3	Director, Subdirector, Gerente, Asesor o profesional,	Establece la(s) acción(es) asociadas al control que mitigan o reducen cada		**Punto de control:** Verifica que las acciones formuladas

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
	(Gestores de procesos)	riesgo, determinando el periodo de ejecución, indicador, área responsable y registro que evidencie el cumplimiento de la acción.		estén orientadas a reducir o eliminar las causas identificadas.
4	Director, Subdirector, Gerente, Asesor o profesional, (Gestores de procesos)	Diligencia la fecha de aprobación en el Anexo 1 Mapa de Riesgos de Gestión y Corrupción y en el anexo 2 Mapa de Riesgos de Seguridad de la Información. Remite los anexos al responsable de proceso, junto con las tablas de análisis, valoración de controles y valoración de riesgos.		**Observación:** El Anexo 1, está debidamente formulado y no se requiere información adicional.
5	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Responsable de Proceso)	Aprueba la información contenida en los Anexos 1 y 2 correspondiente al proceso. Remite en medio magnético vía SIGESPRO o Outlook a la Dirección de Planeación los anexos 1 y 2 junto con las tablas de análisis, valoración de controles y valoración de riesgos.	Anexo 1 Mapa de Riesgos de Gestión y Corrupción. Anexo 2: Mapa de Riesgos de Seguridad de la Información	**Punto de Control:** Verifica que los anexos se hayan diligenciado de conformidad con lo establecido en los anexos correspondientes. Para el envío de los anexos, se tendrá en cuenta la Circular Periodicidad reporte de Información.
6	Profesional Dirección de Planeación	Revisa técnicamente los documentos y los anexos del Mapa de Riesgos Institucional. En conjunto con la Dirección de Tecnologías de la Información y las comunicaciones y la Dirección Administrativa y Financiera - Proceso de Gestión Documental, se revisa		**Observaciones:** El Mapa de Riesgos de Corrupción hace parte del Plan Anticorrupción y de Atención al Ciudadano.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		técnicamente el anexo de riesgos de seguridad de la información. Presenta al Director de Planeación las observaciones, en caso de ser necesario, quien informará al responsable de proceso para los ajustes correspondientes. Regresa actividad No. 1. Consolida el Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información con base en el reporte de riesgos remitidos por los responsables de procesos.		
7	Director Técnico de Planeación	Presenta ante el Comité Directivo el Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información para su conocimiento y aprobación.		
8	Contralor (Comité Directivo)	Aprueba el Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información.	Acta de Comité Directivo	**Punto de Control:** Verifica que dentro del acta quede consignado la aprobación del Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información.
9	Profesional, Técnico Dirección de Planeación	Extrae del Anexo 1, los riesgos de corrupción, como componente del Plan Anticorrupción y atención al ciudadano.		

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
10	Profesional, técnico Dirección de Planeación	Publica Mapa de Riesgos de Gestión y Corrupción y Mapa de Riesgos de Seguridad de la Información en la Intranet y Pagina WEB de la entidad, a más tardar el 31 de enero de cada vigencia.		
5.4. Revisión Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información (Responsable de Proceso)				
1	Contralor Auxiliar, Director, Jefe Oficina (Responsable de Proceso)	Identifica la necesidad de modificar el Mapa de Riesgos del proceso. Diligencia y remite solicitud de modificación debidamente sustentada a la Dirección de Planeación, junto con la actualización de los anexos respectivos.	Solicitud de creación, actualización o eliminación de información documentada del SIG	**Observación** Anexo 1 del Procedimiento para mantener la información documentada del SIG. Las solicitudes de modificación deben efectuarse previo al vencimiento de las acciones
2	Profesional Dirección de Planeación	Revisa técnicamente los documentos contentivos de 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.		Observación Si la solicitud de modificación contempla riesgos de seguridad de la información, revisa en conjunto con la Dirección de Tecnologías de la Información y las comunicaciones y la Dirección Administrativa y Financiera - proceso de gestión documental.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
3	Director Técnico de Planeación	Presenta al Contralor Auxiliar la solicitud de modificación del Mapa de Riesgos Institucional para su aprobación.		**Punto de Control:** Asegura que las modificaciones a los riesgos contemplen los parámetros establecidos en los anexos de este procedimiento.
4	Contralor Auxiliar	Analiza y aprueba las solicitudes de modificación y las remite a la Dirección de Planeación.	Comunicación oficial Interna	
5	Profesional, Técnico Dirección de Planeación	Actualiza la versión del Mapa de Riesgos de Gestión y Corrupción o el Mapa de Riesgos de Seguridad de la Información según sea el caso, con las solicitudes de modificación aprobadas, en el evento de no ser aprobada se comunica al proceso respectivo.	Anexo 1: Mapa de Riesgos de Gestión y Corrupción. Anexo 2: Mapa de Riesgos de Seguridad de la Información.	
5.5. Monitoreo Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información (Responsable de Proceso)				
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina. (Responsable de Proceso)	Realiza monitoreo y revisión al Mapa de Riesgos del proceso.		**Observación** El monitoreo y revisión se debe plasmar en los Anexos 1 y 2 según corresponda el caso.
2	Contralor Auxiliar, Director, Jefe Oficina (Responsable de Proceso)	Remite a la Oficina de Control Interno el monitoreo y revisión realizada al Mapa de Riesgos del proceso (medio magnético), dentro de los términos establecidos en la Circular de reporte de información vigente.	Anexo 1: Mapa de Riesgos de Gestión y Corrupción (Monitoreo y revisión) Anexo 2: Mapa de Riesgos de Seguridad de	

