ADMINISTRACIÓN DEL RIESGO EN APC-COLOMBIA

CONTENIDO

TABLAS

1. POLÍTICA

Para la Agencia Presidencial de Cooperación Internacional APC-Colombia es prioritario y estratégico administrar los riesgos inherentes a su gestión, lo cual incluye la formulación del contexto estratégico, identificación, valoración, calificación, tratamiento y seguimiento de los mismos y de las acciones que se formulen para evitarlos, o para atenderlos en caso de que se materialicen.

El presente documento contiene política, diagnóstico, lineamientos y metodología para la identificación y administración del riesgo en APC-Colombia.

La política de riesgos de APC-Colombia tiene los siguientes elementos:

Tabla 1. Elementos de la política de gestión de riesgos

Componente	Desarrollo
Objetivos	La gestión de riesgos está alineada con los objetivos estratégicos de la entidad y tiene por objetivos los previstos en el capítulo denominado “objetivos” en el presente documento.
Alcance	La Administración del Riesgo es extensible y aplicable a todos los procesos de la entidad. Su alcance está descrito en el capítulo denominado “alcance” en el presente documento.
Niveles de aceptación del riesgo	Decisión informada de tomar un riesgo particular. (NTC GTC137, Numeral 3.7.1.6).
Niveles para la calificación del impacto	El análisis del impacto se hará como se describe en el capítulo denominado “impacto” en el presente documento..
Tratamiento del Riesgo	Se hará como se describe en el presente documento.
Seguimiento	La periodicidad para el seguimiento de acuerdo al nivel de riesgo residual se describe en el capítulo destinado al “seguimiento” en el presente documento.
Responsabilidad	Los niveles de responsabilidad en materia de riesgos se describen en el capítulo denominado “responsabilidad” en el presente documento.

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública https://www.funcionpublica.gov.co/guias

Es política de APC-Colombia administrar sus riesgos, teniendo en cuenta lo siguiente:

a) Los riesgos institucionales están integrados por:
   - Los riesgos que sean establecidos específicamente como institucionales.
   - Los riesgos que sean clasificados con mayor criticidad en el mapa de calor.

b) Los planes de contingencia se formulan para los riesgos que se encuentren en las zonas de riesgo de mayor criticidad.

c) Los riesgos pueden ser clasificados en más de una categoría. En este caso se tendrán en cuenta las siguientes consideraciones:

- Si dentro de las múltiples clasificaciones se selecciona la de corrupción, dicha clasificación tendrá prelación sobre las demás y el riesgo será evaluado con la metodología prevista para tal fin.
- Si el riesgo no es de corrupción, pero tiene múltiples clasificaciones, tendrá prelación la clasificación que mayor impacto genere sobre el riesgo.

d) Adicionalmente, en cumplimiento del MECI 2014, esta política contiene:
- Los objetivos que se esperan lograr (ver título denominado “objetivos”)
- Las estrategias para establecer cómo se van a desarrollar a largo, mediano y corto plazo (ver título denominado “estrategia”).
- Los riesgos que se van a controlar (ver mapa de riesgos que se formula).
- Las acciones a desarrollar contemplando el tiempo, los recursos, los responsables y el talento humano requerido (ver mapa de riesgos que se formula).
- El seguimiento y evaluación a su implementación y efectividad (ver título denominado “seguimiento”).
- Los lineamientos con respecto al tratamiento que se le debe dar a los distintos riesgos según su evaluación y valoración (ver mapa de riesgos que se formula).

e) La gestión de riegos tendrá en cuenta las líneas de defensa.

Con el fin de asegurar que las acciones de la gestión del riesgo y los controles que se definan funcionen según lo previsto y de evitar que las alertas en esta materia sean tardías, APC-Colombia no puede limitarse a atender las acciones que deriven de los hallazgos encontrados por las instancias de control.

Si bien los equipos de auditores internos, especialistas en gestión de riesgos, especialistas en control interno, investigadores de fraude, y otros profesionales de riesgo y control pueden ayudar a las entidades a gestionar el riesgo, es necesario tener claridad en los roles específicos y en la coordinación de los mismos, de tal forma que se eviten controles innecesarios o duplicación de funciones y tareas.

Un mecanismo para facilitar esta labor es el modelo de las Tres Líneas de Defensa, elaborada por el Instituto Internacional de Auditores Internos y adoptado como mejor práctica en el entorno internacional.

En APC-Colombia dicho mecanismo es un referente en la administración de riesgos, incluyendo los de corrupción y los de los sistemas de gestión.

La administración de riesgos, como se mencionó en el alcance, compromete a servidores, contratistas y terceros de toda la APC-Colombia. Es responsabilidad de todos y cada uno, identificar los riesgos asociados a los procesos y objetivos de la

entidad y gestionar las acciones que eviten que se materialicen o de adelantar los planes de contingencia respectivos si se produce dicha materialización.

Por tal razón las líneas de defensa de la entidad incorporan las responsabilidades en los diferentes roles y se aplica de la siguiente manera:

Tabla 2. Líneas de defensa, roles y responsabilidades

Línea de Defensa	Rol	Responsabilidad y Estrategia
Primera	Líderes de Proceso proyectos y/o programas	- Los líderes de proceso son responsables de identificar y evaluar los riesgos y administrarlos. También son responsables de la implantación de acciones preventivas y correctivas correspondientes y de mantener controles internos eficaces. - Involucrar a todos los miembros de su equipo en la implementación de los lineamientos de la política de la administración para la gestión del riesgo. - Determinar de forma objetiva la probabilidad y el impacto de los riesgos identificados, en un ejercicio determinante para establecer controles que mitiguen el riesgo. - Realizar el seguimiento y la evaluación a los controles diseñados e implementados y hacer los registros en el aplicativo Brújula o en la herramienta establecida en el caso que el aplicativo presente fallas. - Definir las medidas preventivas resultantes de las autoevaluaciones. - Realizar las actualizaciones al mapa de riesgos resultantes de las autoevaluaciones del proceso.
Segunda	Oficina de Planeación (o quien haga sus veces)	- El grupo de trabajo con funciones de Planeación, establece los lineamientos y hace el acompañamiento metodológico a los procesos para la documentación de los riesgos. - Definir y elaborar los lineamientos de la administración del riesgo. - Elaborar y realizar la difusión de lineamientos, metodología, seguimiento y consolidación los mapas de riesgo. - Hacer el acompañamiento metodológico a los procesos para la documentación de los riesgos. - Realizar seguimiento a los procesos para que den alcance a la política de seguimiento y evaluación a los riesgos. - Realizar seguimiento a los indicadores, al desarrollo de herramientas y documentación de los controles. - Articular la formulación de la política con las áreas que tienen sistemas de gestión a cargo.
Segunda	Todo el personal de la entidad	- Los equipos de trabajo de los diferentes procesos establecen y ejecutan las acciones y los controles. - Identificar peligros y evaluar los riesgos.[1] - Participar en la evaluación del Sistema de Control Interno[2]. - Evaluar los riesgos[3]. - Proponer y desarrollar planes de mejora para abordar debilidades identificadas[4]. - Aplicar y fortalecer el autocontrol como principio clave en el seguimiento a los riesgos asociados al proceso.

[1] Decreto 1443 de Julio 31 de 2014, capítulo IV, Artículo 15, Parágrafo 1. Compilado en el Decreto 1072 de 2015.
[2]Meci 2014.
[3]Meci 2014.
[4]Meci 2014.

Línea de Defensa	Rol	Responsabilidad y Estrategia
Tercera	Director General	- Involucrar, la participación activa de los líderes y sus equipos de trabajo para la identificación, diseño, estandarización y actualización permanente de los procesos a su cargo, la gestión de los riesgos y la verificación constante sobre la aplicación de los mecanismos de verificación de su gestión, de la cual hará parte la realizada por los diferentes organismos de control - Formular la política de Administración del Riesgo con las instancias que se hayan definido para tal fin. - Estimular la cultura de la identificación y prevención del riesgo. - Establecer canales de comunicación. - Apoyar todas las acciones emprendidas, propiciando espacios y asignando recursos necesarios. - Nombrar a un representante que asesore y apoye todo el proceso de diseño e implementación de la Administración de Riesgo. - Gestionar y aplicar la metodología de Administración del riesgo.
Tercera	Oficina de Control Interno (o quien haga sus veces	El área con funciones de control interno, coadyuva a construir y supervisar los controles de la primera línea de defensa, a través de: - Revisar la implementación de prácticas eficaces de evaluación y mitigación de riesgos, incluyendo los de corrupción, así como registrar y comunicar adecuadamente la información asociada a dichos riesgos en toda la entidad. - Revisar riesgos específicos, como el incumplimiento de las leyes y reglamentos aplicables. - Realizar auditoría y promover la autoevaluación. - Seguir, evaluar y verificar si la política para la gestión del riesgo está actualizada acorde con los cambios que se dispongan y si se realizan revisiones periódicas e informar la eficacia de la política en el control de los riesgos institucionales y por proceso. - Verificar dentro de la evaluación y seguimiento, que la entidad cuente con políticas de administración de riesgos actualizadas, que se estén ejecutando y que se realicen revisiones periódicas a las mismas.[5] - Brindar apoyo en la metodología de administración del riesgo para su identificación a través # de su rol de asesoría y acompañamiento. - Asesorar y capacitar a la alta dirección y a los líderes de los procesos en la metodología para su gestión, y verificar que los controles existentes sean efectivos para minimizar la probabilidad e impacto de la ocurrencia de los mismos.[6] - Entregar a la alta dirección una evaluación objetiva e independiente sobre la eficacia y efectividad de la administración del riesgo adoptada por la Entidad. - Verificar si los líderes de los procesos realizan seguimiento y registro periódico a los riesgos identificados.
Tercera	Auditores internos	- Proporcionar razonabilidad sobre la eficacia de la gobernanza, la administración de riesgos y el control interno, incluyendo la forma en que la primera y segunda líneas de defensa contribuyen a alcanzar los objetivos de administración de riesgos de corrupción y su control.

[5] MECI p.75

[6] manual técnico del MECI. "Valoración del riesgo

Línea de Defensa	Rol	Responsabilidad y Estrategia
Tercera	Comité de Coordinación de Control Interno	- Propender por una adecuada implementación de procedimientos de control interno para todos los riesgos significativos, independientemente de su naturaleza (operativa, de cumplimiento, financieros, fiscales).[7] - Formular la política de Administración del Riesgo con el Representante Legal de la entidad.[8] - Someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.[9]
Tercera	Comité Paritario de Seguridad y Salud en el Trabajo de COPASST.	- Apoyar la identificación y seguimiento a los riesgos de salud y seguridad laboral. - Realizar las inspecciones de las instalaciones de la entidad. - Emitir las recomendaciones a que haya lugar sobre la identificación de peligros y la evaluación de riesgos de SST.[10]
Tercera	Comité de Conciliación	- Aprobar la política para la prevención del daño antijurídico.
Tercera	Comité de seguridad de la información	- Revisar la política de seguridad de la información.
Tercera	Comité Institucional de Desarrollo Administrativo	- Aprobar las políticas en materia de riesgos. - Conocer de los resultados de la gestión de riesgos de la entidad, en el marco de la revisión por la dirección y la revisión de las políticas de desarrollo administrativo. - Realizar recomendaciones al Director General respecto con el propósito de lograr una gestión institucional integral. - Gestionar la adopción de las políticas de desarrollo administrativo. - Liderar, coordinar y facilitar la implementación del Modelo Integrado de Planeación y Gestión. - Realizar monitoreo, control y evaluación del Modelo Integrado de Planeación y Seguimiento - Realizar seguimiento al cumplimiento de las políticas de desarrollo administrativo.
Tercera	Enlaces (en caso de tener vigente dicho rol)	- Apoyar al líder de proceso en las actividades que sean necesarias para administrar los riesgos a su cargo.
Tercera	Administradora de Riesgos Laborales - ARL	- Apoyar la documentación de los riesgos relacionados con la salud y la seguridad en el trabajo. - Asesorar la gestión del riesgo de la entidad.

Fuente: Ver normas

2. ALCANCE

La administración de riesgos compromete a servidores, contratistas y terceros de toda la APC-Colombia en el fortalecimiento de la gestión de riesgos de acuerdo con los

[7] Meci 2014.
[8] Numeral 1.3.1 MECI
[9] Decreto 648 de 2017, Artículo 2.2.21.1.6.
[10] Decreto 1072 de 2015-Artículo 2.2.4.6.15

requisitos de las partes interesadas, las interfaces y dependencias entre las actividades realizadas por la organización y las que realizan otras organizaciones[11].

3. OBJETIVOS

La Administración de Riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con los procesos de una forma que permita a la entidad minimizar pérdidas y maximizar oportunidades[12]. En el marco de este concepto los objetivos definidos por la entidad en la gestión del riesgo son:

3.1 Objetivo general

Asegurar que la gestión institucional de la Agencia Presidencial de Cooperación Internacional de Colombia, APC-Colombia, no se vea afectada en el logro de sus metas, objetivos institucionales y de cumplimiento legal, con la materialización de los riesgos que se identifiquen.

3.2 Objetivos específicos

- Orientar la manera de identificar los riesgos internos y externos a los que está expuesta la entidad, independiente de la naturaleza[13] de los mismos.
- Gestionar acciones preventivas para evitar que los riesgos identificados se materialicen.
- Gestionar acciones de contingencia, si llegase a materializarse el riesgo.
- Gestionar acciones correctivas para evitar que el riesgo se vuelva a materializar.
- Aplicar las disposiciones que en materia de riesgos deba atender APC-Colombia.[14]
- Propiciar en los Servidores Públicos una cultura de Autocontrol y Autoevaluación del riesgo al interior de la Agencia.
- Generar mecanismos orientados a prevenir o evitar la materialización de los riesgos de corrupción.
- Articular la gestión de riesgos en los diferentes sistemas de gestión.
- Formular un documento que sirva de insumo para el diseño de nuevas funcionalidades en el aplicativo Brújula, para el módulo de riesgos.

4. ARTICULACIÓN EN LOS SISTEMAS DE GESTIÓN

La gestión de riesgos está prevista en los sistemas de gestión, así:

[11] Da cumplimiento a lo establecido en la Norma NTC-ISO/IEC 27001:2013, numerales 4.3.a a 4.3.c
[12] Referencia hecha en el Numeral 1.3. del MECI 2014 al Estándar Australiano AS/NZS 4360:199910.
[13] OHSAS 18001, 4.3.1
[14] Incluye lo contenido en: a) OHSAS 18001, 4.3.1.a y b. b) Decreto 1443 de 2014, capítulo III, artículo 8, numeral 6. c) Numeral 1.3. del MECI 2014, entre otras.

Tabla 3. Elementos de la gestión de riesgos, requeridos en las normas que regulan los sistemas de gestión.

Tema	**Calidad**	**Ambiental**	**Seguridad de la información**	**Seguridad y salud**		**MECI 2014**	**GEL**	**Anti corrupción**
NORMA / Ítem	**NTCGP 1000:2009**	**ISO 14001:2015**	**NTC-ISO/IEC 27001:2013**	**OHSAS 18001**	**SGSST Dec1443/ 2014 compilado en Dec 1072 de 2015**	**Decreto 943 de 2014 May 21**	**GEL**	**Decreto 124 de 2016**
Política						1.3.1 y 1.3.5		VI-1
Metodología			4.1., 6.1.1. y 8.2	4.3.1.a y b	Art 15, 16, 23 y 24	1.3., 1.3.2., 1.3.3. y 3		
Procedimiento			6.1.2.	4.4.3.2.a 4.3.1	Art 26			
Identificación	7.5.1.g	6.1	6.1.1	4.3.1	Art 8 y 15	1.3., 1.3.1., 1.3.2., 1.3.3.	x	
Controles	4.1.g		6.1.3	4.3.1 4.4.6				
Registros				4.3.1 4.4.4.e	Art 12 y 33	3		
Formación				4.4.2	Art 11			
Roles					Art 15	1.3., 1.3.1., 1.3.2., 1.3.3., 2.1.1		
Valoración			6.1.2			1.3.3.		VI-6.6
Insumo para			6.1.3., 6.2.c., 9.3.c	4.3.3	Art 12, 24 y 31	1.2.4., 2.1.1		
Seguimiento						1.3., 1.3.2		VI-5
Apropiación					Art 11	1.3.1., 1.3.2		
Revisión					Art 31 y 33	1.3.1., 1.3.2		

Fuente: Normas de los sistemas de gestión

Es de señalar que los sistemas sobre los cuales aplican estas normas son integrables entre sí, de acuerdo con normas como las siguientes:

Tabla 4. Normativa de Integración de los sistemas de gestión

Lineamiento	Articulación
Decreto 2609 de diciembre 14 de 2012, compilado en el Decreto 1080 de 2015	El Programa de Gestión Documental (PGD) con los otros sistemas administrativos y de gestión establecidos por el Gobierno Nacional o los que se establezcan en el futuro.
Ley 872 de diciembre 30 de 2003	El Sistema de Gestión de calidad con el Sistema de Control Interno en cada uno de sus componentes.
Plan Nacional de Desarrollo 2014-2018 "Todos Por Un Nuevo País", aprobado mediante la Ley 1753 de junio 09 de 2015, Artículo 133	Sistemas de Gestión de Calidad con el de Desarrollo Administrativo. Sistema de Gestión con los Sistemas Nacional e Institucional de Control Interno.
Norma Técnica de Calidad en la Gestión Pública NTCGP 1000 Versión 2009, cuya actualización se aprobó mediante Decreto 4485 de Noviembre 18 de 2009, compilado en el Decreto 1083 de 2015, anexo C	Seguridad y Salud en el Trabajo (NTC-OSHAS 18001:2007), Gestión ambiental (NTC-ISO 14001:2004) y Calidad (NTCGP 1000:2009).
Decreto 2482 de 2012 estableció el formulario Único Reporte de Avance de la Gestión – Furag (preguntas 175, 176, 185, 186, 187).	Sistemas de gestión, la certificación de los mismos y la auditoría integral.
Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública	Administración de riesgos de contratación con la de riesgos institucionales. Administración de riesgos de proyectos con la de riesgos institucionales.

