TABLA DE CONTENDIDO

9. ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

Este documento presenta la metodología, marco de acción y las actividades que se deben planear y ejecutar para realizar la gestión de activos de información y de riesgos de seguridad de la información.

La aplicación de la metodología permite documentar el inventario de los activos de información y el mapa de riesgos de seguridad de la información de cada activo de información, que gestiona cada uno de los procesos institucionales de la Agencia Presidencial de Cooperación Internacional de Colombia - APC Colombia, en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y sus pilares de Confidencialidad, Integridad y Disponibilidad.

En este documento se detallan los pasos para aplicar el tratamiento de los riesgos de seguridad de la información, sobre cada activo de información y evaluar el nivel de protección soportando los objetivos de los procesos institucionales, dando cumplimiento al documento: Política de gestión del riesgo, Código: E-OT-008.

2. OBJETIVOS

2.1. Objetivo general

Establecer la metodología y el marco de acción para la gestión de activos de información y de riesgos de seguridad de la información de los procesos institucionales de APC Colombia, bajo las buenas prácticas de estándares internacionales generalmente aceptados en Colombia y la adaptación de lineamientos definidos por el Ministerio de las Tecnologías de la

Información y las Comunicaciones (MINTIC) y el Departamento Administrativo de la Función Pública (DAFP).

2.2. Objetivos específicos

- Definir y documentar el lineamiento metodológico para la gestión de activos de información y de riesgos de seguridad de la información de los procesos institucionales de la Agencia.
- Definir el marco de acción, secuencia de actividades e identificación de responsables para la gestión de los activos y riesgos de seguridad de la información de cada uno.
- Cumplir la conformidad de la norma internacional ISO/IEC 27001:2022. Así como, los lineamientos emitidos por el DAFP y el MINTIC en materia de la gestión de activos de información y riesgos de seguridad de la información, conforme a: *"Anexo 4, Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas" (MINTIC, 2018), y "Guía No 5 para la Gestión y Clasificación de Activos de Información". (MINTIC, 2016) y la adaptación de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6 (DAFP, 2022).*

3. ALCANCE

El presente lineamiento deberá ser aplicado por los procesos institucionales de APC Colombia, en el marco del cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG) y de las Políticas del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

4. TÉRMINOS Y DEFINICIONES

Los principales términos y definiciones técnicas (tipo glosario), se encuentran documentados y conciliados en el documento: Política de seguridad y privacidad de la información, Código: A-OT-011, la cual agrupa siglas y/o términos y definiciones de los diferentes documentos del SGSPI. Sin embargo, acorde con el presente documento, se registra lo siguiente:

- **Activo de información:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos asociados con el manejo de los datos e información misional, operativa y administrativa de APC Colombia (CONPES 3854 de 20116, acondicionada para APC Colombia).

5. SIGLAS

- **APC Colombia:** Agencia Presidencial del Cooperación Internacional de Colombia.
- **CGDI:** Comité Institucional de Gestión y Desempeño.
- **DAFP:** Departamento Administrativo de la Función Pública.
- **PHVA:** Planear, Hacer, Verificar y Actuar.
- **MINTIC:** Ministerio de las Tecnologías de la Información y las Comunicaciones.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **SGI:** Sistema de Gestión Integral.
- **SGSPI:** Sistema de gestión de seguridad y privacidad de la información.
- **SMLMV:** Salario mínimo legal mensual vigente.
- **TRD:** Tablas de Retención Documental

6. MAPA DE PROCESOS Y CONTEXTO

La Agencia Presidencial de Cooperación Internacional de Colombia - APC Colombia, creada mediante Decreto 4152 del 3 de Noviembre de 2011, tiene como objetivo *"Gestionar, orientar y coordinar técnicamente la cooperación internacional pública, privada, técnica y financiera no reembolsable que reciba y otorgue el país y Administrar y apoyar la canalización y ejecución de recursos, programas y proyectos de cooperación internacional, atendiendo los objetivos de la Política Exterior y el Plan Nacional de Desarrollo"*, (Plan Estratégico Institucional, 2019).

APC Colombia adoptó para su operación institucional, mediante la Resolución No. 507 de 2017 *"Por la cual se conforma el Comité Institucional de Gestión y Desempeño y se adopta la actualización del Modelo Integrado de Planeación y Gestión"*, permitiendo la adecuada gestión por procesos y la adopción de un Sistema de Gestión Integral (SGI) que, actualmente opera con catorce (14) procesos, como se denominan en la siguiente ilustración:

Ilustración 1. Mapa de procesos de APC Colombia

Fuente: Información tomada de la sede electrónica de APC Colombia.