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
			la Información (Monitoreo y revisión)	
5.6 Seguimiento Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la información, Oficina de Control Interno – OCI				
1	Profesional Oficina de Control Interno	Planifica el seguimiento al Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información 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.
2	Jefe Oficina de Control Interno	Comisiona los auditores de la Oficina de Control Interno para realizar seguimiento al Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información.		
3	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.	Comunicación oficial Interna	
4	Profesional Oficina de Control Interno	Realiza seguimiento al Mapa de Riesgos, utilizando el Anexo 1 Mapa de Riesgos de Gestión y Corrupción y Anexo 2 Mapa de Riesgos de Seguridad de la Información y determina el Estado de los Riesgos, así: • Abierto: El riesgo continúa para seguimiento. • Mitigado: el riesgo se		**Punto de control** Verifica la inclusión de la totalidad de los riesgos y que el cumplimiento de las acciones esté soportado en los documentos que evidencien su ejecución y que se hayan realizado dentro de los términos establecidos.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		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.		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.
5	Profesional Oficina de Control Interno	Elabora informe de seguimiento al Mapa de Riesgos de Gestión y Corrupción y el Mapa de Riesgos de Seguridad de la Información presenta para aprobación al Jefe de la Oficina de Control Interno.		**Observación**: Este 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.

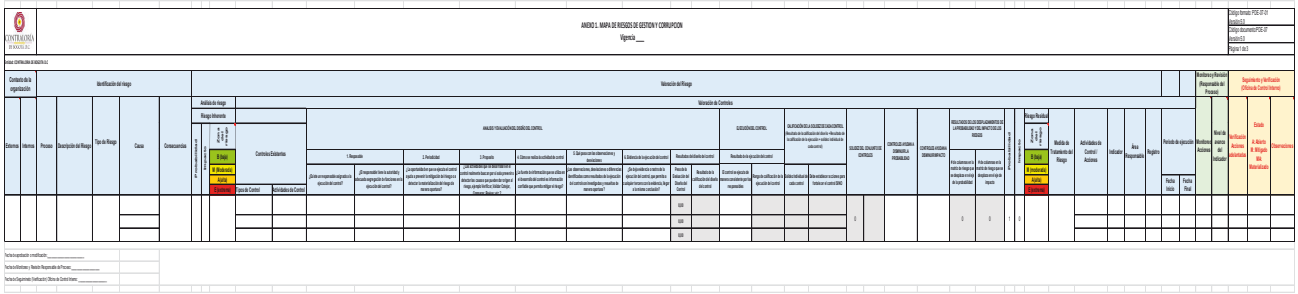
No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
6	Jefe Oficina de Control Interno	Aprueba el Informe de Seguimiento al Mapa de Riesgos Institucional. Remite el resultado del seguimiento a los responsables de cada proceso.	Informe de Seguimiento al Mapa de Riesgos de Gestión y Corrupción y el de Riesgos de Seguridad de la información Memorando Interno.	**Punto de control.** Verifica que el seguimiento sea coherente con la verificación realizada en los Anexos 1 y 2 del presente procedimiento. Verifica que las políticas de prevención del daño antijurídico se encuentren reflejadas en el Mapa de riesgos a cargo de las dependencias competentes.
7	Jefe Oficina de Control Interno	Envía seguimiento al Mapa de Riesgos de Gestión y Corrupción y Mapa de Riesgos de Seguridad de la Información (copia magnética) a la Dirección de Tecnologías de la Información y las Comunicaciones para la publicación en la Intranet y página WEB.	Anexo 1: Mapa de Riesgos de Gestión y Corrupción y Anexo 2: Mapa de Riesgos de Seguridad de la Información (Verificación OCI)	**Observación** La publicación del seguimiento a los riesgos de corrupción se debe realizar dentro de los diez (10) primeros días de los meses de mayo, septiembre y enero.
8	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,	Acta de Equipo de Gestores	El acta deberá remitirse a la OCI.