Fuente: Normas referenciadas en la tabla.

5. DIAGNÓSTICO

5.1 Lineamientos

Los primeros lineamientos para la administración del Riesgo de la entidad se formularon en marzo 11 de 2013 por medio de un documento que inicialmente se identificó como DG-D-008. Este documento, actualmente identificado como E-OT-008, ha sido el elemento orientador en esta materia y a lo largo del tiempo ha venido incorporando mejoras que le permiten a la entidad articular diferentes aspectos de la gestión en diferentes campos.

5.2 Herramienta tecnológica

En 2014 fue adquirida una herramienta tecnológica para el Sistema de Gestión. Actualmente es conocida como “Brújula”, se accede desde la Intranet de la entidad y tiene las siguientes funcionalidades:

Tabla 5. Módulos del aplicativo Brújula

Módulo	Contenido	Opciones
Estrategia	BSC	Edición; Medición; Reportes; Cargar Información; Terminar Sesión
	Planes y proyectos	Parametrización; Planes y Políticas de Operación (Creación / Edición); Recursos y fuentes (Creación / Edición); Proyecto / Actividad (Creación / Edición); Ejecución Proyectos / Actividades; Reportes; Terminar Sesión
Procesos	Documentos	Edición; Editar glosario; Edición normograma; Solicitud documentos; Listado maestro de documentos; Glosario; Normograma; Reportes; Terminar Sesión
	Planes de mejoramiento	Edición; Reportar Hallazgos; Reportes; Editar fechas tareas; Terminar Sesión
	Auditorías	Edición; Programa de auditoría; Ejecución auditorías; Seguimiento auditorías; Reportes; Reportes estadísticos; Terminar Sesión
Reuniones	Reuniones	Edición; Actas revisión por la dirección; Actas general; actas; Reportes; Terminar Sesión
Talento Humano	Hojas de vida	Edición profesiones; Edición hojas de vida; Reportes; Terminar Sesión
	Plan Institucional de capacitación	Edición; Ejecución; Reportes; Terminar Sesión
	Programa de bienestar social	Edición; Ejecución; Reportes; Terminar Sesión
	Evaluación de competencias	Edición; Evaluación cargos de carrera administrativa; Reportes; Terminar Sesión
	Salud Ocupacional - S&SO	Edición; Actividades Subprogramas; Avance Actividades Subprogramas; Edición Legal; Creación Matriz Legal; Edición Riesgos; Creación Matriz Riesgos; Novedad Personal; Generar Versión; Reportes; Terminar Sesión
Encuestas	Encuestas	Edición profesiones; Edición hojas de vida; Reportes; Terminar Sesión
Meci	Meci	Edición; Evaluación del MECI; MECI; Ayuda; Terminar Sesión
Riesgos	Riesgos	Edición; Creación e identificación riesgos; Seguimiento Líder Proceso; Seguimiento Control Interno; Reportes; Terminar Sesión
Administración	Administración	Dependencias; MacroProcesos; Procesos; Cargos; Usuarios; Perfiles; Comités / Coordinaciones / Procesos; Cargar información; Terminar Sesión

Fuente: Brújula

Como se aprecia en la zona resaltada en la tabla anterior, dicha herramienta cuenta con un módulo destinado a la administración de los riesgos.

Dicho módulo fue diseñado con la metodología de riesgos expedida por el Departamento Administrativo de la Función Pública - DAFP, se encuentra en operación y allí están almacenados los datos de los riesgos actualmente identificados para los doce (12) procesos establecidos en el Sistema de Gestión.

En la opción “ayuda” de dicho módulo se encuentra el instructivo de uso del mismo.

La herramienta tecnológica no suple todas las necesidades de la entidad en materia de riesgos. Requiere algunos ajustes para que permitan incorporar otros riesgos cuya metodología tiene algunas variaciones respecto de la del DAFP, como por ejemplo los de salud y seguridad laboral, que por el momento recurren a herramientas ofimáticas alternas y no permiten su total integración.

Por el momento la gestión de los mismos se apoya en otros mecanismos como el formato externo aplicable a los riesgos de Salud y Seguridad laboral o las variaciones del formato estándar.

5.3 Mapa de riesgos

La entidad, desde su creación, ha formulado su mapa de riesgos y lo ha publicado en el portal Web, en cumplimiento de lo establecido en el plan anticorrupción y de atención al ciudadano para todas las entidades públicas de Colombia. No obstante, son pocos los registros que dan cuenta de su seguimiento y análisis al interior de la entidad. Su evolución en este aspecto es medible especialmente con los mecanismos externos, tal y como se explica en el numeral 8.16 del presente documento.

5.4 Integración de la información

Las directrices del orden nacional promueven la integración de los sistemas de gestión, pero los lineamientos se expiden de manera específica para cada temática, como es el caso de riesgos de SGSST, riesgos de corrupción, riesgos de seguridad de la información, etc., que son documentos establecidos para una temática en particular.

Por tanto, el fortalecimiento interno exige encontrar elementos comunes que permitan articular las diferentes metodologías de gestión de riesgos, lo cual se tiene previsto a través del presente documento.

Una de las dificultades encontradas para llegar a este propósito es que, como consecuencia de lineamientos nacionales diferentes, existen diferentes formas de presentar los riesgos lo cual no permiten su comparación. Por ejemplo, los riesgos de los procesos están actualmente clasificados en el mapa de calor de la siguiente manera:

Cantidad de riesgo residual	
Zona de riesgo	Cantidad
B. Zona de Riesgo Baja.	2
M. Zona de Riesgo Moderada.	4
A. Zona de Riesgo Alta.	6
E. Zona de Riesgo Extrema.	1

En tanto los de la seguridad y salud en el trabajo, se adelanta a partir de una matriz entregada por la ARL, en la cual se encuentran registrados los peligros y se evalúan los riesgos, que potencialmente se repiten de una zona a otra, así:

Tabla 6. Estado de riesgos de SST

Zona	Bajo	Medio	Alto	Muy alto	Total
Dirección general	0	10	3	0	13
Recepción	0	6	2	0	8
Zona 1 (Dirección Administrativa - Coordinación Administrativa - Coordinación Financiera - Jurídica - Asesor Jurídico y Contractual)	0	8	2	0	10
Zona 2: Dirección Demanda - Dirección Oferta - DCI -	0	9	3	0	12
Zona 3: Oficinas de Talento Humano - Comunicaciones - Gestión TI - Control Interno.	0	8	2	0	10
Salas de reuniones	0	2	0	0	2
Data center	4	0	0	0	4
Archivo y gestión documental	0	3	0	1	8
Cafetería	2	0	2	0	4
Bodegas	2	0	1	0	3
Pasantes	0	6	2	0	8
Conductores	1	5	0	0	6
Total	9	57	17	1	84

Fuente: matriz de peligros SST.

Lo mismo ocurre con otros esquemas como el de seguridad de la información.

Las diferencias más representativas entre los lineamientos de Riesgos para los diferentes sistemas de gestión se concretan en las matrices de calor, que son diferentes en todos los casos y se contraponen frente a un riesgo que puede ser parte de más de uno de los sistemas de gestión. Por ejemplo, un riesgo detectado para el Sistema de Gestión Ambiental queda clasificado en una zona de la matriz de calor, pero el mismo riesgo identificado en el sistema de Seguridad de la Información no necesariamente coincide en la zona en que se clasificó para el primero de los sistemas. De otra parte, el alto número de riesgos identificados ya es de por sí una dificultad para su seguimiento, y se complica si no se cuenta con un mecanismo unificado para tal fin.

5.5 Cultura interna

La entidad ha hecho un gran esfuerzo en la identificación de riesgos, pero aún debe fortalecer dicha identificación, al igual que el seguimiento y la cotidianidad de los registros.

En cuanto a la apropiación del concepto, el mismo se ha incluido en las actividades del sistema de calidad, así:

Tabla 7. Actividades de apropiación del concepto de gestión del riesgo en 2016 y 2017

<table>
<tr><th>Fecha</th><th>Actividad</th><th>Desarrollo</th></tr>
<tr><td>Abril 25 y 27 de 2016</td><td>Actividad lúdica</td><td>A cada persona le fue dejado en su escritorio un documento con algunos conceptos del Sistema de Gestión de Calidad, unos días después un personaje animado de Foamy los visitó y les hizo preguntas con respecto a dichos conceptos, entre los cuales se incluyeron los de gestión del riesgo.</td></tr>
<tr><td>Mayo 04 al 16 de 2016</td><td>Cuestionario 1 de apropiación de conceptos</td><td>A través de Brújula fue enviado un cuestionario de 10 preguntas a 112 personas de la entidad, de las cuales 77 respondieron. Una de las preguntas involucraba el concepto de gestión del riesgo, y se evidenció una baja apropiación, dado que solo fue considerado por 5 personas.
<table>
<tr><th>Pregunta</th><th>Respuesta</th><th>Análisis</th></tr>
<tr><td>Los planes de mejoramiento (preventivos, correctivos y de mejora) se formulan como consecuencia de:</td><td>a) Hallazgos identificados en auditoría interna. = 43
b) Reincidencia en productos no conformes. = 9
c) Identificación de riesgos. = 5
d) Como resultado del análisis de los resultados obtenidos en la aplicación de indicadores. = 3
e) Como resultado del ejercicio de autoevaluación. = 7
Sin respuesta = 42</td><td>De todas las posibles fuentes de plan de mejora, se ha apropiado la de auditorías.</td></tr>
</table></td></tr>
<tr><td>Septiembre 5 al 16 de 2016</td><td>Cuestionario 2 de apropiación de conceptos</td><td>A través de Brújula fue enviado un cuestionario de 10 preguntas a 91 personas de la entidad, de las cuales 49 respondieron. Una de las preguntas involucraba el concepto de gestión del riesgo.
<table>
<tr><th>Pregunta</th><th>Respuestas</th><th>Análisis</th></tr>
<tr><td>4. En el ciclo PHVA, el seguimiento a los planes, indicadores, riesgos, etc, hace parte del:</td><td>a) Planear = 3
b) Hacer = 1
c) Verificar = 69
d) Ajustar = 4
e) Sin respuesta = 36</td><td>El 90% de las personas que respondieron la encuesta acertaron en señalar el seguimiento como parte del verificar del ciclo PHVA.</td></tr>
</table></td></tr>
<tr><td>Octubre 18 a 21 de 2016</td><td>Crucigrama</td><td>El martes 18 de octubre se dejó en cada escritorio una hoja impresa con el crucigrama y una colombina.
El crucigrama se responde con palabras relacionadas con el Sistema de Gestión de la Calidad, ubicadas 10 en posición horizontal y 19 en forma vertical, para un total de 29. La línea 8 vertical daba cuenta del concepto de gestión del riesgo. Respondieron 77 personas de las cuales 76 acertaron en el concepto.</td></tr>
<tr><td>Noviembre 21 de 2016</td><td>Día de la calidad</td><td>Durante toda la tarde se visitaron todas las islas de la entidad y cada persona seleccionó uno de los papelitos que contenían las preguntas y daba respuesta a las mismas. El concepto de gestión del riesgo se preguntó de diversas maneras y la gente respondió acertadamente.</td></tr>
<tr><td>Mayo 4 al 18 de 2017</td><td>Cuestionario de apropiación de conceptos</td><td>El jueves 04 de mayo de 2017 se cargó en Brújula un cuestionario de 10 preguntas, formuladas en rima simple, sin rigor fonético ni métrico literario, para seleccionar una única respuesta entre cuatro opciones para cada una. Dicho cuestionario llegó los destinatarios por mail con un vínculo a Brújula, desde el cual accedieron al mismo. La pregunta 5 incluyó la gestión del riesgo para establecer si la gente lo percibe como una exclusión.
<table>
<tr><th>Pregunta</th><th>Respuestas</th><th>Análisis</th></tr>
<tr><td>5. El diseño y desarrollo... no cuenta para la Agencia... en el Manual del Sistema... se elimina su presencia.</td><td>• Trazabilidad = 6
• Validación = 2
• Riesgo = 15
• Exclusión = 39
• Sin respuesta = 26</td><td>15 de las 58 personas que respondieron el cuestionario consideran erradamente que el riesgo está asociado al concepto de diseño y desarrollo.</td></tr>
</table></td></tr>
</table>

Fuente: Informes de las actividades señaladas.

5.6 Consulta externa

El mapa de riesgos está disponible en el portal Web de la entidad para consulta de los interesados. En 2016 el portal Web de la entidad tuvo 831.282 visitas, de las cuales algunas se hicieron a temas relacionados con la gestión de riesgos. En esta materia las más visitadas son:

Tabla 8. Visitas al portal Web en materia de riesgos

Sitio	Visitantes
Mapa de Riesgos 2016 - APC-Colombia	222
Mapa de Riesgos 2015 - APC-Colombia	92

Fuente: Reporte Web

5.7 Seguimiento a controles y acciones

Durante el 2016 se hizo un seguimiento a controles y acciones del mapa de riesgos del Sistema de Gestión de Calidad de dicha vigencia, con recaudo manual de la información tomada a partir de reuniones con los diferentes procesos, el cual se consolidó en agosto 31 del mismo año.

La mayoría de las acciones se cumplieron:

Tabla 9. Cumplimiento de acciones en materia de riesgos

Desarrollo de la acción	Cantidad de acciones
Cumplida	19
Cumplida parcialmente	3
No aplicó	1

Fuente: Análisis propio

La mayoría de los controles fueron útiles:

Tabla 10. Utilidad de los controles en materia de riesgos

Utilidad del control	Cantidad de controles
Control útil.	12
Control insuficiente	6
Control poco útil.	2
No corresponde con el riesgo.	3

Fuente: Análisis propio

Un resumen del seguimiento 2016 se muestra a continuación.

Tabla 11. Seguimiento a controles y acciones en la gestión del riesgo

Proceso	Riesgo	Seguimiento a las acciones	Seguimiento a los controles
Direccionamiento Estratégico y Planeación	Disminución en el presupuesto de inversión.	Cumplida	No corresponde con el riesgo.
Direccionamiento Estratégico y Planeación	Imprecisión en la formulación y ejecución de la planeación estratégica y planes de acción de la organización.	Cumplida	Control útil.
Direccionamiento Estratégico y Planeación	Generación de cambios que afecten el Sistema de Gestión Integral.	Cumplida	No corresponde con el riesgo.
Gestión de Comunicaciones	Entrega de información no confiable a los medios de comunicación.	Cumplida	Control útil.
Identificación y Priorización	Incumplimiento de las prioridades definidas en la Hoja de Ruta.	Cumplida	Control poco útil.
Preparación y Formulación	Incumplimiento de las condiciones y tiempos en la presentación de iniciativas en la cooperación internacional.	Cumplida	No corresponde con el riesgo.
Implementación y Seguimiento	Incumplimiento de los objetivos de los proyectos de cooperación internacional.	Cumplida	Control útil.
Implementación y Seguimiento	Incumplimiento en la ejecución de las actividades de cooperación sur-sur (CSS) y triangular (CT) programadas.	_ _ _	_ _ _
Gestión del Talento Humano	Posesionar personal que no cumple requisitos.	Cumplida	Control útil.
Gestión del Talento Humano	Incumplimiento en la ejecución de los planes y programas de Talento Humano.	Cumplida parcialmente	Control insuficiente
Gestión Contractual	Estudios previos y/o prepliegos de condiciones elaborados para favorecer a un oferente en particular.	Cumplida	Control insuficiente
Gestión Contractual	Contratar bienes y/o servicios que realmente no requiere la entidad.	Cumplida	Control útil.
Gestión Contractual	Ejecución del contrato sin el cumplimiento de requisitos y legalización.	Cumplida parcialmente	Control poco útil.
Gestión Administrativa	Pérdida, daño o hurto de los elementos o bienes de la entidad.	Cumplida	Control insuficiente
Gestión Administrativa	Pérdida o daño de información del archivo físico de la Entidad.	Cumplida	Control insuficiente
Gestión Administrativa	Destinación indebida de los recursos asignados a la caja menor.	Cumplida	Control insuficiente
Gestión Financiera	Incumplimiento en el pago de los compromisos financieros adquiridos por la entidad.	Cumplida	Control útil.
Gestión Financiera	Eventos financieros que afectan el manejo de las cuentas bancarias de la entidad.	Cumplida	Control útil.
Gestión Financiera	Pérdida de recursos monetarios disponibles en caja y bancos.	No aplicó	Control útil.
Gestión de Tecnologías de la Información	Pérdida de información contenida en la plataforma tecnológica.	Cumplida	Control útil.
Gestión de Tecnologías de la Información	Interrupción no programada del servicio de la plataforma tecnológica.	Cumplida parcialmente	Control insuficiente
Gestión Jurídica	Daño antijurídico en la actuación de la entidad que pueda afectar los intereses de la misma o a terceros.	Cumplida	Control útil.
Evaluación, Control y Mejoramiento	Incumplimiento en el plan de trabajo que aprobó el Comité Institucional de Desarrollo Administrativo en materia de Control Interno para la vigencia.	Cumplida	Control útil.
Evaluación, Control y Mejoramiento	Incumplir el envío de los informes o requerimientos de ley de las diferentes entidades y/o órganos de control.	Cumplida	Control útil.