La operación por procesos conduce a la producción de información, siendo pertinente caracterizar u agrupar en activos de información e identificar los niveles de propiedad, como se registra en el apartado: *"Propietarios del activo de información y de la gestión del riesgo de seguridad de la información",* con el propósito de gestionar la seguridad de información en el marco de los pilares de: confidencialidad, integridad y disponibilidad.

7. MARCO DE ACCIÓN PARA GESTIÓN DE ACTIVOS DE INFORMACIÓN Y DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Tabla 1. Marco de acción para gestionar los activos de información y de riesgos de seguridad de la información

No	ACTIVIDAD	RESPONSABLE	REGISTRO	FRECUENCIA
1	Gestión de activos de información: Identificación, clasificación, valoración y documentación del inventario de activos de información con aplicación del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información, Código: A-OT-125.	Procesos institucionales.	Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272.	Definido en el Documento: Plan de seguridad y privacidad de la información, Código: A-OT-101. Por demanda (cuando el proceso identifique la necesidad de actualizar los activos de información y/o su valoración.

No	ACTIVIDAD	RESPONSABLE	REGISTRO	FRECUENCIA
2	Gestión de riesgos de seguridad de la información: Identificación de riesgos de seguridad de la información, evaluación del riesgo de seguridad de la información, definición del tratamiento y mapeo de controles con aplicación de: del documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información, Código: A-OT-125.	Procesos institucionales.	Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272.	Definido en el Documento: Plan de seguridad y privacidad de la información, Código: A-OT-101. Por demanda (cuando el proceso identifique nuevos activos de información y/o riesgos de seguridad de la información).

No	ACTIVIDAD	RESPONSABLE	REGISTRO	FRECUENCIA
3	Certificación de la gestión de activos de información y de riesgos de seguridad de la información y presentación para aprobación del Comité Institucional de Gestión y Desempeño (CIGD)	Procesos institucionales. CIGD.	Acta del CIGD.	Definido en el Documento: Plan de seguridad y privacidad de la información, Código: A-OT-101. Por demanda (cuando el proceso identifique nuevos activos).
4	Publicación de una copia del Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272, en la sede electrónica.	Proceso Gestión comunicaciones. Proceso Gestión de tecnologías de la información.	Sede electrónica.	Definido en el Documento: Plan de seguridad y privacidad de la información, Código: A-OT-101. Por demanda (cuando el proceso identifique nuevos activos).

No	ACTIVIDAD	RESPONSABLE	REGISTRO	FRECUENCIA
5	Disponibilidad del instrumento del mapa de riesgos de seguridad de la información y controles en un recurso de red para los procesos institucionales	Proceso Gestión de tecnologías de la información.	Recurso de red compartido. Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272.	No aplica.

Fuente: Elaborado por el proceso Gestión de tecnologías de la información de APC Colombia, septiembre 2023.

8. PROPIETARIOS DEL ACTIVO DE INFORMACIÓN Y DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

APC Colombia cumple su cometido estatal mediante la gestión de procesos, siendo estos que, con sus equipos de trabajo, producen la información institucional que generalmente se documenta en activos de información.

Estos activos de información adquieren unos atributos relacionados con los propietarios, los cuales se clasifican por niveles y propiedad y es necesario identificar para la gestión de riesgo de seguridad de la información.

Esta gestión se determina en la siguiente estructura de la propiedad de los activos de información:

Tabla 2. Propietarios de los activos de información y compromiso

ID	PROPIETARIO DEL ACTIVOS DE INFORMACIÓN	NIVEL DE PROPIEDAD DEL ACTIVO DE INFORMACIÓN	ROL DEL PROCESO	ROL DE LAS PERSONAS DE LOS PROCESOS
1	Agencia Presidencial de Cooperación Internacional de Colombia - APC Colombia.	Propietario principal de los activos de información.	Propietario de información institucional.	No aplica (persona jurídica).
2	Dependencia(s) a nivel de Dirección(es) y/o directores de dependencias.	Propietario de nivel secundario de activos de información.	Líder(es) de proceso(s) institucional(es). Productor de información. Custodio de activos de información.	El rol de Líder de(los) Procesos corresponde al(los) director(es) de cada dependencia, el cual acepta(n) la actualización de los activos de información y de

ID	PROPIETARIO DEL ACTIVOS DE INFORMACIÓN	NIVEL DE PROPIEDAD DEL ACTIVO DE INFORMACIÓN	ROL DEL PROCESO	ROL DE LAS PERSONAS DE LOS PROCESOS
				los riesgos de seguridad de la información asociados que, son documentados por los responsables de sus procesos, mediante un certificado que se genera en el instrumento: “Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272”.