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		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.		
9	Profesional Oficina Asesora Jurídica (Secretario del Comité de Conciliación)	Revisa el seguimiento al Mapa de Riesgos de Gestión y Corrupción (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.		**Observación** Las directrices del Comité de Conciliación se comunican a través de la Oficina asesora Jurídica.
10	Director de Tecnologías de la Información y las Comunicaciones y/o responsable de seguridad de la información.	Revisa el seguimiento al Mapa de Riesgos de Seguridad de la Información. Presenta los resultados en un informe ante el Comité SIGEL o la instancia que haga sus veces, para que imparta las instrucciones a las que haya lugar.		
11	Jefe Oficina de Control Interno (Secretario de	Presenta al Comité Institucional de Coordinación de Control Interno el Informe Ejecutivo sobre el seguimiento al Mapa de Riesgos de	Acta Comité Institucional de Coordinación	**Observación:** La Oficina de Control Interno en desarrollo del artículo 76 de la ley

No	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
	Comité Institucional de Coordinación de Control Interno)	Gestión y Corrupción y Mapa de Riesgos de Seguridad de la Información, según programación de reuniones de este Comité.	de Control Interno	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. ANEXOS:

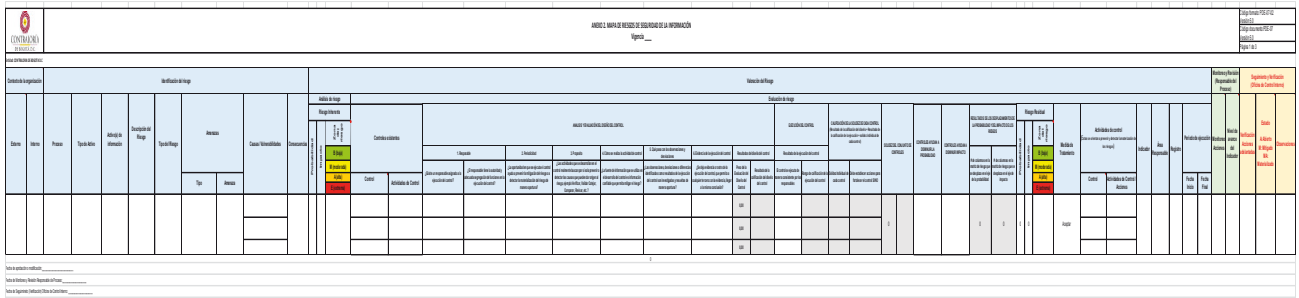
ANEXO No 1: y Corrupción



CONTRALORÍA DE BOGOTÁ, D.C.	ANEXO 1.1. MATRIZ DEFINICIÓN DEL RIESGO DE CORRUPCIÓN Vigencia _____	Código formato: PDE-07-01 Versión 5.0
		Código documento:PDE-07 Versión 5.0
		Página 1 de 3

Descripción del riesgo	Acción u Omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado

ANEXO 2. Mapa de Riesgos de Seguridad de la Información



TABLAS SOPORTES DE LOS ANEXOS

Tabla No 1. Guía de Amenazas Comunes
Fuente: ISO/IEC 27005:2009 Y MINTIC guía de gestión de riesgos

TIPO	AMENAZA
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológico
	Inundación
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de energía
	Falla en equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia
	comprometida
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	Uso no autorizado del equipo /información
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Falsificación de derechos
	Abuso de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Amenazas Humanas: Las amenazas humanas pueden provenir de empleados con o sin intención, proveedores y piratas informáticos, entre otros. Estas presentan una motivación

AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto	Piratería
	Ego	Ingeniería Social
	Rebelión	Intrusión en el sistema
	Estatus	forzados al sistema
	Dinero	Acceso no autorizado
Criminal de la computación	Destrucción información	Crimen por computador
	Divulgación ilegal de la información	Acto fraudulento
	Ganancia monetaria	Soborno de la información
	Alteración autorizada datos	Suplantación de identidad
Terrorismo	Chantaje	Intrusión en el sistema
	Destrucción	Bomba/Terrorismo
	Explotación	Guerra de la información
	Venganza	Ataques contra sistema DDoS
	Ganancia política	Penetración sistema
	Cubrimiento de los medios de comunicación	Manipulación sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva	Ventaja de defensa
	Espionaje económico	Hurto de información
Intrusos (empleados con entrenamiento deficiente,descontentos,malintencionados , negligentes, deshonestos o despedidos)	Curiosidad	Asalto a un empleado
	Ganancia monetaria	Chantaje

Tabla No 2. Guía de Vulnerabilidades Comunes
Fuente: ISO/IEC 27005 Y MINTIC guía de gestión de riesgos

TIPO DE ACTIVO	VULNERABILIDADES
HARDWARE	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (al polvo o la suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
SOFTWARE	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
	Defectos bien conocidos en el software
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Software de distribución amplia
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Configuración incorrecta de parámetros
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlado de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Software obsoleto
	Fallas en la producción de informes de gestión
RED	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de fallas
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
PERSONAL	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
	Procedimientos inadecuados de contratación
	Uso incorrecto de software y hardware
	Ausencia de mecanismos de monitoreo
LUGAR	Uso inadecuado de los controles de acceso al edificio y recintos
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Áreas susceptibles a inundación
	Red energética inestable
	Ausencia de protección física de la edificación (Puertas y ventanas)
ORGANIZACIÓN	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros).
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
	Ausencia de auditorias
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento del servicio
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Ausencia de procedimientos de control de cambios
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información

	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso de correo electrónico
	Ausencia de procedimientos para introducción del software en los sistemas operativos
	Ausencia de registros en bitácoras
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de autorización de los recursos de procesamiento de información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad
	Ausencia de revisiones regulares por parte de la Alta Dirección
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.

TABLA 3.Criterios para Calificar la Probabilidad - APLICA PARA TODO TIPO DE RIESGO

DESCRIPTOR	Descripción	Frecuencia	NIVEL DE LA PROBABILIDAD
Rara vez o raro	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años	1
Improbable	El evento puede ocurrir en algún momento.	Al menos de una vez en los últimos 5 años.	2
Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.	3
Probable	Es viable que el evento emente ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.	4
Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.	5
Nota Aplica para todo tipo de riesgos			

TABLA 4. .Criterios para Calificar el Impacto - NO APLICA CORRUPCIÓN

NIVEL DEL IMPACTO	CRITERIOS PARA CALIFICAR EL IMPACTO	VALOR DEL IMPACTO
CATASTRÓFICO	Interrupción de las operaciones de la Entidad por más de cinco (5) días.	5
	Intervención por parte de un ente de control u otro ente regulador.	
	Pérdida de Información crítica para la entidad que no se puede recuperar	
	Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.	
	Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados	
MAYOR	Interrupción de las operaciones de la Entidad por más de dos (2) días.	4
	Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.	
	Sanción por parte del ente de control u otro ente regulador	
	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno	
	Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.	
MODERADO	Interrupción de las operaciones de la Entidad por un (1) día.	3
	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad	
	Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.	
	Reproceso de actividades y aumento de carga operativa	
	Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos	
	Investigaciones penales, fiscales o disciplinarias	
MENOR	Interrupción de las operaciones de la Entidad por algunas horas.	2
	Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.	
	Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.	
INSIGNIFICANTE	No hay interrupción de las operaciones de la entidad.	1
	No se generan sanciones económicas o administrativas.	
	No se afecta la imagen institucional de forma significativa.	