Fuente: Análisis propio.

6. METODOLOGÍA

6.1 Etapas

Teniendo en cuenta el marco normativo aplicable que se relaciona en el capítulo 9 del presente documento, la gestión de riesgos de APC-Colombia opera con el esquema siguiente[15].

Ilustración 1. Esquema General de Administración del Riesgo

Fuente: ISO 31000: 2011

Para los asuntos de seguridad de la información, lo anterior se complementa con el siguiente esquema en el Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI):

Tabla 12. Etapas de la Gestión del Riesgo a lo Largo del MSPI

Etapas del MSPI	Proceso de gestión del riesgo en la seguridad de la información
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.
https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

6.2 Documentación

La metodología aplicable a la gestión de riesgos se encuentra recogida en los mínimos documentales requeridos en las normas asociadas, de la siguiente manera:

[15] Aplican las excepciones que se definan en la política de administración del riesgo.

Tabla 13. Documentos en materia de riesgos

Asunto	Documento
Diagnóstico	- Diagnóstico de riesgos generales presentado en agosto 27 de 2015, mismo documento reportado en el índice de transparencia y que ahora se recoge en el presente documento con las mejoras y actualizaciones respectivas. - Diagnóstico de los riesgos relacionados con la seguridad y salud en el trabajo, generado por la Administradora de riesgos laborales - ARL.
Política, Lineamientos y Metodología	- Política, Lineamientos y Metodología (E-OT-008). Este documento viene articulando la gestión de riegos de todos los sistemas de gestión. - Política de Prevención del daño antijurídico A-OT-015, el cual contiene un numeral que trata los asuntos relacionados con el análisis y distribución de los riesgos para la gestión de contratos y convenios. - Manual de riesgos contractuales A-OT-022.
Procedimiento	- Procedimiento para administración de riesgos (E-PR-008), requerido de manera obligatoria para algunos sistemas de gestión, se conformó de tal forma que fuera aplicable a todos los sistemas de gestión.
Formato	- Formato E-FO-017, el cual es un mecanismo de registro de las variables de la gestión del riesgo mientras se mejora el módulo de riesgos del aplicativo Brújula. - Matriz de riesgos de seguridad y salud ocupacional A-EX-001, plantilla que fue suministrada por la Administradora de riesgos laborales - ARL.
Registro	- Matriz de peligros de seguridad y salud laboral A-OT-044. - Matriz de riesgos de seguridad de la información. - Matríz de riesgos del daño antijurídico. - Mapa de riesgos de los procesos e institucional, antes trabajado como E-OT-028 y actualmente hace parte de los registros que se encuentran almacenados en el módulo de riesgos del aplicativo Brújula y aplicable a los demás sistemas de gestión.
Contexto estratégico	- Formulado por cada proceso en mesas de autocontrol.
Las normas aplicables	- Capítulo de “referencias normativas” del presente documento.

Fuente: Sistema de Gestión Integral de APC-Colombia

6.3 Contexto estratégico

Contexto estratégico “es el análisis que se hace de las brechas institucionales que deben ser intervenidas por la Agencia para el logro de los objetivos. Pueden ser producto de debilidades organizacionales, o bien de eventuales brechas que surgirán para enfrentar nuevos desafíos”[16].

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

La metodología para definir el contexto estratégico está establecida en el flujo que se sigue en el módulo de riesgos del aplicativo Brújula.

Se debe tener en cuenta lo siguiente:

[16] Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública.

- Para el desarrollo de las estrategias (cómo lograr lo propuesto como objetivo), debe conocerse el nivel de desempeño esperado (o sea las metas) y la forma de medirlas (o sea los indicadores).
- Las estrategias deben considerar aspectos como: Posición de la institución, Análisis de los productos (bienes y servicios) generados por la Entidad, Análisis de los grupos de interés.
- Los planes de acción o el conjunto de tareas que la Agencia establecerá para alcanzar los resultados, tiene que facilitar el cierre de las brechas que existan entre la situación actual y la situación deseada.

En la identificación del contexto estratégico, que se hace en la herramienta tecnológica de Brújula, se utiliza la Matriz DOFA, en la cual se aplican los siguientes conceptos:

Tabla 14. DOFA

Factores	Son:
Externos: Condiciones fuera de control de la entidad que son fuente de riesgo (legales. Ambientales. Políticas etc.).	**Oportunidades**: Aspectos que pueden propiciar mejoras en el desempeño.
	Amenazas: Aspectos que dificultan alcanzar niveles óptimos de desempeño.
Internos: Aspectos sobre los cuales la entidad puede ejercer control (organizativo, operacional etc.).	**Fortalezas**: Capacidades especiales con que cuenta la entidad y que le permite tener una posición privilegiada frente a la competencia. Recursos que se controlan, capacidades y habilidades que se poseen, actividades que se desarrollan positivamente, etc.
	Debilidades: Factores que provocan una posición desfavorable frente a la competencia, recursos de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente, etc.
De proceso: Aspectos controlables a nivel interno del proceso.	. . . . .

Fuente: Brújula.

En este sentido el contexto estratégico se identifica de forma institucional y adicionalmente por proceso.

Los factores a tener en cuenta en el contexto estratégico son:

Tabla 15. Factores para cada categoría del Contexto

Contexto	Factor
Externo	Económico: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Político: Cambios de gobierno, legislación, políticas públicas, regulación.
	Social: Demografía, responsabilidad social, orden público.
	Tecnológico: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	Medioambiental: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.
	Legal: Interpretación y aplicación de las normas.
	Información: disponibilidad, integridad y confidencialidad de la información.
Interno	Financiero: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	Personal: Competencia del personal, disponibilidad del personal, seguridad y salud en el trabajo, clima laboral, rotación, fuga de conocimiento.
	Proceso: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, conectividad.
	Estratégico: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
	Información: disponibilidad, integridad y confidencialidad de la información.
	Locativo: Instalaciones, mobiliario, servicios públicos
Del proceso	Diseño Del Proceso: Claridad en la descripción del alcance y objetivo del proceso.
	Interacción Con Procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procedimientos Asociados: Pertinencia en los procedimientos que desarrollan los procesos.
	Responsables Del Proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación Entre Procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública 2011
https://www.funcionpublica.gov.co/guias

Algunas técnicas que resultan fáciles y convenientes para elaborar y establecer el contexto estratégico pueden ser:

- Tomar como referente el objetivo del proceso de tal forma que los análisis se hagan considerando los eventos que impiden que dicho objetivo se cumpla.
- Definir, adicionalmente, lo que es de interés desarrollar, es decir las metas que se han trazado para el proceso y el portafolio de productos/servicios.
- Evitar la definición de un estado final deseado, ya que se corre el riesgo de manipular el ejercicio hacia lo que se desea obtener.

- La lista de las fortalezas y debilidades deben responder a la situación presente, no las proyectadas. En tanto que oportunidades y amenazas son las que existen actualmente y podrían presentarse en el futuro.
- Aplicar la lluvia de ideas, involucrando a quienes puedan aportar conocimientos complementarios.
- En todos los casos selecciones elementos reales, claros, objetivos y bien definidos.

El levantamiento del contexto estratégico se puede adelantar a través de las siguientes estrategias:

Tabla 16. Estrategias del Contexto

Factor	Definición
Inventario de Eventos	Listas de eventos posibles utilizadas con relación a un proyecto, proceso o actividad determinada
Talleres de Trabajo	Reuniones de funcionarios de diversas funciones o niveles. Para aprovechar el conocimiento colectivo del grupo y desarrollar una lista de acontecimientos que están relacionados con un proceso, proyecto o programa.
Análisis de Flujo de Procesos	Representación esquemática de interrelaciones de entradas, tareas, salidas y responsabilidades.

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic. (basada en la Guía de Riesgo del DAFP 2011)

6.4 Identificación de riesgos

La identificación de riesgos[17] consiste en establecer los riesgos. Este ejercicio puede apoyarse en metodologías como la lluvia de ideas, los 5 porqués y la observación directa, entre otras y, en lo posible, debe concretar los riesgos más representativos del proceso, de cada sistema de gestión y de la entidad. Se hace de la siguiente manera:

a) En seguridad y salud en el trabajo, la identificación de peligros y valoración de riesgos se realiza para las actividades desarrolladas en la sede de la Agencia Presidencial de Cooperación internacional y se utilizan herramientas tales como:

- Inspecciones: puesto de trabajo, áreas comunes y zonas especiales. Ver 4.5.

- Estadísticas: actos y condiciones inseguras, incidentes, enfermedades laborales, enfermedad general, ausentismo y comisiones al interior y exterior del país. La persona encargada del tema de seguridad y salud en el trabajo deberá realizar estadísticas de:
  - Índice de frecuencia de accidentes de trabajo.
  - Índice de severidad de accidentes de trabajo.
  - Índice de lesiones incapacitantes de accidentes de trabajo.
  - Tasa de ausentismo por accidentes de trabajo y enfermedad laboral o general.
  - Investigaciones de accidentes de trabajo.

[17] Requerido por la Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública. Pág. 23.

- Eficacia del Sistema de Gestión en Seguridad y Salud en el Trabajo.

- Diagnóstico de las condiciones de salud y de trabajo: corresponde a la consolidación de los resultados de la práctica de exámenes médicos laborales a funcionarios, independientemente de su forma de contratación o vinculación, incluyendo contratistas y subcontratistas, identificando las áreas y poblaciones con mayor incidencia de afectación de la salud.

b) En ambiental, la identificación de riesgos se apoya en:
- Diagnóstico de la gestión ambiental realizado dentro del PIGA.
- Estadísticas de consumo y gestión ambiental.

c) En contractual, la identificación de riesgos se apoya en:
- Gestión de cada dependencia para analizar los riesgos de cada objeto contractual.
- Aplicación del manual de riesgos de contratación.

d) En seguridad de la información, la identificación de riesgos se apoya en:
- Los incidentes que se reportan en la entidad a través del Itop.
- Los activos de información, con los tipos que se describen a continuación:

Tabla 17. Activos de información para riesgos de seguridad de la información

SIGLA	Tipo de Activo
D	Datos o Información ejemplo (Backup, Log, datos de configuración, etc.)
S	Servicios (Correo electrónico. internet etc.)
SW	Software
HW	Hardware
CO	Comunicaciones
MEDIA	Soporte de Información
AU	Auxiliar
L	Instalaciones (donde se hospedan los sistemas de información y comunicaciones)
P	Personal
IN	Información
PE	Personas
SE	Servicios
LO	Locaciones (Instalaciones)

Fuente: Modelo MAGERIT.

Del mismo modo debe ser considerada la clasificación de los activos, a saber:

Tabla 18. Criterios de clasificación de los activos de información para riesgos de seguridad de la información

Confidencialidad	Integridad	Disponibilidad
Información pública reservada	ALTA (A)	ALTA (A)
Información pública clasificada	MEDIA (M)	MEDIA (M)
Información pública	BAJA (B)	BAJA (B)
No clasificada	No clasificada	No clasificada

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

Los niveles de clasificación de dichos criterios son:

Tabla 19. Niveles de clasificación de los activos de información

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

En este sentido la descripción de los riesgos de seguridad de la información contará con lo siguiente:

Tabla 20. Dimensiones de Valoración para los riesgos de seguridad de la información

Tipos de Amenazas	Descripción del Tipo de Amenaza	Tipo de Activo									Origen			Dimensión		
		D	S	SW	HW	CO	MEDIA	AU	L	P	Accidentales	Deliberadas	Entorno	Disponibilidad	Integridad	Confidencialidad
Desastres Naturales	Daños por Agua				X		X	X	X		X			X		
De Origen Industrial	Fuego				X		X	X			X	X	X	X		
	Daños por Agua				X		X	X	X		X	X	X	X		
	Avería de Origen físico o Lógico			X	X		X	X			X	X	X	X		
	Corte del suministro eléctrico				X			X			X	X	X	X		
	Condiciones inadecuadas de temperatura o humedad				X			X			X	X	X	X		
	Fallos de Servicios de Comunicaciones					X					X	X	X	X		
	Interrupciones de otros servicios y suministro							X			X	X	X	X		
	Degradación de los soportes de almacenamiento de la Información						X				X	X	X	X		
Errores y fallos No Intencionados	Errores de los Usuarios	X	X	X			X				X			X	X	X
	Errores del administrador	X	X	X	X	X	X				X			X	X	X
	Errores de Monitorización	X									X				X	
	Errores de Configuración	X									X				X	
	Difusión de [SW] dañino			X							X			X	X	X
	Alteración accidental de la información	X					X				X				X	
	Destrucción de información	X									X			X		
	Fuga de Información	X	X	X		X	X		X	X	X					X
	Vulnerabilidades de los Programas			X							X			X	X	X
	Errores de Mantenimiento			X							X			X	X	
	Errores de mantenimiento / Actualización de Equipos (HW)				X		X	X			X			X		
	No identificación de Necesidades Tecnológicas	X	X	X	X	X		X	X				X	X	X	X
	Caída del Sistema por agotamiento de Recursos		X		X	X					X			X		
	Pérdida de Equipo		X		X			X			X			X		X
	Indisponibilidad del Personal									X	X			X		
Ataques Intencionados	Manipulación de los Registros de Actividad (log)	X										X			X	
	Manipulación de la Configuración	X										X			X	
	Suplantación de la Identidad del usuario	X	X	X	X	X						X		X	X	X
	Abuso de privilegios de Acceso	X	X	X	X	X	X					X		X	X	X
	Uso no Previsto		X	X	X	X						X		X	X	X
	Difusión de Software Dañino			X								X		X	X	X
	Acceso no Autorizado	X	X	X	X	X		X	X			X			X	X
	Destrucción de información	X	X	X	X	X		X	X			X			X	X
	Modificación deliberada de la información	X	X	X		X	X		X			X				X
	Divulgación de Información	X	X	X		X	X		X			X				
	Manipulación de Programas			X								X		X	X	X
	Manipulación de los Equipos				X		X	X				X		X		X
	Denegación de Servicio		X		X	X						X		X		
	Robo				X		X					X		X		X
	No identificación de Necesidades Tecnológicas	X	X	X	X	X		X	X				X	X	X	X

Fuente: Modelo MAGERIT.

f) En los demás sistemas de gestión, se utilizan mesas de trabajo en las cuales los participantes identifican y registran los riesgos.

6.5 Clasificación de riesgos

a) Los riesgos, de manera general, pueden ser, entre otras, de una o más de las siguientes clases:

Tabla 21. Clases de riesgos

Riesgo	Definición
Ambiental	Posibilidad de que se produzca un daño o catástrofe en el medio ambiente debido a un fenómeno natural o a una acción humana. Posibilidad de afectar desfavorablemente el medio ambiente.
Contractual	Entendido como todas aquellas circunstancias que pueden presentarse durante el desarrollo o ejecución de un contrato y que pueden alterar el equilibrio financiero del mismo.[18]
De calidad	Posibilidad de incumplir expectativa o necesidad del usuario.
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.
De Imagen	Está relacionado con la percepción y la confianza por parte de la ciudadanía hacia la institución
De Proyecto	Relacionado con los proyectos que adelanta la entidad o con aquellos en los cuales hace parte o aporta recursos.
De Salud y Seguridad Laboral	Posibilidad de afectar la salud del personal que labora o visita la entidad y/o de ser víctimas de acontecimientos delictivos o de la fuerza de la naturaleza.
De seguridad de la información	Posibilidad de vulnerar, adulterar, enmendar, cambiar o acceder sin autorización la información de la Agencia.
Documental	Posibilidad de vulnerar, adulterar, enmendar, cambiar o acceder sin autorización la información de la Agencia.
Estratégico	Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico 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 gerencia. Eventos que se pueden presentar y afectar el logro de la misión, los objetivos y metas institucionales.
Financiero	Relación con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
Legal	Surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones. Incluye los de daño antijurídico.
Locativo	Relacionado con las instalaciones y las condiciones físicas.
Lógico	Son aquellos daños que el equipo puede sufrir en su estado lógico, perjudicando directamente a su software.
Operativo	Comprende 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.
Tecnológico	Relacionado con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Fuente: Guía del Departamento Administrativo de la Función Pública DAFP para la administración del riesgo

[18] Documento CONPES 3714 /2011

b) Los riesgos, respecto de sus controles, pueden ser:

Tabla 22. Clasificación de riesgos respecto de sus controles

Riesgo	Definición
Inherente	Está relacionado con la naturaleza propia de la gestión y/o de la actividad, sin tener en cuenta el efecto de los controles. Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
Residual	Está igualmente relacionado con la naturaleza propia de la gestión, pero teniendo en cuenta el efecto de los controles. Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

Fuente: Guía para la administración del riesgo.

c) Los riesgos, por su naturaleza, son:

Tabla 23. Clasificación de riesgos respecto de su naturaleza

Riesgo	Definición
Común	Derivado de la situación.
De corrupción[19]:	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 o de un tercero.