TABLA No.5. CRITERIOS PARA CALIFICAR EL IMPACTO - RIESGOS DE CORRUPCIÓN

Nº	Pregunta Si el riesgo de corrupción se materializa podría...	Riesgo 1		Riesgo 2	
		Si	NO	Si	NO
1	¿Afectar al grupo de funcionarios del proceso?				
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?				
3	¿Afectar el cumplimiento de misión de la Entidad?				
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?				
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?				
6	¿Generar pérdida de recursos económicos?				
7	¿Afectar la generación de los productos o la prestación de servicios?				
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?				
9	¿Generar pérdida de información de la Entidad?				
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?				
11	¿Dar lugar a procesos sancionatorios?				
12	¿Dar lugar a procesos disciplinarios?				
13	¿Dar lugar a procesos fiscales?				
14	¿Dar lugar a procesos penales?				
15	¿Generar pérdida de credibilidad del sector?				
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?				
17	¿Afectar la imagen regional?				
18	¿Afectar la imagen nacional?				
19	¿Generar daño ambiental?				
TOTAL					
Clasificación del Impacto					

CALIFICACIÓN IMPACTO RIESGO DE CORRUPCIÓN

RESPUESTAS POSITIVAS	DESCRIPCIÓN	PUNTAJE
1 - 5	Moderado	5
6-11	Mayor	10
12-19	Catastrófico	20

TABLA 6. Criterios para Calificar el Impacto - Riesgos de Seguridad Digital

Descriptor	Descripción	calificación riesgos estratégicos
Insignificante	Sin afectación de la integridad de la información Sin afectación de la disponibilidad de la información Sin afectación de la confidencialidad de la información	1
Menor	Afectación leve de la integridad de la información Afectación leve de la disponibilidad de la información Afectación leve de la confidencialidad de la información	2
Moderado	Afectación moderada de la integridad de la información Afectación moderada de la disponibilidad de la información Afectación moderada de la confidencialidad de la información	3
Mayor	Afectación grave de la integridad de la información Afectación grave de la disponibilidad de la información Afectación grave de la confidencialidad de la información	4
Catastrófico	Afectación muy grave de la integridad de la información Afectación muy grave de la disponibilidad de la información Afectación muy grave de la confidencialidad de la información	5

TABLA No.7 Mapa de Calor

ZONA DE RIESGO - NO APLICA RIESGOS DE CORRUPCIÓN

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Rara vez (1)	B	B	M	A	E
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

ZONA DE RIESGO

MEDIDA DE TRATAMIENTO DEL RIESGO

B: Zona de riesgo baja: ACEPTAR EL RIESGO
M: Zona de riesgo moderada: REDUCIR O COMPARTIR O EVITAR EL RIESGO
A: Zona de riesgo Alta:REDUCIR O COMPARTIR O EVITAR EL RIESGO
E: Zona de riesgo extrema: REDUCIR O COMPARTIR O EVITAR EL RIESGO

ZONA DE RIESGO - CORRUPCIÓN

PROBABILIDAD	IMPACTO		
	Moderado (5)	Mayor (10)	Catastrófico (20)
Casi Seguro (5)	E	E	E
Probable (4)	A	E	E
Posible (3)	A	E	E
Improbable (2)	M	A	E
Rara vez (1)	M	A	E

ZONA DE ~~RIESGO~~

MEDIDA DE TRATAMIENTO DEL RIESGO DE CORRUPCIÓN

M: Zona de riesgo moderada: REDUCIR O COMPARTIR O EVITAR EL RIESGO
A: Zona de riesgo Alta: REDUCIR O COMPARTIR O EVITAR EL RIESGO
E: Zona de riesgo extrema: REDUCIR O COMPARTIR O EVITAR EL RIESGO

TABLA No. 8 Tipos de Controles

CONTROLES GENERALES	
GESTIÓN	Políticas claras aplicadas
	Seguimiento al plan estratégico y operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento a cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos
OPERATIVOS	Conciliaciones
	Consecutivos
	Verificación de firmas
	Listas de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal capacitado
	Aseguramiento y calidad
LEGALES	Normas claras y aplicadas

TABLA No. 9 CONTROLES SEGURIDAD DE LA INFORMACIÓN

Controles 27001:2013		
5 Políticas de seguridad	A.5.1 Políticas de seguridad	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
	A.5.2 Revisión de las Políticas de seguridad	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
zación de la seguridad de la	A.6.1.1 Roles y responsabilidades	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	A.6.1.2. Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