Fuente: Estrategias para la construcción del Plan Anticorrupción y Atención al Ciudadano.

d) Los riesgos, según la causa de la corrupción, son:

Tabla 24. Matriz de definición del riesgo de corrupción

Componente	si	no
Acción u omisión		
Uso indebido de poder		
Desviación de la gestión de lo público		
Beneficio privado		
Total		

Fuente: Guía para la Administración del Riesgo de Corrupción 2015. Departamento Administrativo de la Función Pública
https://www.funcionpublica.gov.co/guias
http://www.funcionpublica.gov.co/documents/418537/616038/GUIA+PARA+LA+GESTION+DE+RIESGO+DE+CORRUPCION+%282%29.pdf/e301def2-8218-4205-a320-99c3ef9989f6

e) Los riesgos, por el daño en los activos de información, pueden ser:

Tabla 25. Clasificación de riesgos respecto del daño en los activos de información

	Tipo
A	Natural
	Humano
B	Accidentales
	Deliberadas

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

[19] Estrategias para la construcción del Plan Anticorrupción y Atención al Ciudadano. Pág. 9

f) Los peligros de seguridad y salud en el trabajo, pueden ser:

Tabla 26. Peligro y factores de riesgo de salud y seguridad laboral

Clasificación del peligro	Peligro
Biológico	Virus
	Bacterias
	Hongos
	Ricketsias
	Parásitos
	Picaduras
	Mordeduras
	Fluidos o excrementos
Físico	Ruido (Impacto intermitente y continuo)
	Iluminación (Luz visible por exceso o por deficiencia)
	Vibración (Cuerpo entero, segmentaria)
	Temperatura extremas (Calor o frío)
	Radiaciones ionizantes (Rayos x gamma beta y alfa)
	Radiaciones no ionizantes (láser ultravioleta infrarroja)
Químico	Polvos orgánicos e inorgánicos
	Fibras
	Líquidos
	Gases y vapores
	Humos metálicos, no metálicos
	Material particulado
Psicosocial	Gestión organizacional (inducción, capacitación, evaluación de desempeño, manejo de cambios
	Características de la organización del trabajo
	Condiciones de la tarea (carga mental, contenido de la tarea, demandas emocionales, sistema de control, definición de roles
	Jornada de trabajo
Biomecánicos	Postura prolongada mantenida, forzada, antigravitacionales
	Esfuerzo
	Movimiento repetitivo
	Manipulación manual de cargas
Condiciones de seguridad	Mecánico
	Eléctrico
	Locativo
	Tecnológico
	Accidentes de transito
	Públicos (robos, atracos, asaltos, atentados, desorden público)
Fenómenos naturales	Sismo
	Terremoto
	Vendaval
	Precipitaciones(lluvias, granizadas, heladas)

Fuente: Matriz de peligros y factores de riesgo de salud y seguridad laboral A-OT-044

g) Los riesgos, según la actividad contractual, pueden ser:

Tabla 27. Riesgos, respecto de la gestión contractual

Riesgo	Definición
Previsibles	Aquellas circunstancias que tienen la potencialidad de alterar el equilibrio financiero del mismo, siempre que sean identificables y cuantificables.
Cubiertos bajo el régimen de garantías en la contratación pública	Son aquellos relacionados y respaldados con las garantías de seriedad de la oferta, el cumplimiento de las obligaciones contractuales, la responsabilidad extracontractual que pueda surgir para la administración por las actuaciones, hechos u omisiones de sus contratistas o subcontratistas; y de forma general, los demás riesgos a que se encuentre expuesta la administración según el tipo de contrato, de acuerdo a lo dispuesto en el artículo 7 de la Ley 1150 de 2007.
Imprevisibles	Es aquel riesgo que se puede presentar de forma inesperada al ejecutar un contrato, como, por ejemplo: un suceso que se produce después de celebrado el contrato cuya ocurrencia no era previsible al momento de suscribirlo; una situación preexistente al contrato que se desconocía por las partes sin que le sea imputable a ninguna de ellas; y un suceso previsto, cuyos efectos dañinos para el contrato resultan ser tan diferentes de los planeados, que se vuelve irresistible.
Obligaciones Contingentes	Son aquellas obligaciones en virtud de las cuales una entidad estipula contractualmente a favor de su contratista el pago de una suma de dinero, determinada o determinable a partir de factores identificados por la ocurrencia de un evento futuro e incierto. A diferencia de los riesgos antes enunciados, tienen un proceso de gestión especial, desde la identificación y valoración, hasta la mitigación y el seguimiento. En todo caso, se aclara que puede haber riesgos previsibles que correspondan a obligaciones contingentes, pero no todas las obligaciones contingentes son riesgos previsibles.
Generados Por Malas Prácticas	Son aquellos sucesos que pueden ocasionarse por acciones negativas en la contratación o por riesgos operacionales, que se manifiestan durante el proceso precontractual y que afectan la ejecución del contrato.
Económicos	Son aquellos que se derivan del comportamiento del mercado, tales como la fluctuación de los precios de los insumos, desabastecimiento y especulación de los mismos, entre otros.
Sociales o Políticos	son aquellos que se derivan por cambios de las políticas gubernamentales que sean probables y previsibles, tales como cambios en la situación política, sistema de gobierno y cambio en las condiciones sociales que tengan impacto en la ejecución del contrato.
Operacionales	Son aquellos riesgos asociados a la operatividad del contrato, en cualquiera de sus fases.
Financieros	Este riesgo tiene dos componentes básicos: el riesgo de consecución de financiación o riesgo de liquidez, y el riesgo de las condiciones financieras.
Regulatorios	Son los posibles cambios regulatorios o reglamentarios que siendo previsibles, afecten el equilibrio contractual.
De La Naturaleza	Son los eventos causados por la naturaleza sin la intervención o voluntad del hombre, que, aunque pueden ser previsibles por su frecuencia o diagnóstico, están fuera del control de las partes.
Ambientales	Se refiere a las obligaciones que emanan de las licencias ambientales, de los planes de manejo ambiental, de las condiciones ambientales o ecológicas exigidas y de la evolución de las tasas retributivas y de uso del agua. Por ejemplo, cuando durante la ejecución del contrato se configuren pasivos ambientales causados por mala gestión de la licencia ambiental y/o el plan de manejo ambiental o el costo de las obligaciones ambientales resulte superior al estimado no siendo imputables a las partes.
Tecnológicos	Se refiere a eventuales fallos en las telecomunicaciones, suspensión de servicios públicos, advenimiento de nuevos desarrollos tecnológicos o estándares que deben ser tenidos en cuenta para la ejecución del contrato así como la obsolescencia tecnológica.

Fuente: Conpes 3714.

h) Los riesgos, según los eventos de seguridad de la información, pueden ser:

Tabla 28. Riesgos más comunes de seguridad de la información

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
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Pérdida 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
	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
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

i) Los riesgos, según el daño antijurídico, pueden ser:

Tabla 29. Riesgos, en daño antijurídico

RIESGO IDENTIFICADO	DESCRIPCIÓN
Estudios previos y/o pre pliegos de condiciones elaborados para favorecer a un oferente en particular	Beneficiar a un oferente en particular mediante la elaboración de los estudios previos, pre-pliegos de condiciones o invitaciones a ofertar de un proceso de selección
Decisiones erróneas en la selección y vinculación de personal	Realizar selección y vinculación de personal sin el cumplimiento de los requisitos legales exigidos para el cargo.
Incumplimiento en los compromisos financieros adquiridos por la entidad	No tramitar, registrar y pagar los compromisos financieros que adquiere la entidad
No se evidencian a tiempo riesgos financieros asociados al manejo de las cuentas bancarias.	No realizar de forma mensual el proceso de conciliación bancaria aumenta el riesgo de no identificar de manera oportuna los hechos financieros que afectan las cuentan bancarias de la entidad
Liquidaciones inexactas derivadas del procesamiento de la nómina.	El pago de la nómina y los demás emolumentos se realizan de forma inexacta o fuera del tiempo previsto por la Ley.
Ejecución del contrato sin el cumplimiento de requisitos legales.	Perfeccionar un contrato, convenio sin el cumplimiento de los requisitos legales.

Fuente: política de prevención de daño antijurídico Código: A-OT-015 - Versión: 04 – Fecha: abril 03 de 2017

6.6 Descripción del riesgo

Se detalla o define el riesgo para ofrecer una imagen o una idea completa de él[20].

6.7 Análisis de causas y consecuencias

Una vez identificado el riesgo, deben analizarse todas esas situaciones que lo pueden generar, así mismo los efectos que puede producir si se llega a materializar.

6.8 Análisis del riesgo

El análisis del riesgo[21] busca establecer qué tan probables que el riesgo se materialice y que tan grave sería el impacto si se llega a materializar.

Este análisis puede resultar subjetivo en la medida que un mismo evento puede ser no deseable para alguien, pero bienvenido para alguien más. Por ejemplo, un cambio de personal

[20] Guía Administración del Riesgo. Departamento Administrativo de la Función Pública. pág. 14
[21] Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública. Pág. 26

podría ser evaluado como un riesgo por cuanto podría afectar la continuidad de la gestión, pero podría no serlo si dicho cambio representa una medida para eliminar la corrupción en un asunto. Por ello es recomendable que no sea una única persona quien haga este análisis, sino que se haga de forma consensuada.

Existen dos aspectos a tener en cuenta en el análisis de los riesgos identificados: Probabilidad e Impacto.

6.8.1 Probabilidad

Es la posibilidad de ocurrencia del riesgo. La escala aplicable se muestra a continuación:

a) Escala de Probabilidad para riesgos de salud y seguridad laboral.

Tabla 30. Escala de Probabilidad para riesgos de salud y seguridad laboral

Nivel de probabilidad	Valor de NP	Significado
Muy Alto (MA)	Entre 40 y 24	Situación deficiente con exposición continua, o muy deficiente con exposición frecuente. Normalmente la materialización del riesgo ocurre con frecuencia.
Alto (A)	Entre 20 y 10	Situación deficiente con exposición frecuente u ocasional, o bien situación muy deficiente con exposición ocasional o esporádica. La materialización del Riesgo es posible que suceda varias veces en la vida laboral
Medio (M)	Entre 8 y 6	Situación deficiente con exposición esporádica, o bien situación mejorable con exposición continuada o frecuente. Es posible que suceda el daño alguna vez.
Bajo (B)	Entre 4 y 2	Situación mejorable con exposición ocasional o esporádica, o situación sin anomalía destacable con cualquier nivel de exposición. No es esperable que se materialice el riesgo, aunque puede ser concebible.

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.

b) Escala de Probabilidad para riesgos contractuales.

Tabla 31. Escala de Probabilidad para riesgos contractuales

valoración	Categoría	Descripción
1	Raro	Puede ocurrir excepcionalmente.
2	Improbable	Puede ocurrir ocasionalmente
3	Posible	Puede ocurrir en cualquier momento futuro.
4	Probable	Probablemente va a ocurrir.
5	Casi Cierto	Ocurre en la mayoría de las circunstancias.

c) Escala de Probabilidad para riesgos de los demás sistemas de gestión

Tabla 32. Escala de Probabilidad aplicable a otros sistemas de gestión

Nivel	Probabilidad	Descripción	Frecuencia
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Se ha presentado más de una vez al año.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Se ha presentado al menos de una vez en el último año.
3	Posible	El evento podría ocurrir en algún momento	Se ha presentado al menos de una vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Se ha presentado al menos de una vez en los últimos 5 años.
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública https://www.funcionpublica.gov.co/guias

En términos generales, la probabilidad se mide con criterios de:

- Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o
- Factibilidad, teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

6.8.2 Impacto

Es la gravedad de las consecuencias que puede ocasionar la materialización del riesgo a la organización. La escala aplicable se muestra a continuación:

a) Escala de impacto para riesgos de corrupción.

El impacto[22] de la materialización de un riesgo de corrupción es único, por cuanto lesiona la imagen, credibilidad, transparencia y la propiedad de las entidades y del Estado, afectándolos recursos públicos, la confianza y el cumplimiento de las funciones de la administración, siendo por tanto inaceptable la materialización de un riesgo de corrupción.

Si se trata de un riesgo de corrupción, el mecanismo para determinar el impacto que le aplica consiste en responder a las 18 preguntas siguientes:

[22] Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano. Secretaria de Transparencia. Presidencia de la Republica2012. Pág. 12.

Tabla 33. Preguntas para determinar el impacto en un riesgo de corrupción

Nª	Si el riesgo de corrupción se materializa, podría	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 sectorial que pertenece la entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afecta la generación de los productos o la prestación de servicios?		
8	¿Da 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	¿Generar pérdida de credibilidad del sector?		
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?		
	Total		

Fuente: Guía para la gestión de Riesgo de Corrupción.
https://www.funcionpublica.gov.co/guias

La suma de las respuestas ubica el riesgo en la siguiente clasificación:

Tabla 34. Clasificación del impacto de riesgos de corrupción

Preguntas respondidas con “si”	Impacto	Nivel	Aplica cuando
1 a 5	Moderado	05	• Afectación parcial al proceso y a la dependencia. • Genera medianas consecuencias para la entidad.
6 a 11	Mayor	10	• Impacto negativo en la entidad. • Genera altas consecuencias para la entidad.
12 a 18	Catastrófico	20	• Consecuencias desastrosas para el sector. • Genera desastrosas consecuencias para la entidad.

Fuente: Guía para la Administración del Riesgo de Corrupción. Departamento Administrativo de la Función Pública
https://www.funcionpublica.gov.co/guias

b) Escala de impacto para riesgos de seguridad y salud laboral.

Tabla 35. Escala de impacto (consecuencias) para riesgos de seguridad y salud laboral

Nivel de Consecuencias	NC	Significado Daños Personales
Mortal o Catastrófico (M)	100	Muerte (s)
Muy grave (MG)	60	Lesiones o enfermedades graves irreparables (Incapacidad permanente parcial o invalidez).
Grave (G)	25	Lesiones o enfermedades con incapacidad laboral temporal (ILT).
Leve (L)	10	Lesiones o enfermedades que no requieren incapacidad.

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.

c) Escala de impacto para riesgos contractuales.

Tabla 36. Escala de impacto (consecuencias) para riesgos contractuales

Clasificación cualitativa	Obstruye la ejecución del contrato de manera intrascendente.	Dificulta la ejecución del contrato de manera baja. Aplicando medidas mínimas se puede lograr el objeto contractual.	Afecta la ejecución del contrato sin alterar el beneficio de las partes.	Obstruye la ejecución del contrato sustancialmente pero aun así permite la consecución del objeto contractual.	Perturba la ejecución del contrato de manera grave imposibilitando la consecución del objeto contractual
Clasificación monetaria	Los sobrecostos no representan más del uno por ciento (1%) del valor del contrato.	Los sobrecostos no representan más del cinco por ciento (5%) del valor del contrato.	Genera un impacto sobre el valor del contrato entre el cinco (5%) y el quince por ciento (15%).	Incrementa el valor del contrato entre el quince (15%) y el treinta por ciento (30%).	Impacto sobre el valor del contrato en más del treinta por ciento (30%).
Categoría	**Insignificante**	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Valoración	**1**	**2**	**3**	**4**	**5**

d) Escala de impacto para riesgos de seguridad de la información.

Se mide teniendo en cuenta la confidencialidad de la Información, así

Tabla 37. Impacto Sobre la Confidencialidad de la Información

Nivel	Concepto
1	Personal
2	Grupo de trabajo
3	Relativa al proceso
4	Institucional
5	Estratégica

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

e) Escala de impacto para riesgos ambientales.

Tabla 38. Escala de impacto (consecuencias) para riesgos ambientales

Valor	Sobre el entorno humano				Sobre el entorno natural			
	Cantidad	Peligrosidad	Extensión	Población afectada	Cantidad	Peligrosidad	Extensión	Población afectada
4	Muy alta	Muy peligrosa	Muy extenso	Muy Alto	Muy alta	Muy peligrosa	Muy extenso	Muy elevada
3	Alta	Peligrosa	Extenso	Alto	Alta	Peligrosa	Extenso	Elevada
2	Poca	Poco peligrosa	Poco extenso	Bajo	Poca	Poco peligrosa	Poco extenso	Media
1	Muy poca	No peligrosa	Puntual	Muy bajo	Muy poca	No peligrosa	Puntual	Baja

Fuente: norma española UNE 150008 2008 - Evaluación de riesgos ambientales.

f) Escala de impacto para riegos de los demás sistemas de gestión.

Tabla 39. Escala de impacto para riegos de los demás sistemas de gestión

		Cuantitativo				Cualitativo			
Nivel	Impacto	Afecta la ejecución presupuestal en:	Pérdida de cobertura en la prestación de los servicios de la entidad	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en	Pago de sanciones por incumplir normatividad aplicable ante un ente regulador, que afectan el presupuesto general de la entidad en:	Interrupción de las operaciones de la Entidad	Pérdida de Información crítica para la entidad	Imagen institucional afectada	Otras
5	Catastrófico	≥50%.	≥50%.	≥50%	≥50%	Más de cinco (5) días.	No se puede recuperar.	En el orden nacional o regional, por actos o hechos de corrupción comprobados.	• Intervención por parte de un ente de control u otro ente regulador. • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.
4	Mayor	≥20%.	≥20%.	≥20%	≥20%	Más de dos (2) días.	Puede ser recuperada de forma parcial o incompleta.	En el orden nacional o regional, por incumplir la prestación del servicio a los usuarios o ciudadanos.	• Sanción del ente de control o regulador. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.
3	Moderado	≥5%	≥10%.	≥5%	≥5%	Por un (1) día.	No aplica	En el orden nacional o regional, por retrasos en la prestación del servicio a los usuarios o ciudadanos.	• 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. • Investigaciones penal, fiscal o disciplinaria.
2	Menor	≤1%	≤5%.	≤1%	≤1%	Por algunas horas.	No aplica	Localmente, por retrasos en la prestación del servicio a los usuarios o ciudadanos.	• Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.
1	Insignificante	≤0,5%	≤1%.	≤0,5%	≤0,5%	No hay interrupción	No aplica	No se afecta de forma significativa.	• No se generan sanciones económicas o administrativas.

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública
https://www.funcionpublica.gov.co/guias

6.9 Criticidad del riesgo

La criticidad de cualquier riesgo resulta de combinar la probabilidad con el impacto. Esta criticidad se visualiza a través de una matriz o mapa de calor, que APC-Colombia administra con las siguientes convenciones:

B. Zona de Riesgo Baja.
M. Zona de Riesgo Moderada.
A. Zona de Riesgo Alta.
E. Zona de Riesgo Extrema.

La matriz o mapa de calor tiene diferencias de un sistema de gestión a otro. En APC-Colombia aplican los siguientes:

a) Criticidad para el riesgo de corrupción:

Tabla 40. Matriz de calor de un riesgo de corrupción

PROBABILIDAD	Casi Seguro (5)	M (25)	A (50)	E (100)
	Probable (4)	M (20)	A (40)	E (80)
	Posible (3)	M (15)	A (30)	E (60)
	Improbable (2)	B (2)	M (20)	A (40)
	Raro (1)	B (5)	B (10)	M (20)
	IMPACTO	Moderado (I3 = 5)	Mayor (I4 = 10)	Catastrófico (I5 = 20)

Fuente: Guía para la gestión de Riesgo de Corrupción.
https://www.funcionpublica.gov.co/guias

b) Criticidad para el riesgo contractual:

Tabla 41. matriz de calor de un riesgo contractual

			IMPACTO				
			Insignificante	Menor	Moderado	Mayor	Catastrófico
	Categoría	**Valoración**	**1**	**2**	**3**	**4**	**5**
PROBABILIDAD	Raro	**1**	2	3	4	5	6
	Improbable	**2**	3	4	5	6	7
	Posible	**3**	4	5	6	7	8
	Probable	**4**	5	6	7	8	9
	casi cierto	**5**	6	7	8	9	10

Fuente: Manual De Riesgos A-OT-022

En estos casos, el significado del nivel de riesgo es:

VALORACIÓN DEL RIESGO	8, 9 Y 10	Riesgo Extremo
	6 y 7	Riesgo Alto
	5	Riesgo Medio
	2, 3 y 4	Riesgo Bajo

c) Criticidad para el riesgo de salud y seguridad laboral:

Tabla 42. Matriz de calor de los riesgos de salud y seguridad laboral

Nivel de riesgo NR = NP x NC		Nivel de Probabilidad (NP)			
		40-24	20-10	8-6	4-2
Nivel de consecuencias (NC)	100	I 4000-2400	I 2000-1200	I 800-600	II 400-200
	60	I 2400-1440	I 1200-600	II 480-360	II 240 / III 120
	25	I 1000-600	II 500-250	II 200-150	III 100-50
	10	II 400-240	II 200 / III 100	III 80-60	III40 / IV 20

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.

En estos casos, el significado del nivel de riesgo y de intervención es:

Tabla 43. Significado del nivel de riesgo y de intervención salud y seguridad laboral

Nivel	Valor de NR	Significado
I	4000-600	Situación crítica. Suspender actividades hasta que el riesgo esté bajo control. Intervención urgente.
II	500 – 150	Corregir y adoptar medidas de control de inmediato.
III	120 – 40	Mejorar si es posible. Sería conveniente justificar la intervención y su rentabilidad
IV	20	Mantener las medidas de control existentes, pero se deberían considerar soluciones o mejoras y se deben hacer comprobaciones periódicas para asegurar que el riesgo aún es aceptable.

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.

d) Criticidad para el riesgo de seguridad de la información

Tabla 44. matriz de calor de un riesgo de seguridad de la información

			IMPACTO				
			Insignificante	Menor	Moderado	Mayor	Catastrófico
	Categoría	**Valoración**	**1**	**2**	**3**	**4**	**5**
PROBABILIDAD	Raro	**1**	B	B	M	A	A
	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

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

e) Criticidad para el riesgo de los demás sistemas de gestión y daño antijurídico.

Tabla 45. matriz de calor de los demás sistemas de gestión

PROBABILIDAD	Casi Seguro (5)	A (5)	A (10)	E (15)	E (20)	E (25)
	Probable (4)	M (4)	A (8)	A (12)	E (16)	E (20)
	Posible (3)	B (3)	M (6)	A (9)	E (12)	E (15)
	Improbable (2)	B (2)	B (4)	M (6)	A (8)	E (10)
	Raro (1)	B (1)	B (2)	M (3)	A (4)	E (5)
	IMPACTO	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)

Fuente: Guía para la gestión de Riesgo de Corrupción.
https://www.funcionpublica.gov.co/guias

6.10 Identificación de controles

En la identificación de controles la entidad adelanta, principalmente, los siguientes aspectos:

A) Estado

Parte del análisis implica establecer si se cuenta o no con controles, y la utilidad de los mismos, así:

Tabla 46. Estado de los controles

Estado de los controles:
No existen
No efectivos y no documentados
No Efectivos y documentados
Efectivos y no documentados
Efectivos y documentados
Documentados, efectivos y aplicados

B) Aspectos de selección

La selección de los controles implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deberá considerar aspectos como:

Tabla 47. Aspectos para la selección de controles

Aspecto	Definición	Aplicable a
Viabilidad jurídica	Velar por que los controles que se van a implantar no vayan en contra de la normatividad vigente.	Todos los sistemas de gestión
Viabilidad técnica e institucional	Establecer claramente si la entidad está en capacidad de implantar y sostener a largo plazo nuevas tecnologías u otros mecanismos necesarios para ejecutar el control.	
Análisis de costo-beneficio	Prácticamente todas las respuestas a los riesgos implican algún tipo de costo directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el costo inicial del diseño e implementación de una respuesta (procesos, personal, tecnología), así como el costo de mantener la respuesta de forma continua. Este caso se puede dar específicamente para aquellos controles nuevos que requieren contrataciones adicionales a los funcionarios que desarrollan los proceso o bien cuando se requiere diseñar e implementar sistemas de información o tecnologías específicas para ejecutar el control.	
Número de trabajadores expuestos	Importante tenerlo en cuenta para identificar el alcance del control a implementar.	Sistema de gestión de seguridad y salud laboral
Peor consecuencia	Aunque se han identificado los efectos posibles, se debe tener en cuenta que el control a implementar evite siempre la peor consecuencia al estar expuesto al riesgo.	
Existencia requisito legal asociado	La organización podría establecer si existe o no un requisito legal específico a la tarea que se está evaluando para tener parámetros de priorización en la implementación de las medidas de intervención.	

Fuente1: Guía para la Administración del Riesgo v3 Departamento Administrativo de la Función Pública - Dirección de Control Interno y Racionalización de Trámites Bogotá, D.C., Octubrede2014
Fuente 2: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional.
Fuente 3: Guía Técnica Colombiana GTC 45.

C) Tipo de Control.

Para cada riesgo es necesario establecer el(los) control(es) que está(n) implementado(s). Los controles tienen las siguientes clasificaciones:

Tabla 48. Clasificación de los controles

Clasificación por	Tratamiento	Definición
Naturaleza	Preventivo	Aquel que actúa para eliminar las causas del riesgo para prevenir su ocurrencia o materialización. Su presencia reduce la probabilidad de ocurrencia. Evitan que un evento suceda. Por ejemplo, el requerimiento de un login y password en un sistema de información es un control preventivo. Éste previene (teóricamente) que personas no autorizadas puedan ingresar al sistema. Dentro de esta categoría pueden existir controles de tipo detectivo, por ejemplo, registro de las entradas de todas las actividades llevadas a cabo en el sistema de información, traza de los registros realizados, de las personas que ingresaron, entre otros.
	Correctivo	Aquel que permite el restablecimiento de actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia. Su presencia reduce el impacto. Éstos no prevén que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Por ejemplo en caso de un desastre natural u otra emergencia mediante las pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, es posible volver a recuperar las operaciones.
	Detectivo	Aquel que registra un evento después de presentado; sirve para descubrir resultados no previstos y alertar sobre la presencia de un riesgo. Se aplica en los riesgos de corrupción.
Clase	Manual	Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeos, controles de seguridad con personal especializado entre otros.
	Automático	Utilizan herramientas tecnológicas como sistemas de información o software, diseñados para prevenir, detectar o corregir errores o deficiencias, sin que tenga que intervenir una persona en el proceso.
Jerarquía de salud y seguridad laboral	Eliminación	Modificar un diseño para eliminar el peligro, por ejemplo, introducir dispositivos mecánicos de alzamiento para eliminar el peligro de manipulación manual.
	Sustitución	Reemplazar por un material menos peligroso o reducir la energía del sistema (por ejemplo, reducir la fuerza, el amperaje, la presión, la temperatura, etc.).
	Controles de ingeniería	Instalar sistemas de ventilación, protección para las máquinas, enclavamiento, cerramientos acústicos, etc.
	Controles administrativos	Señalización, advertencias: instalación de alarmas, procedimientos de seguridad, inspecciones de los equipos, controles de acceso, capacitación del personal
	Equipos / elementos de protección	Gafas de seguridad, protección auditiva, máscaras faciales, sistemas de detención de caídas, respiradores y guantes.
Vulnerabilidad de controles de seguridad de la información	Física	Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema. Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.
	Natural	Las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos. Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo

Clasificación por	Tratamiento	Definición
		no disponer de reguladores, no-breaks, mal sistema de ventilación o calefacción, etc.
	Hardware	Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema
	Software	Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo, controles de acceso, seguridad, implantación, etc.). Ambos factores hacen susceptible al sistema a las amenazas de software.
	Red	Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto. En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio. Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.
	Factor Humano	Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema. Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo.

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública
Fuente: Guía para la gestión de Riesgo de Corrupción. https://www.funcionpublica.gov.co/guias
Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.
Fuente: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#16

Los puntos de control documentados en los diferentes procesos y procedimientos pueden ser considerados como controles del riesgo siempre que permitan obtener información para la toma de decisiones.

D) Controles posibles.

a) Posibles controles para los riesgos de seguridad de la información:

Tabla 49. Valoración de controles de seguridad de la información

Dominios	Control	Control de Referencia
A5 políticas de la seguridad de la información	A5.1Orientación de la dirección para la gestión de la seguridad de la información	A5.1.1 Políticas para la seguridad de la información
		A5.1.2 Revisión de las políticas para la seguridad de la información.
A6 organización de la seguridad de la información	A6.1Organización interna	A6.1.1 Roles y responsabilidades para la seguridad de la información
		A6.1.2 Separación de deberes
		A6.1.3 Contacto con las autoridades
		A6.1.4 Contacto con grupos de interés especial
		A6.1.5 Seguridad de la información en la gestión de proyectos.
	A6.2Dispositivos móviles y teletrabajo	A6.2.1 Política para dispositivos móviles
		A6.2.2 Teletrabajo
A7 seguridad de los recursos humanos	A7.1Antes de asumir el empleo	A7.1.1 Selección
		A7.1.2 Términos y condiciones del empleo
	A7.2Durante la ejecución del empleo	A7.2.1 Responsabilidades de la dirección
		A7.2.2 Toma de conciencia educación y formación en la seguridad de la información.
		A7.2.3 Proceso disciplinario
	A7.3Terminación y cambio de empleo	A7.3.1 Terminación o cambio de responsabilidades de empleo
A8 gestión de activos	A8.1Responsabilidad por los activos	A8.1.1 Inventario de activos
		A8.1.2 Propiedad de los activos
		A8.1.3 Uso aceptable de los activos
		A8.1.4 Devolución de activos
	A8.2Clasificación de la información	A8.2.1 Clasificación de la información
		A8.2.2 Etiquetado de la información
		A8.2.3 Manejo de activos
	A8.3Manejo de medios	A8.3.1 Gestión de medios removibles
		A8.3.2 Disposición de los medios
		A8.3.3 Transferencia de medios físicos
A9 control de acceso	A9.1Requisitos del negocio para el control de acceso	A9.1.1 Política de control de acceso
		A9.1.2 Acceso a redes y a servicios en red
	A9.2Gestión de acceso de usuarios	A9.2.1 Registro y cancelación del registro de usuarios
		A9.2.2 Suministro de acceso de usuarios
		A9.2.3 Gestión de derechos de acceso privilegiado
		A9.2.4 Gestión de información de autenticación secreta de usuarios
		A9.2.5 Revisión de los derechos de acceso de usuarios
		A9.2.6 Retiro o ajuste de los derechos de acceso
	A9.3Responsabilidades de los usuarios	A9.3.1 Uso de información de autenticación secreta
	A9.4Control de acceso a sistemas y aplicaciones	A9.4.1 Restricción de acceso a la información
		A9.4.2 Procedimiento de ingreso seguro
		A9.4.3 Sistema de gestión de contraseñas
		A9.4.4 Uso de programas utilitarios privilegiados
		A9.4.5 Control de acceso a códigos fuente de programas
A10 criptografía	A10.1Controles criptográficos	A10.1.1 Política sobre el uso de controles criptográficos
		A10.1.2 Gestión de llaves
	A11.1Áreas seguras	A.11.1.1 Perímetro de seguridad física
		A.11.1.2 Controles de Accesos Físicos

Dominios	Control	Control de Referencia
A11 seguridad física y del entorno		A.11.1.3 Seguridad de oficinas, recintos e instalaciones.
		A.11.1.4 Protección contra amenazas externas y ambientales.
		A.11.1.5 Trabajo en áreas seguras.
		A.11.1.6 Áreas de carga, despacho y acceso público
	A11.2Equipos	A11.2.1 Ubicación y protección de los equipos
		A11.2.2 Servicios de suministro
		A11.2.3 Seguridad en el cableado.
		A11.2.4 Mantenimiento de los equipos.
		A11.2.5 Retiro de activos
		A11.2.6 Seguridad de equipos y activos fuera de las instalaciones
		A11.2.7 Disposición segura o reutilización de equipos
		A11.2.8 Equipos de usuario desatendido
		A11.2.9 Política de escritorio limpio y pantalla limpia
A12 seguridad de las operaciones	A12.1Procedimientos operacionales y responsabilidades	A.12.1.1 Procedimientos de operación documentados
		A.12.1.2 Gestión de cambios
		A.12.1.3 Gestión de capacidad
		A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
	A12.2Protección contra códigos maliciosos	A.12.2.1 Controles Contra Código Maliciosos
	A12.3Copias de respaldo	A.12.3.1 Respaldo de la Información
	A12.4Registro y seguimiento	A.12.4.1 Registro de Eventos
		A.12.4.2 Protección de la Información de Registro
		A.12.4.3 Registros del Administrador y del Operador
		A.12.4.4 Sincronización de Relojes
	A12.5Control de software operacional	A.12.5.1 Instalación de software en sistemas operativos
	A12.6Gestión de la vulnerabilidad técnica	A.12.6.1 Gestión de las vulnerabilidades técnicas
		A.12.6.2Restricciones sobre la instalación de software
	A12.7Consideraciones sobre auditorias de sistemas de información	A.12.7.1 Controles de auditorías de sistemas de información
A13 seguridad de las comunicaciones	A13.1Gestión de la seguridad de las redes	A13.1.1 Controles de redes
		A13.1.2 Seguridad de los servicios red
		A13.1.3 Separación en las redes
	A13.2Transferencia de información	A13.2.1 Políticas y procedimientos de transferencia de información
		A13.2.2 Acuerdo transferencia de información
		A13.2.3 Mensajería Electrónica
		A13.2.4 Acuerdos de Confidencialidad o de no divulgación
A14 adquisición desarrollo y mantenimiento de sistemas	A14.1Requisitos de seguridad de los sistemas de información	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información
		A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas
		A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.
	A14.2Seguridad en los procesos de Desarrollo y de Soporte	A.14.2.1 Política de desarrollo seguro
		A.14.2.2 Procedimientos de control de cambios en sistemas
		A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
		A.14.2.4 Restricciones en los cambios a los paquetes de software
		A.14.2.5 Principio de Construcción de los Sistemas Seguros.
		A.14.2.6 Ambiente de desarrollo seguro