TABLA No. 9 CONTROLES SEGURIDAD DE LA INFORMACIÓN

Controles 27001:2013		
	A.6.1.3. Contacto con las autoridades	Control: Se debe mantener los contactos apropiados con las autoridades pertinentes
	A.6.1.4. Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
	A.6.1.5 Seguridad de la información en gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
	A.6.2.1 Política para dispositivos móviles	Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
	A.6.2.2 Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7 Seguridad de los recursos humanos	A.7.1.1 Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
	A.7.1.2 Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
	A.7.2.1 Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
	A.7.2.3 Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados hayan cometido una violación a la seguridad de la información.
	A.7.3.1 Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se debe definir, comunicar al empleado o contratista y hacer cumplir.
A.8 Gestión de activos	A.8.1.1 Inventario de activos	Control: Se debe identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se deber elaborar y mantener un inventario de estos activos.
	A.8.1.2 Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
	A.8.1.3 Uso aceptable de los activos	Control: Se debe identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
	A.8.1.4 Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
	A.8.2.1 Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
	A.8.2.2 Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
	A.8.2.3 Manejo de activos	Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
	A.8.3.1 Gestión de medios removibles	Control: Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
	A.8.3.2 Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
	A.8.3.3 Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9 Control de acceso	A.9.1.1 Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información
	A.9.1.2 Política sobre el uso de los servicios de red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A.9.2.1 Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de usuarios, para posibilitar la asignación de los derechos de acceso.
	A.9.2.2 Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
	A.9.2.3 Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	A.9.2.4 Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal.
	A.9.2.5 Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	A.9.2.6 Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios.
	A.9.3.1 Uso de la información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta
	A.9.4.1 Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se deben restringir de acuerdo con la política de control de acceso.
	A.9.4.2 Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
	A.9.4.3 Sistema de gestión de contraseña	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas
	A.9.4.4 Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
	A.9.4.5 Control de acceso a códigos fuente de programas	Control: Se deben restringir el acceso a los códigos fuente de los programas.
r i p t o	A.10.1 Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

TABLA No. 9 CONTROLES SEGURIDAD DE LA INFORMACIÓN

Controles 27001:2013		
	A.10.1.2 Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11 Seguridad física y del entorno	A.11.1.1 Perímetro de seguridad física	Control: Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
	A.11.1.2 Controles físicos de entrada	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
	A.11.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
	A.11.1.5 Trabajo en áreas seguras	Control: Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.
	A.11.1.6 Áreas de despacho y carga	Control: Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
	A.11.2.1 Ubicación y protección de los equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
	A.11.2.2 Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
	A.11.2.3 Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño
	A.11.2.4 Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.11.2.5 Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa
	A.11.2.6 Seguridad de equipos y instalaciones	Control: Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
	A.11.2.7 Disposición segura o reutilización de equipos	Control: Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
	A.11.2.8. Equipos de usuario desatendidos	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.
	A.11.2.9 Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 Seguridad de las operaciones	A.12.1.1 Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
	A.12.1.2 Gestión de cambios	Control: Se deben 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.
	A.12.1.3 Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
	A.12.2.1 Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	A.12.3.1 Respaldo de información	Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
	A.12.4.1 Registro de eventos	Control: Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	A.12.4.2 Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
	A.12.4.3 Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
	A.12.4.4 sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo
	A.12.5.1 Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	A.12.6.1 Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	A.12.6.2 Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.
	A.12.7.1 Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 Seguridad de las comunicaciones	A.13.1.1 Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	A.13.1.2 Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
	A.13.1.3 Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
	A.13.2.1 Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
	A.13.2.2 Acuerdos sobre transferencia de información	Control: Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.

TABLA No. 9 CONTROLES SEGURIDAD DE LA INFORMACIÓN

Controles 27001:2013		
	A.13.2.3 Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
	A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Control: Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimientos de sistemas	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
	A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
	A.14.2.1 Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
	A.14.2.2 Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
	A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
	A.14.2.4 Restricciones en los cambios a los paquetes de software	Control: Se debe desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
	A.14.2.5 Principios de construcción de sistemas seguros	Control: Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
	A.14.2.6 Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
	A.14.2.7 Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
	A.14.2.9 Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
	A.14.3.1 Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15 Relación con los proveedores	A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se debe establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
	A.15.1.3 Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
	A.15.2.2 Gestión de cambios en los servicios de proveedores	Control: Se debe gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.16 Gestión de incidentes de seguridad de la información	A.16.1.1 Responsabilidad y procedimientos	Control: Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
	A.16.1.2 Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
	A.16.1.3 Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
	A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información.
	A.16.1.5 Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
	A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
	A.16.1.7 Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
	A.17.1.2 Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
	A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