Dominios	Control	Control de Referencia
		A.14.2.7 Desarrollo contratado externamente
		A.14.2.8 Pruebas de seguridad de sistemas
		A.14.2.9 Prueba de aceptación de sistemas
	A14.3Datos de prueba	A.14.3.1 Protección de datos de prueba
A15 relaciones con los proveedores	A15.1Seguridad de la información en las relaciones con los proveedores.	A15.1.1 Política de seguridad de la información para las relaciones con proveedores
		A15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
		A15.1.3 Cadena de suministro de tecnología de información y comunicación
	A15.2Gestión de la prestación de servicios de proveedores	A15.2.1 Seguimiento y revisión de los servicios de los proveedores
		A15.2.2 Gestión del cambio en los servicios de los proveedores
A16 gestión de incidentes de seguridad de la información	A16.1Gestión de incidentes y mejoras en la seguridad de la información	A16.1.1 Responsabilidades y procedimientos
		A16.1.2 Reporte de eventos de seguridad de la información
		A16.1.3 Reporte de debilidades de seguridad de la información
		A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
		A16.1.5 Respuesta a incidentes de seguridad de la información
		A16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información
		A16.1.7 Recolección de evidencia
A17 aspectos de seguridad de la información de la gestión de continuidad de negocio	A17.1Continuidad de Seguridad de la información	A17.1.1 Planificación de la continuidad de la seguridad de la información
		A17.1.2 Implementación de la continuidad de la seguridad de la información
		A17.1.3 Verificación revisión y evaluación de la continuidad de la seguridad de la información
	A17.2Redundancias	A17.2.1 Disponibilidad de instalaciones de procesamiento de información
A18 cumplimiento	A18.1Cumplimiento de requisitos legales y contractuales	A18.1.1 Identificación de la legislación aplicable.
		A18.1.2 Derechos propiedad intelectual (DPI)
		A18.1.3 Protección de registros
		A18.1.4 Privacidad y protección de información de datos personales
		A18.1.5 Reglamentación de controles criptográficos.
	A18.2Revisiones de seguridad de la información	A18.2.1 Revisión independiente de la seguridad de la información
		A18.2.2 Cumplimiento con las políticas y normas de seguridad
		A18.2.3 Revisión del cumplimiento técnico

Fuente: Guía 8 de Mintic para la Seguridad y Privacidad de la información. Controles de Seguridad y Privacidad de la Información.

b) Posibles controles para los riesgos de los demás sistemas de gestión:

Tabla 50. Posibles controles para los riesgos de los demás sistemas de gestión

Control	Ejemplos
Políticas claras Aplicadas	Políticas claras aplicadas Seguimiento al plan estratégico y operativo Indicadores de gestión Tableros de control Seguimiento a cronograma Informes de gestión
Conciliaciones	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
Normas claras y Aplicadas	Normas claras y aplicadas Control de términos

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública
https://www.funcionpublica.gov.co/guias

E) Frecuencia. Debe establecerse en que periodos de tiempo se aplica el control.

6.11 Valoración de controles existentes

La valoración de los controles existentes se hace con relación a la existencia de la herramienta y al seguimiento que se le adelanta, con base en una calificación predeterminada, que permitirán ponderar de manera objetiva los controles y poder determinar el desplazamiento dentro de la Matriz de calificación, evaluación y respuesta a los riesgos.

a) Valoración general de controles

Tabla 51. Parámetros de valoración de controles

Criterios	Puntaje
¿El control previene la materialización del riesgo (afecta probabilidad) ¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?	0
¿Existen manuales, instructivos o procedimientos para el manejo del control?	15
¿Están definidos los responsables de la ejecución del control y del seguimiento?	5
¿El control es automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros).	15
¿El control es manual? (Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros)	10
La frecuencia de la ejecución del control y seguimiento es adecuada	15
¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10
En el tiempo que lleva la herramienta ha demostrado ser efectiva	30
Total	100

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública
Fuente: Guía para la gestión de Riesgo de Corrupción.
https://www.funcionpublica.gov.co/guias

b) Valoración de controles en los riesgos de corrupción

La calificación de controles en los riesgos de corrupción, a partir de la suma obtenida en la tabla anterior, se da de la siguiente manera:

Tabla 52. Calificación de los controles de los riesgos

Calificación	Puntaje/cuadrante a disminuir
0 a 50	0
51 a 75	1
76 a 100	2

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública
Fuente: Guía para la gestión de Riesgo de Corrupción.
https://www.funcionpublica.gov.co/guias

c) Valoración de controles en los riesgos de seguridad de la información.

Tabla 53. Parámetros de valoración de controles de seguridad de la información

	Criterios	Puntaje
Herramientas para ejercer el control	¿Posee una herramienta para ejercer el control	15
	¿Existen manuales, instructivos o procedimientos para el manejo de la herramienta?	15
	¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30
Seguimiento al control	¿Están definidos los responsables de la ejecución del control y del seguimiento?	15
	La frecuencia de la ejecución del control y seguimiento es adecuada	25
	Total	100

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

Para este último caso, el desplazamiento en la matriz de calor se hace como sigue:

Tabla 54. Desplazamiento en la matríz de calificación

Rango	Cuadrantes a disminuir en probabilidad	Cuadrantes a disminuir en impacto
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

6.12 Evaluación del riesgo

La evaluación del riesgo es el producto de confrontar los resultados del análisis del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas.

Es el equivalente a un nuevo análisis de la probabilidad e impacto del riesgo, pero teniendo en cuenta los controles existentes, que según sean preventivos o correctivos reclasificarán la criticidad del riesgo en el mapa de calor.

6.13 Identificación del tratamiento o intervención

Según quede evaluado el riesgo, y de su posición en el mapa de calor del riesgo residual, se determina el tratamiento que debe darse al mismo, con una y solo una de las siguientes opciones:

a) Tratamiento o intervención en riesgos de corrupción.

Tabla 55. Medidas de respuesta aplicables en cada zona de riesgo de corrupción

Tratamiento	Zona de riesgo en que aplica el tratamiento			
Tratamiento	Baja	Moderada	Alta	Extrema
Eliminar o reducir con los controles establecidos en la entidad	X			
Eliminar o llevar a zona baja		X		
Eliminar o llevar a zona moderada o baja			X	
Prioritario: Implementar controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomas las medidas de protección.				X

Fuente: Guía para la Gestión de Riesgo de Corrupción 2015, página 23. https://www.funcionpublica.gov.co/guias

b) Tratamiento o intervención en riesgos de salud y seguridad laboral.

Tabla 56. intervenciones en los riesgos de salud y seguridad laboral

Tratamiento	Definición
Eliminación	Modificar un diseño para eliminar el peligro, por ejemplo, introducir dispositivos mecánicos de alzamiento para eliminar el peligro de manipulación manual.
Sustitución	Reemplazar por un material menos peligroso o reducir la energía del sistema (por ejemplo, reducir la fuerza, el amperaje, la presión, la temperatura, etc.).
Controles de ingeniería	Instalar sistemas de ventilación, protección para las máquinas, enclavamiento, cerramientos acústicos, etc.
Controles administrativos	Señalización, advertencias: instalación de alarmas, procedimientos de seguridad, inspecciones de los equipos, controles de acceso, capacitación del personal
Equipos / elementos de protección	Gafas de seguridad, protección auditiva, máscaras faciales, sistemas de detención de caídas, respiradores y guantes.

Fuente: Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.

El seguimiento a los controles de la tabla anterior se opera a través de la Matriz de peligros de A-OT-044.

c) Tratamiento o intervención en riesgos de los demás sistemas de gestión.

Tabla 57. Medidas de respuesta aplicables en cada zona de riesgo de los demás sistemas de gestión.

Tratamiento		Zona de riesgo en que aplica el tratamiento			
Tratamiento	Definición	Baja	Moderada	Alta	Extrema
Asumir	Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.	X	X		
Reducir	Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.		X	X	X
Evitar	Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.			X	X
Compartir o Transferir	Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.			X	X

Fuente1: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

Fuente2: Guía para la administración del riesgo expedida por la Dirección de Control Interno y Racionalización de Trámites. Departamento Administrativo de la Función Pública (DAFP).
https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

6.14 Priorización de Riesgos a controlar – administrar

La totalidad de riesgos identificados en el mapa de riesgos institucional y por procesos estarán sujetos al seguimiento, monitoreo, control y ajuste mediante la aplicación del procedimiento establecido.

Tendrán prelación aquellos riesgos ubicados en la zona de riesgo extrema y alta, u otras escalas y serán atendidos de forma inmediata a través de acciones concretas. Los riesgos de corrupción hacen parte de esta priorización.

Para la priorización de acciones relacionadas con los riesgos de salud y seguridad laboral, se debería tener en cuenta el potencial de reducción de riesgo de los controles planificados. Puede ser preferible que las acciones que abordan una actividad de alto riesgo u ofrecen una reducción considerable de éste tengan prioridad sobre otras acciones que solamente ofrecen un beneficio limitado de reducción del riesgo. En algunos casos puede ser necesario modificar los procesos, actividades o tareas laborales hasta que los controles del riesgo estén implementados, o aplicar controles de riesgo temporales hasta que se lleven a cabo acciones más eficaces. Por ejemplo, el uso de protección auditiva como una medida temporal hasta que se pueda eliminar la fuente de ruido, o la separación del lugar de trabajo hasta que se reduzcan los niveles de ruido. Los controles temporales no se deberían considerar como un sustituto a largo plazo de medidas de control de riesgo más eficaces[23].

6.15 Formulación de acciones y planes de contingencia

Los planes o el conjunto de tareas que la Agencia establecerá para alcanzar los resultados, tiene que facilitar el cierre de las brechas que existan entre la situación actual y la situación deseada.

Las acciones asociadas a los riesgos se documentan así:

- De manera general en el formato E-FO-017.
- De manera detallada según lo establecido en el procedimiento E-PR-006 Procedimiento Planes de Mejoramiento y con el diligenciamiento del formato Plan de Mejoramiento.
- Las acciones para salud y seguridad laboral, en el documento externo denominado Matriz de riesgos de seguridad y salud ocupacional A-EX-001.

Para aquellos riesgos de mayor criticidad, incluyendo los riesgos de corrupción, se formulan planes de contingencia, cuya gestión deberá activarse cuando el riesgo se materialice.

Para los riesgos de seguridad y salud ocupacional, se documenta y aplica el plan de emergencias. Adicionalmente, las fuentes para identificar oportunidades de mejora son:

- El cumplimiento de los objetivos del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST);
- Los resultados de la intervención en los peligros y los riesgos priorizados;
- Los resultados de la auditoría y revisión del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), incluyendo la investigación de los incidentes, accidentes y enfermedades laborales;

[23] Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Guía Técnica Colombiana GTC 45.

- Las recomendaciones presentadas por los trabajadores y el Comité Paritario de Seguridad y Salud en el Trabajo o Vigía de Seguridad y Salud en el Trabajo, según corresponda;
- Los resultados de los programas de promoción y prevención;
- El resultado de la supervisión realizado por la alta dirección; y
- Los cambios en legislación que apliquen a la organización.

Para los riesgos de seguridad de la información, se documenta y aplica el plan de seguridad y continuidad de Tecnologías de la Información – TI.

En todos los casos implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales; por lo tanto, se deberá considerar para la implementación de acciones y controles, aspectos como: Viabilidad jurídica, viabilidad técnica, viabilidad institucional, viabilidad financiera o económica y análisis costo – beneficio.

La reincidencia del riesgo, la debilidad de sus controles o su materialización son razón para formular acciones correctivas que deberán incluirse en los planes respectivos.

6.16 Publicación

Los riesgos y sus diferentes variables, se consolidan en un documento denominado “Mapa de Riesgos”. La denominación de los riesgos y la definición dada a los mismos en dicho documento, se publican en el portal Web de la entidad, en cumplimiento de lo establecido en el Decreto 124 de 2016.

Se exceptúan de la publicación aquellos riesgos que consideren los procesos y sistemas de gestión, que no deben ser publicados basados en su naturaleza o que puedan generar nuevos riesgos.

6.17 Seguimiento a las acciones y efectividad de los controles

La gestión de riesgos tiene, entre otras, las siguientes fuentes de seguimiento, mismas que seguirán siendo los mecanismos para evaluar el cumplimiento de las variables asociadas a un buen desempeño en la materia. Son:

6.17.1 Reporte de Formulario Único Reporte de Avance de la Gestión - FURAG.

De acuerdo con lo establecido en el Decreto 2482 de 2012, el Formulario Único Reporte de Avance de la Gestión, es una herramienta en línea para el monitoreo, evaluación y control de los resultados institucionales y sectoriales.

Según la circular externo 100-002- 2015 están obligados a diligenciarlo, las entidades de la Rama Ejecutiva del Orden Nacional con excepción de: Los Fondos sin estructura administrativa ni planta de personal, los Fondos Ganaderos, las Electrificadoras y las entidades en proceso de liquidación, supresión o disolución, aunque continúan con la obligación de aplicar, en lo pertinente las políticas de desarrollo administrativo y reportar su avance en los medios que tengan establecidos.

Una parte del reporte indaga por la gestión de riesgos y especialmente en cuanto a riesgos de corrupción. La gestión de riesgos en APC-Colombia ha sido evaluada a través del Furag (2013 en 2014, 2014 en 2015, 2015 en 2016 y 2016 en 2017), con los siguientes resultados:

Tabla 58. Evaluación en Furag sobre la gestión de riesgos

Ítem	2013	2014	2015	2016
Elaboración del mapa de riesgos de corrupción	85	100	60	50
Elementos del mapa de riesgos de corrupción	100	86	-------	-------
Efectividad de los controles del mapa de riesgos de corrupción	66	100	100	-------
Riesgos de corrupción identificados y mejoras realizadas	83	50	84	-------
Publicación del seguimiento	100	-------	-------	-------
Seguimiento	83	100	-------	100
Acciones de mejoras del mapa de riesgos de corrupción	-------	100	0,0	-------
Materialización de Riesgos de Corrupción	-------	-------	100	-------

Fuente: Furag 2013, 2014, 2015 y 2016.

Aunque los esquemas no sean comparables entre sí totalmente por la terminología y variables que ha usado Furag de una vigencia a otra, se puede apreciar lo fluctuante que ha sido la gestión de riesgos en la entidad.

El Furag 2016 recomienda que, para futuras oportunidades, en la construcción del Mapa de Riesgos de Corrupción la entidad adelante un proceso participativo, en el cual se invite a ciudadanos, usuarios o grupos de interés.

6.17.2 Índice de transparencia nacional – ITN

El Índice de transparencia nacional – ITN pide evidencias de la gestión de riesgos, y aunque no es objeto de calificación directa incide en los resultados de la encuesta, en el sub-indicador de “Plan anticorrupción y de atención al ciudadano”, el cual hacen parte del indicador “Políticas y medidas anticorrupción”, que a su vez hace parte del factor de “Institucionalidad”.

La gestión de riesgos hace parte del plan anticorrupción el cual, en la última medición, obtuvo las siguientes calificaciones:

Tabla 59. Seguimiento 2015-2016 ITN

Sub-indicador Plan anticorrupción y de atención al ciudadano		Indicador Políticas y medidas anticorrupción		Factor Institucionalidad	
Real	Ponderado	Real	Ponderado	Real	Ponderado
60,80	1,70	30,40	1,70	61,00	24,40

Fuente: ITN

Es de señalar que este índice solicita formular riesgos para:

- Visibilidad
- Interinstitucionalidad.
- Control y sanción.
- Delitos contra la administración pública.