TABLA No. 9 CONTROLES SEGURIDAD DE LA INFORMACIÓN		
Controles 27001:2013		
A.18 Cumplimiento	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
	A.18.1.2 Derechos de propiedad intelectual	Control: Se debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
	A.18.1.3 Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
	A.18.1.4 Privacidad y protección de datos personales	Control: Cuando sea aplicable, se debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes
	A.18.1.5 Reglamentación de controles criptográficos	Control: se debe usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes
	A.18.2.1 Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
	A.18.2.2 Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
	A.18.2.3 Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

TABLA 10. Peso o Participación de cada variable en el Diseño del Control para la Mitigación del Riesgo

Criterio de evaluación	Aspecto a Evaluar en el Diseño del Control	Opciones de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realiza la actividad de control.	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?.	Confiable	15
		No confiable	0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la..	Completa	10
		Incompleta	5
		No existe	0

TABLA 11. Calificación del Diseño del Control

Rango de calificación del diseño del control	Resultado - peso en la evaluación del diseño del control	RANGO DE CALIFICACIÓN DEL DISEÑO
Fuerte	Calificación entre 96 y 100	0
Moderado	Calificación entre 86 y 95	1
Débil	Calificación entre 0 y 85	2

TABLA 12. Calificación de Ejecución del Control

Rango de calificación de la ejecución del control	Resultado - peso en la evaluación de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

TABLA 13. Calificación Solidez Individual del Control

Peso individual del diseño (DISEÑO)	El control se ejecuta de manera consistente por los responsables. (EJECUCIÓN)	Solidez individual de cada control fuerte:100 moderado:50 debil:0	Aplica plan de acción para fortalecer el control Sí / NO
fuerte calificación entre 96 y 100	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Si
	débil (no se ejecuta)	fuerte + débil = débil	Si
moderado calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Si
	moderado (algunas veces)	moderado + moderado = moderado	Si
	débil (no se ejecuta)	moderado + débil = débil	Si
débil entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Si
	moderado (algunas veces)	débil + moderado = débil	Si
	débil (no se ejecuta)	débil + débil = débil	Si

TABLA 14. Calificación de la Solidez del Conjunto de Controles	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50.

TABLA 15. Resultados de los Posibles desplazamientos de la Probabilidad y del Impacto de los Riesgos

Solidez del conjunto de los controles	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de impacto
fuerte	directamente	directamente	2	2
fuerte	directamente	Indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	Indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

7. CONTROL DE CAMBIOS:

Versión	R.R. No.	Descripción de la modificación
1.0	R.R. 02 09 mayo 2013	Se unificaron los Procedimientos para Elaborar el Mapa de Riesgo Institucional código 01010 versión 1.0 y Procedimiento de Evaluación y Seguimiento de los Riesgos Código PEC05 versión 1.0, en el Procedimiento para Elaborar y Realizar Monitoreo y Seguimiento al Mapa de Riesgos Institucional, Código PDE-10, el cual hace parte del Proceso de Direccionamiento Estratégico. En consecuencia se modificó el alcance, base legal, definiciones, anexos y descripción del procedimiento.
2.0	R.R. 011 25 abril 2016	El procedimento cambia de versión, a fin de dar cumplimiento a las directrices impartidas por la Alta Dirección mediante Circular 3-2017-16522 de junio 27 de 2017, en la cual se estableció la necesidad de ajustar todos los documentos del Sistema Integrado de Gestión al nuevo esquema del mapa de procesos de la Entidad, generado por los cambios surtidos en las normas ISO 9001:2015, ISO 14001:2015, Decreto 1072 de 2015 y demás normas reglamentarías, Acuerdo 658 de 2016, modificado parcialmente por el Acuerdo 664 de 2017. Mapa de Procesos que fue formalizado en la nueva versión del Manual del SIG, la cual fue adoptada mediante Resolución Reglamentaria No. 30 del 25 de septiembre de 2017. En consecuencia el procedimiento fue ajustado en algunos de sus apartes como: objetivo, alcance, base legal, definiciones, descripción del procedimiento y anexos. Así mismo, se ajustó el formato a la nueva estructura definida en el Procedimiento para Mantener Información Documentada del SIG. Se cambia el nombre del procedimiento de Procedimiento para Elaborar y Realizar Monitoreo y Seguimiento al Mapa de Riesgos Institucional por *"Procedimiento para Elaborar el Mapa de Riesgos Institucional"*

Versión	R.R. No.	Descripción de la modificación
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.
5.0	R.R.008 14 febrero 2019	