6.17.3 Índice de Gobierno en línea – GEL

El índice de Gobierno en línea – GEL pide evidencias de la gestión de riesgos a través de una auditoría que adelanta de forma presencial el Ministerio de Tecnologías de la Información y las Comunicaciones, particularmente en lo relacionado con seguridad de la información. La última medición se hizo en diciembre 11 de 2015 y el reporte arrojó para la entidad los siguientes resultados en materia de riesgos, sobre un máximo de 100 puntos posibles:

Tabla 60. Seguimiento índice GEL 2015

ítem	Calificación
La entidad genera acciones para tratar riesgos y oportunidades de seguridad de la información	25
Gestión de riesgos de seguridad y privacidad de la información	0

Fuente: Resultados del índice de Gobierno en línea 2015 emitido por Ministerio de Tecnologías de la Información y las Comunicaciones para la Estrategia de Gobierno en Línea http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-14714.html

6.17.4 Plan Anticorrupción y de Atención al Ciudadano

El Plan Anticorrupción y de Atención al Ciudadano establece la obligatoriedad de la formulación del mapa de riesgos, en especial el de corrupción. En la última aplicación de dicho instrumento, APC-Colombia publicó el mapa de riesgos requerido para el periodo evaluado, junto con su seguimiento.

6.17.5 Informe Ejecutivo Anual del Modelo Estándar de Control Interno - MECI

Cada año se debe diligenciar una herramienta para medir la sostenibilidad del Modelo Estándar de Control Interno – MECI. Más de 35 preguntas del mismo hacen referencia a la gestión del

riesgo. Por tanto, dicha herramienta se suma a todas aquellas con las cuales se hace seguimiento.

6.17.6 Auditorías de la Contraloría General de la República.

La Contraloría General de la República ha efectuado auditorías regulares, las cuales han evaluado, entre otros asuntos, la gestión del riesgo.

En 2015 evaluó la gestión realizada en las vigencias 2013-2014. En los capítulos 2.1.1., 3.1.1. y 3.1.5 del informe de dicha auditoría se muestra que uno de los elementos débiles de la operación de dichas vigencias fue la gestión de riesgos.

En 2016 evaluó la gestión realizada en la vigencia 2015 e hizo alusión al riesgo contractual y al riesgo en la salud y el ambiente.

6.17.7 Auditorías de Control Interno.

El grupo que cumple funciones de Control Interno hará los seguimientos y evaluaciones que considere necesarios y los que establezcan las normas que rigen la materia. Así mismo harán el muestreo de las evidencias presentadas en la autoevaluación.

La gestión de riesgos ha sido revisada en los siguientes informes de Control Interno.

- Periodo Agosto - noviembre de 2013.
- Periodo Abril- Julio de 2013.
- Pormenorizado Control Interno.
- Periodo noviembre 2012 a marzo 2013.
- Periodo diciembre 2013 a marzo 2014.
- Periodo Abril - agosto 2014.
- Periodo Septiembre - diciembre 2014.
- Pormenorizado I cuatrimestre 2015.
- Pormenorizado I cuatrimestre 2016, capítulo 1.3.
- Informe de Auditoria de Gestión del Riesgo, diciembre 19 de 2016.

En varios de ellos fue reiterativo encontrar el llamado de atención sobre la evaluación permanente a los riesgos y de los controles identificados, no obstante, en el último reporte ya se reconocen avances en la gestión.

En el último de los informes referido, Control Interno hace unas recomendaciones, las cuales se espera haber atendido al final de la vigencia 2017.

6.17.8 Auditorías Internas

Las situaciones encontradas en auditoría relacionadas con los riesgos no han sido muchas, como se muestra en el siguiente cuadro:

Tabla 61. Situaciones encontradas en auditoría relacionadas con los riesgos de APC-Colombia

	En materia de riesgos			Total de la auditoría		
Auditoría	Hallazgos	Oportunidades	Total	Hallazgos	oportunidades	Total
Pre auditoría de calidad, diciembre 4 y 5 de 2014	0	2	2	32	12	44
Primer ciclo de auditoria interna, febrero 16 y 17 de 2016	10	0	10	86	8	94
Segundo ciclo de auditoria interna, mayo 26 y 27 de 2016	4	1	5	41	32	73
Auditoría de preparación, agosto 24 y septiembre 12 al 14 de 2016	2	5	7	9	38	47
Primer ciclo de auditoria interna SGSST	2	0	2	18	0	18

Fuente: informes de auditoría.

Aunque no han sido muchas auditorías, en todas ellas se han encontrado situaciones relacionadas con debilidades en la gestión del riesgo.

6.17.9 Autocontrol

Es tal vez el mecanismo más importante, pero a la vez el menor posicionado en la actualidad.

- Autoevaluación: Como parte del autocontrol, cada área hace seguimiento a los riesgos identificados en sus respectivos procesos.
- Instancias de control y seguimiento. La gestión de riesgos es susceptible de ser evaluada por organismos certificadores y/o de control y seguimiento.
- La alta Dirección: en el marco de la Revisión por la Dirección.
- Inspecciones: método que se practica con el fin de identificar los riesgos de salud y seguridad laboral presentes en cada área y tarea de la entidad, las inspecciones pueden ser planeadas o no planeadas y las puede realizar el COPASST, los integrantes de la brigada de emergencias, la persona encarga del tema de Seguridad y Salud en el Trabajo o a ARL, dependiendo cual sea la condición que se debe revisar.
- En cumplimiento de los seguimientos ordenados en la Estrategia Anticorrupción y de Atención al Ciudadano que se aprobó mediante Decreto 124 de enero 26 de 2016.

- El Comité de Conciliación, como instancia administrativa que actúa como sede de estudio, análisis y formulación de políticas sobre prevención del daño antijurídico y defensa de los intereses de la entidad.

El monitoreo a las acciones establecidas en el mapa de riesgos y a la efectividad de los controles se realizará por lo menos una vez al año para todos los riesgos.

El control y su seguimiento, se hará basándose en lo definido en el mapa de riesgos, en los planes y los objetivos institucionales o por procesos.

6.18 Indicadores de riesgo

Debe establecerse un mecanismo que permita medir el riesgo y su gestión, que permita alertar sobre las situaciones en las cuales se deben tomar medidas. Por ejemplo:

a) Riesgos materializados en la vigencia, con respecto a los riegos identificados en la misma.
b) Riesgos con acciones de mejoramiento formuladas, con respecto a los riegos identificados en la misma.

6.19 Acciones para el manejo de riesgos materializados

Si dentro del seguimiento realizado, bien sea por parte de la Oficina de Control Interno o por los líderes de los procesos, se establece que se ha materializado uno o más riesgos, las acciones requeridas son las siguientes:

Tabla 62. Lineamientos para el manejo de Riesgos Materializados

	Riesgo de Corrupción	Demás riesgos			
Detectado por	Todas las categorías del reisgo	Extrema	Alta	Moderada	Baja
Oficina de Control Interno	1. Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. 2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. 3. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. 4. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.	1. Informar al líder del proceso sobre el hecho encontrado. 2. Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho. 3. Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente. 4. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada cuando se trate de un riesgo inaceptable.			1. Informar la líder del proceso sobre el hecho.
Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso	1. Informar a la Alta Dirección sobre el hecho encontrado. 2. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo. 3. Iniciar con las acciones correctivas necesarias. 4. Realizar el análisis de causas y determinar acciones preventivas y de mejora. 5. Análisis y actualización del mapa de riesgos.	1. Tomar las acciones correctivas necesarias, dependiendo del riesgo materializado. 2. Iniciar el análisis de causas y determinar acciones preventivas y de mejora. 3. Analizar y actualizar el mapa de riesgos. 4. Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.			Aplicar las orientaciones de la política de riesgos institucional. (Verificar los niveles de aceptación del riesgo).
Área con funciones de Planeación	1. Orientar técnicamente sobre las acciones determinadas en la política de riesgos institucional.	1. Orientar técnicamente sobre las acciones determinadas en la política de riesgos institucional.			1. Orientar técnicamente sobre las acciones determinadas en la política de riesgos institucional.

Fuente: Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública
https://www.funcionpublica.gov.co/guias

6.20 Documentos y registros de la administración del riesgo

La entidad conservará los documentos del Sistema de Gestión Integral y los registros resultantes de la gestión de riesgos, atendiendo lo establecido en las tablas de retención documental que le apliquen y a los mecanismos tecnológicos en los cuales se apoye la gestión respectiva.

6.21 Tratamiento especial

Adicionalmente a lo tratado en el presente documento, los siguientes riesgos tendrán un tratamiento especial:

- Riesgos identificados en el sistema de gestión en seguridad y salud ocupacional: se apoyan en la asesoría que entregue la ARL a la cual está afiliada la entidad y se registra en el(los) formato(s) que se definan para tal fin de acuerdo con lo establecido en la Guía Técnica Colombiana 45 de 2012.

- Riesgos propios del esquema contractual de Colombia Compra Eficiente: se orientan con el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación, metodología que Colombia Compra Eficiente adoptó con base en el Estándar AS/ NZS ISO 31000 y con el Manual de Riesgos contractuales A-OT-022. Se debe analizar su articulación con la Administración del Riesgo Institucional.

- Riesgos de los proyectos: se aplicará la metodología presentada en este documento, teniendo observancia de lo establecido en la Guía del Departamento Administrativo de la Función Pública para la Administración del Riesgo, que reza que " algunos aspectos relacionados con las escalas de impacto del proyecto giran en torno a los cuatro (4) objetivos clave del proyecto, como son: Costo, Tiempo, Alcance y Calidad, por lo que se hace necesario ahondar en los fundamentos desarrollados por el Project Management Institute, información que puede ser consultada en https://americalatina.pmi.org/. Esta metodología se irá implementando paulatinamente en la medida que la dinámica de la entidad lo permita.

- Los riesgos de daño antijurídico se apoyan en los contenidos del Manual para la elaboración de políticas de prevención del daño antijurídico.

Finalmente, con respecto a los registros, mientras Brújula se adapta a todas las condiciones de los diferentes sistemas de gestión, los registros se llevarán de la siguiente manera:

Sistema	Medio de registro
Seguridad y salud en el trabajo	A-OT-044
Seguridad de la información	Formato diseñado para tal fin
Gestión ambiental	Formato diseñado para tal fin
Gestión contractual	Contrato respectivo
Proyectos	Ficha EBI
Demás Sistemas	Brújula

7. PERIODICIDAD

La gestión de riesgos tiene en cuenta la periodicidad. [24]

La Administración del Riesgo pretende anticiparse a la ocurrencia de posibles eventos, en consecuencia, su identificación y acciones se harán en forma preventiva.

La Política de Administración del Riesgo se establece desde el inicio del periodo de gobierno y serán revisadas en la medida que se requiera o hasta el siguiente cuatrienio, dado que los riesgos, deberán someterse al marco estratégico de la entidad y al contexto estratégico que se identifique para tal fin.

La revisión al contenido del mapa de riesgos de la APC-Colombia, se realizará como mínimo una vez al año o de manera adicional cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales en la plataforma estratégica o en el contexto estratégico, modificaciones o cambios relevantes en los procesos y/o procedimientos, o cualquier hecho sobreviniente externo o interno que afecte la operación de la entidad.

El seguimiento a los controles y a las acciones se hará en las fechas establecidas en el aplicativo.

En cuanto a la periodicidad del seguimiento, para los riesgos asociados a posibles actos de corrupción, se debe dar cumplimiento a las fechas establecidas por la guía de la Secretaría de Transparencia, denominada “Estrategias para la construcción del plan anticorrupción y de atención al ciudadano”; para los riesgos de gestión ubicados en las diferentes zonas de riesgo residual, se tomarán en cuenta las fechas establecidas en la política de riesgos institucional. Las frecuencias de medición definidas no deben superar los tres meses, de forma que permitan que el seguimiento realizado sea base para la toma de decisiones, y que se logren introducir correctivos en el momento adecuado.

8. TÉRMINOS Y DEFINICIONES

En la gestión del riesgo aplican los siguientes términos y definiciones:

Tabla 63. Definiciones generales de la gestión del riesgo

Definición	Aplicable a
Acción correctiva. Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.	General

[24] OHSAS 18001

Definición	Aplicable a
Acción preventiva. Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.	General
Accidente de trabajo. Suceso repentino que sobreviene por causa o con ocasión del trabajo, y que produce en el trabajador una lesión orgánica, una perturbación funcional, una invalidez o la muerte. Es también accidente de trabajo aquel que se produce durante la ejecución de órdenes del empleador, o durante la ejecución de una labor bajo su autoridad, incluso fuera del lugar y horas de trabajo (Decisión 584 de la Comunidad Andina de Naciones).	SGSST
Actividad rutinaria. Actividad que forma parte de un proceso de la organización, se ha planificado y es estandarizable.	SGSST
Actividad no rutinaria. Actividad que no se ha planificado ni estandarizado dentro de un proceso de la organización o actividad que la organización determine como no rutinaria por su baja frecuencia de ejecución.	SGSST
Activo de información: Cualquier componente tecnológico o documental (análogo o digital) en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la entidad	Seguridad de la Información
Administración del riesgo. Conjunto de elementos de control y sus interrelaciones, para que la entidad evalué e intervenga aquellos eventos, tanto internos como externos que puedan efectuar de manera positiva o negativa el logro de sus objetivos institucionales. Contribuye a que la Entidad consolide su Sistema de Control Interno y a que se genere una Cultura de Autocontrol y Autoevaluación al interior de la misma.	General
Análisis del riesgo. Proceso para comprender la naturaleza del riesgo (véase el numeral 2.30) y para determinar el nivel del riesgo (véase el numeral 2.24) (ISO 31000).	SGSST
Asignación del riesgo: Es el proceso de distribuir los riesgos de acuerdo con la capacidad de cada una de las partes para gestionarlo, controlarlo, administrarlo y mitigarlo.	Contractual
Autenticidad: Es la condición de poder identificar que el generador o receptor (interlocutor) de la información es realmente quien dice ser.	Seguridad de la Información
Causa. Medio, las circunstancia y agente generador de riesgo.	General
Causa: Son los medios, circunstancias y agentes que generan los riesgos.	Contractual
Confidencialidad: Principio básico que impide la divulgación de información a personas o sistemas no autorizados.	Seguridad de la Información
Conciliación extrajudicial, es la conciliación que se realiza antes o por fuera de un proceso judicial[25]. En asuntos de lo contencioso administrativo es un mecanismo de solución de los conflictos entre los particulares y el Estado, la cual debe, obligatoriamente, adelantarse ante un agente del Ministerio Público[26] como requisito de procedibilidad, antes de presentar una demanda ante la jurisdicción de lo contencioso administrativo, en asuntos de naturaleza conciliable.	Daño antijurídico
Consecuencia. Resultado de un evento.	General
Contexto estratégico. Condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución. Las situaciones del entorno o externas pueden ser de carácter social, cultural, económico, tecnológico, político, ambiental y legal, bien sea internacional, nacional o regional según sea el caso de análisis. Las situaciones internas están relacionadas con la estructura, cultura organizacional, el modelo de operación, el cumplimiento de los Planes, Programas y Proyectos, los sistemas de información, los procesos y procedimientos y los recursos humanos y económicos con los que cuenta una entidad, entre otros.[27]	General

[25] Ley 640 de 2001 Art. 3

[26] Ley 640 de 2001 Art. 23

[27] Decreto943de mayo 21 de 2014, MECI2014.

Definición	Aplicable a
Control. Medida que modifica el riesgo. - Correctivos. Aquellos que permiten el restablecimiento de actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia. - Preventivos: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.	General
Corrupción. Uso indebido del poder, de los recursos o de la información, que lesiona los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.	General
Consecuencia. Resultado, en términos de lesión o enfermedad, de la materialización de un riesgo, expresado cualitativa o cuantitativamente. 2.6 Competencia. Atributos personales y aptitud demostrada para aplicar conocimientos y habilidades.	SGSST
Competencia. Atributos personales y aptitud demostrada para aplicar conocimientos y habilidades.	SGSST
Daño antijurídico: "la lesión de un interés legítimo, patrimonial o extra patrimonial, que la víctima no está en la obligación de soportar, que no está justificado por la ley o el derecho". [28]	Daño antijurídico
Demanda judicial: Acto por el que el actor demandante solicita del órgano jurisdiccional frente al demandado una tutela jurídica en forma de sentencia favorable, mediante un escrito en el que expone los antecedentes del hecho del caso y sus razonamientos jurídicos, con el que ordinariamente se comienza el proceso	Daño antijurídico
Diagnóstico de condiciones de salud. Resultado del procedimiento sistemático para determinar "el conjunto de variables objetivas de orden fisiológico, psicológico y sociocultural que determinan el perfil sociodemográfico y de morbilidad de la población trabajadora" (Decisión 584 de la Comunidad Andina de Naciones).	SGSST
Disponibilidad: Principio básico que permite encontrar la información a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.	Seguridad de la Información
Efecto. Consecuencia de la ocurrencia del riesgo sobre los objetivos de la Entidad.	General.
Elemento de Protección Personal (EPP): Dispositivo que sirve como barrera entre un peligro y alguna parte del cuerpo de una persona.	SGSST
Enfermedad. Condición física o mental adversa identificable, que surge, empeora o ambas, a causa de una actividad laboral, una situación relacionada con el trabajo o ambas.	SGSST
Enfermedad profesional. Todo estado patológico que sobreviene como consecuencia obligada de la clase de trabajo que desempeña el trabajador o del medio en que se ha visto obligado a trabajar, bien sea determinado por agentes físicos, químicos o biológicos (Ministerio de la Protección Social, Decreto 2566 de 2009).	SGSST
Equipo de protección personal: Dispositivo que sirve como medio de protección ante un peligro y que para su funcionamiento requiere de la interacción con otros elementos. Ejemplo, sistema de detección contra caídas.	SGSST
Estimación del riesgo: Es valorar la probabilidad de ocurrencia y el nivel de impacto de los riesgos que han sido tipificados.	Contractual
Evaluación Higiénica. Medición de los peligros ambientales presentes en el lugar de trabajo para determinar la exposición ocupacional y riesgo para la salud en comparación con los valores fijados por la autoridad competente.	SGSST
Evaluación del riesgo. Proceso para determinar el nivel asociado al nivel de probabilidad y el nivel de consecuencia.	SGSST
Evento. Presencia o cambio de un conjunto particular de circunstancias.	General
Exposición. Situación en la cual las personas se encuentran en contacto con los peligros.	SGSST
Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.	General
Identificación del peligro. Proceso para reconocer si existe un peligro y definir sus características.	SGSST

[28] Consejo de Estado. Sala de lo Contencioso Administrativo. Sección Tercera. Sentencia de 2 de marzo de 2000. C.P. Mará Elena Giraldo Gómez. Exp. 11945, entre otras. Cfr. Consejo de Estado. Sala de lo Contencioso Administrativo. Sección Tercera. Aclaración de voto de Enrique Gil Botero de 30 de julio de 2008. Exp. 15726

Definición	Aplicable a
Identificación Del Riesgo: Es la descripción (verbalización) de la situación no deseada, teniendo en cuenta el objeto a contratar, el valor de la contratación, la modalidad de selección, la ejecución contractual y financiera, así como las actividades a desarrollar y el lugar de ejecución, al igual que todas aquellas posibles causas que pueden ocasionar el rompimiento del equilibrio económico del contrato.	Contractual
Impacto: Son las consecuencias que puede ocasionar a la entidad la materialización del riesgo.	Contractual Seguridad de la información
Incidente. Evento(s) relacionado(s) con el trabajo, en el (los) que ocurrió o pudo haber ocurrido lesión o enfermedad (independiente de su severidad) o víctima mortal.	SGSST
Integridad: Principio básico que busca mantener los datos libres de modificaciones no autorizadas.	Seguridad de la Información
Jurisdicción Contencioso Administrativa: Los jueces de esta jurisdicción están llamados a solucionar los conflictos que se presentan entre particulares y el Estado, o los conflictos que se presentan al interior del Estado mismo.	Daño antijurídico
Línea Jurisprudencial: Criterio constante y uniforme de aplicar el derecho, mostrado en las sentencias de los tribunales judiciales superiores.	Daño antijurídico
Litigio: Disputa, contienda o alteración de índole judicial.	Daño antijurídico
Lugar de trabajo. Cualquier espacio físico en el que se realizan actividades relacionadas con el trabajo, bajo el control de la organización.	SGSST
Medida(s) de control. Medida(s) implementada(s) con el fin de minimizar la ocurrencia de incidentes.	SGSST
Mejora continua. Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.	General
Monitoreo biológico. Evaluación periódica de muestras biológicas (ejemplo sangre, orina, heces, cabellos, leche materna, entre otros) tomadas a los trabajadores con el fin de hacer seguimiento a la exposición a sustancias químicas, a sus metabolitos o a los efectos que éstas producen en los trabajadores.	SGSST
Nivel de consecuencia (NC). Medida de la severidad de las consecuencias.	SGSST
Nivel de deficiencia (ND). Magnitud de la relación esperable entre (1) el conjunto de peligros detectados y su relación causal directa con posibles incidentes y (2) con la eficacia de las medidas preventivas existentes en un lugar de trabajo.	SGSST
Nivel de exposición (NE). Situación de exposición a un peligro que se presenta en un tiempo determinado durante la jornada laboral.	SGSST
Nivel de probabilidad (NP). Producto del nivel de deficiencia por el nivel de exposición.	SGSST
Nivel de riesgo. Magnitud de un riesgo resultante del producto del nivel de probabilidad por el nivel de consecuencia.	SGSST
No repudio: También conocido como “no negación”, es la condición que evita que se niegue la autoría o recepción de un mensaje o información.	Seguridad de la Información
Partes Interesadas. Persona o grupo dentro o fuera del lugar de trabajo (véase el numeral 2.18) involucrado o afectado por el desempeño de seguridad y salud ocupacional de una organización.	SGSST
Peligro: Fuente, situación o acto con potencial de daño en términos de enfermedad o lesión a las personas, o una combinación de estos.	SGSST
Personal expuesto. Número de personas que están en contacto con peligros. Grado de posibilidad de que ocurra un evento no deseado y pueda producir consecuencias.	SGSST
Posibles consecuencias – efecto: Son los que constituyen los efectos de la ocurrencia del riesgo sobre los procesos contractuales.	Contractual
Probabilidad. Grado de posibilidad de que ocurra un evento no deseado y pueda producir consecuencias.	SGSST
Probabilidad. Oportunidad de que algo suceda.	General
Probabilidad: Es una medida para estimar la posibilidad de que ocurra un incidente o evento.	Contractual

Definición	Aplicable a
Probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.[29]	Seguridad de la información
Proceso. Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.	SGSST
Proceso judicial: Conjunto de procedimientos y trámites judiciales tendientes a la obtención de una decisión por parte del tribunal de justicia llamado a resolver la cuestión controvertida.	Daño antijurídico
Providencia judicial: Actos que representan la manifestación de la voluntad del estado, emitidas por un funcionario con competencia para proferirla (es decir; que a dicho funcionario se le ha delegado la función de administrar justicia en dicho caso), al interior de un proceso judicial.	Daño antijurídico
Régimen Jurídico: conjunto de leyes y normativas al que debe someterse cierta materia.	Daño antijurídico
Requisito de procedibilidad: Toda persona natural o jurídica (pública o privada) que con ocasión de la expedición de un acto administrativo particular o de la ocurrencia de un daño antijurídico derivado de la celebración, ejecución, terminación o liquidación de un contrato estatal o como consecuencia de un hecho, una omisión o una operación administrativa, considere que le han causado un detrimento en su patrimonio, debe intentar, obligatoriamente, la celebración de un acuerdo conciliatorio de las controversias existentes con las entidades u organismos de derecho público o con el particular, (qué ejerza funciones públicas) antes de presentar la respectiva demanda encaminada a obtener una pretensión económica[30].	Daño antijurídico
Riesgo. Evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.	General
Riesgo. Combinación de la probabilidad de que ocurra un(os) evento(s) o exposición(es) peligroso(s), y la severidad de lesión o enfermedad, que puede ser causado por el (los) evento(s) o la(s) exposición(es).	SGSST
Riesgo. Efecto de la incertidumbre.	Ambiental
Riesgo Aceptable. Riesgo que ha sido reducido a un nivel que la organización puede tolerar con respecto a sus obligaciones legales y su propia política en seguridad y salud ocupacional.	SGSST
Riesgo Contractual: El riesgo contractual en general es entendido como todas aquellas circunstancias que pueden presentarse durante el desarrollo o ejecución de un contrato y que pueden alterar el equilibrio financiero del mismo. Ha tenido una regulación desde cinco ópticas, asociadas con el proceso de gestión que se requiere en cada caso.[31]	Contractual
Seguridad de la Información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.	Seguridad de la Información
Sentencia: Acto mediante el cual un juez o magistrado expresa la voluntad que el estado toma sobre el objeto del proceso, es decir; las pretensiones formuladas por el demandante y la conducta que frente a ellas adopte el demandado.	Daño antijurídico
Tipificación del riesgo: Proceso de caracterización de los riesgos que puedan preverse en las diferentes etapas del contrato, agrupados dentro de diferentes clases que presentan características similares. Así, la tipificación de los riesgos previsibles podrá consistir en la identificación de los distintos riesgos que pueden ocurrir durante la ejecución del contrato y su incorporación en una clase, si ella existe.	Contractual
Valoración de los riesgos. Proceso de evaluar el(los) riesgo(s) que surge(n) de un(os) peligro(s), teniendo en cuenta la suficiencia de los controles existentes, y de decidir si el(los) riesgo(s) es (son) aceptable(s) o no.	SGSST

[29] Fuente: Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic.

[30] Ley 640 de 2001 Art.35

[31] Documento CONPES 3714 /2011

Definición	Aplicable a
Valor límite permisible (VLP) LP. Concentración de un contaminante químico en el aire, por debajo de la cual se espera que la mayoría de los trabajadores puedan estar expuestos repetidamente, día tras día, sin sufrir efectos adversos a la salud.	SGSST
Valoración de riesgos: Es la determinación del nivel de riesgos en función del impacto y de la probabilidad de ocurrencia del riesgo.	Contractual

Fuentes:
Norma Técnica de Calidad en la Gestión Pública. NTC GP 1000:2009. Página 29.
Norma Técnica Colombiana NTC ISO 31000. Gestión del Riesgo.
Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional.
Guía Técnica Colombiana GTC 45.
Política de daño antijurídico de APC-Colombia.
Política de seguridad de la información de APC-Colombia.
Decreto 943 de mayo 21 de 2014, MECI2014. y otros.

9. REFERENCIAS NORMATIVAS

Ley 87 de noviembre 29 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
http://www.mininterior.gov.co/la-institucion/normatividad/ley-87-de-1993

Decreto Ley 1295 de junio 22 de 1994: el cual determina la organización y administración del Sistema General de Riesgos Profesionales.
http://www.secretariasenado.gov.co/senado/basedoc/decreto_1295_1994.html

Ley 489 de diciembre 29 de 1998. Estatuto básico de Organización y funcionamiento de la Administración Publica. Capítulo VI. Sistema Nacional de Control Interno.
http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=836

Decreto 4485 de noviembre 18 de 2009. Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública. NTC GP 1000:2009.
https://www.mintic.gov.co/portal/604/articles-3618_documento.pdf

Ley 1474 de Julio 12 de 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. Plan Anticorrupción y de Atención al Ciudadano.
http://www.secretariasenado.gov.co/senado/basedoc/ley_1474_2011.html

Ley 1562 de julio 11 de 2012: por la cual se modifica el sistema de riesgos laborales y se dictan otras disposiciones en materia de salud ocupacional.
http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/ley156211072012.pdf

Decreto 2482 de diciembre 3 de 2012. Por la cual se establecen los lineamientos generales para la integración de la planeación y la gestión.

https://www.mintic.gov.co/portal/604/articles-3581_documento.pdf

Decreto1510 de julio 17 de 2013: Reglamenta el sistema de compras y contratación pública.
http://www.colombiacompra.gov.co/es/decreto-1510-de-2013

Decreto 943 de mayo 21 de 2014. Por el cual se actualiza el Modelo Estándar de Control Interno para el Estado Colombiano.
https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/decreto_0943_2014.htm

Decreto 1443 de julio 31 de 2014: Por el cual se dictan disposiciones para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), compilado en el Decreto 1072 de mayo 26 de 2015.
http://www.mintrabajo.gov.co/normatividad/decreto-unico-reglamentario-trabajo.html

Ley 1753 de junio 09 de 2015: por la cual se adopta el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS".
http://www.secretariasenado.gov.co/senado/basedoc/ley_1753_2015.html

Decreto Único Reglamentario 1082 de mayo 26 de 2015.
http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Paginas/mayo.aspx

Decreto 124 de enero 26 de 2016, Estrategia para la construcción del Plan Anticorrupción y de Atención al Ciudadano.
http://www.secretariatransparencia.gov.co/secretaria/Documents/Estrategia-Construccion-Plan-Anticorrupcion-Atencion-Ciudadano-v2.pdf

Manual de Gobierno en Línea - GEL.
http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia compra eficiente.
http://www.colombiacompra.gov.co/sites/default/files/manuales/cce_manual_riesgo_web.pdf

Guía 2015 para la gestión del riesgo de corrupción.
https://www.funcionpublica.gov.co/guias

Cartilla “Guía para la Administración del Riesgo” diseñada por el Departamento Administrativo de la Función pública – DAFP, versión 3, diciembre de 2014.
https://www.funcionpublica.gov.co/guias

Cartilla “Guía para la Gestión del Riesgo de corrupción” diseñada por el Departamento Administrativo de la Función pública – DAFP, versión 2015.
https://www.funcionpublica.gov.co/guias

Guía de gestión de riesgos. Seguridad y privacidad de la información. Guia 7 de MIntic. Abril 01 de 2016.

https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Manual para la elaboración de políticas de prevención del daño antijurídico 2014. Documentos Especializados de la Agencia Nacional de Defensa Jurídica del Estado.
http://www.defensajuridica.gov.co/gestion/publicaciones-andje/Guia-generacion-politica-prevencion/Documents/cartilla11_250814.pdf

ISO 14001: por la cual se orienta el Sistema de Gestión Ambiental.
Publicación restringida

Norma Técnica Colombiana NTC OHSAS 18001:2007, por la cual se orienta el Sistema de Seguridad y Salud en el Trabajo.
Publicación restringida

Norma Técnica Colombiana NTC-ISO/IEC 27001:2013: por la cual se orienta el Sistema de Gestión de Seguridad de la Información.
Publicación restringida

ISO 15489-1:2001: por la cual se orienta el Sistema de Gestión de archivo.
Publicación restringida

Norma Técnica Colombiana NTC-ISO 31000:2011
Publicación restringida

Norma Técnica Colombiana NTC ISO 31000: establece principios básicos para la gestión del riesgo.
Publicación restringida

Guía técnica colombiana para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional GTC 45 de diciembre 15 de 2012 o la guía técnica que haga sus veces.
Publicación restringida

Norma Técnica Colombiana NTC-ISO 31000:2011.
Publicación restringida

Guía técnica exposición de factores de riesgo ocupacional de la protección social.
Publicación restringida

NTC 4114:1997 Seguridad industrial: realización de inspecciones planeadas.
Publicación restringida

10. CONTROL DE CAMBIOS

Versión	Código	Nombre	Acto	Control de cambios
1	DG-D-008	Lineamientos Administración del Riesgo	Acta21Mar11/2013	Nuevo 01/03/2013
2	DG-D-008	Lineamientos Administración del Riesgo	No tiene	Actualización imagen institucional 01/05/2013
3	DG-D-008	Lineamientos Administración del Riesgo	No tiene	Actualización imagen institucional 27/10/2014
4	DG-D-008	Lineamientos Administración del Riesgo	No tiene	Se incluye anexo de análisis de contexto estratégico
5	DG-D-008	Política, lineamientos y metodología de identificación y administración del riesgo	Acta noviembre 19 de 2015	Se reorganizó la información del documento, se amplió el alcance a otros sistemas de gestión, se completó la información y las referencias a otros documentos del Sistema de Gestión Integrado, y se articula con el formato DG-F-017 y el procedimiento respectivo.
6	E-OT-008	Política, lineamientos y metodología de identificación y administración del riesgo	Acta diciembre 22 de 2015	Cambió el código del documento. Incluyó nueva dirección de la entidad e incluyó parámetros específicos para los riesgos de corrupción
1	A-OT-022	Manual de identificación y distribución del riesgo contractual de la Agencia Presidencial de Cooperación Internacional de Colombia, APC-Colombia.	Brújula Junio 10 de 2016	Se crea el Manual de identificación y distribución de riesgos contractuales.
7	E-OT-008	Política, lineamientos y metodología de identificación y administración del riesgo	Brújula, Agosto 01 de 2016	Se incluyen pasos en la herramienta Brújula.
8	E-OT-008	Política, lineamientos y metodología de identificación y administración del riesgo	Brújula, Octubre 28 de 2016.	Se incluyó el diagnóstico y las líneas de defensa. Se precisaron las categorías para calificar el impacto y se incluyeron consideraciones específicas para cada sistema de gestión SISO Y SSI. Se aclararon los tratamientos. Se ajustaron las referencias normativas.
9	E-OT-008	Política, lineamientos y metodología de identificación y administración del riesgo	Brújula, marzo 08 de 2017	Se ajusta a la nueva imagen institucional.
10	E-OT-008	Política, lineamientos y metodología de identificación y administración del riesgo	Brújula, mayo 19 2017	Amplía el detalle a los elementos relacionados con el Sistema de Seguridad de la información, daño antijurídico, y Plan de Gestión Ambiental. Aborda las sugerencias emitidas por Control Interno en el Informe de Auditoria de Gestión del Riesgo, diciembre 19 de 2016..Amplía el diagnóstico.