ID	PROPIETARIO DEL ACTIVOS DE INFORMACIÓN	NIVEL DE PROPIEDAD DEL ACTIVO DE INFORMACIÓN	ROL DEL PROCESO	ROL DE LAS PERSONAS DE LOS PROCESOS
3	Proceso(s) institucional(es).	Propietario de nivel terciario de activos de información.	Responsable del proceso institucional. Productor de información. Custodio de activos de información.	Este rol corresponde generalmente al(los) asesor(es) de la dirección general y coordinador(es) de los grupos internos de trabajo (o quien(es) hagan sus veces) el cual deben actualizar los activos de información y gestionar los riesgos de seguridad de la información asociados.

ID	PROPIETARIO DEL ACTIVOS DE INFORMACIÓN	NIVEL DE PROPIEDAD DEL ACTIVO DE INFORMACIÓN	ROL DEL PROCESO	ROL DE LAS PERSONAS DE LOS PROCESOS
				Estas actualizaciones se certifican mediante un documento que es generado desde el instrumento: "Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272".

Fuente: Elaborado por el proceso Gestión de tecnologías de la información de APC Colombia, septiembre 2023.

Los líderes y los responsables de los procesos institucionales, en el marco de su gestión interna y de sus procedimientos, designan el personal de su(s) equipo(s) de trabajo para la producción de información, la administración y custodia de activos de información y de

gestión de los riesgos de seguridad de la información asociados con base en los pilares de:

confidencialidad, integridad y disponibilidad.

9. METODOLOGIA PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN Y DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

9.1. Metodología de gestión de activos de información

La gestión de activos de información comienza con la identificación de estos activos por cada uno de los procesos institucionales y su correspondiente documentación en el instrumento: Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272, siguiendo el instructivo que contiene este documento para diligenciar el registro en cada uno de los campos.

A continuación, se ilustran y se detalla una serie de pasos que deben ejecutar los responsables de los procesos institucionales para esta documentación:

Ilustración 2. Identificación y documentación de activos de información

Fuente: Elaborado por el proceso Gestión de tecnologías de la información de APC Colombia, septiembre 2023.

9.1.1. Pasos para la identificación y registro de activos de información

- **Paso 1: Listar y/o registrar activos de información:** El proceso institucional tiene como base el inventario existente de sus activos de información, el cual se encuentra publicado en la sede electrónica de la Agencia. Este insumo permite listar los activos de información para validar su estado, complementación, actualización y/o eliminación.

- **Paso 2: Asociación de activos de información con las TRD:** En la documentación de los activos de información se debe identificar la pertinencia de aplicar la asociación de cada activo de información frente a las Tablas de Retención Documental (TRD), teniendo en cuenta la descripción, el tipo de activo de información y los lineamientos del proceso de gestión administrativa.

- **Paso 3: Documentar el esquema de publicación de los activos de información:** Es necesario especificar la información que caracteriza el esquema de publicación de los activos de información, por ejemplo: ámbito geográfico, idioma, lugar de consulta y almacenamiento entre otros.

- **Paso 4: Documentar la valoración del activo de información:** Los procesos institucionales deberán definir la calificación y la valoración del activo de información con relación a su nivel de importancia y su criticidad atendiendo la conformidad de la

norma ISO/IEC 27001, y la política de gobierno digital del MINTIC, y se detallan en los siguientes apartados.

- **Paso 5: Documentar la clasificación normativa del activo de información:** Los procesos institucionales en función de su producción de información deberán identificar el tipo de información de cada activo de información, conforme a la(s) normativa(s) de índole jurídico y legal de la república de Colombia, como se detalla en los siguientes apartados.

9.1.2. Clasificación por tipo de activo de información

Los tipos de activos de información se definen conforme a los criterios enunciados en la siguiente tabla, así:

Tabla 3. Lineamiento para clasificar por tipo de activo de información

ÍTEM	TIPO DE ACTIVO	DESCRIPCIÓN
1	Información	Corresponde con aquella información almacenada en formatos físicos tales como (papel, carpetas, tableros, medios magnéticos) o en formatos digitales o electrónicos como (ficheros en bases de datos, correos electrónicos, archivos de ofimática, documentos electrónicos, expedientes electrónicos, etc.) que por su criticidad y valor organizacional (cualitativo) deben ser considerados como activos de información.
2	Software	Aquellos activos informáticos con los que cuenta la entidad ya sean aplicativos, herramientas ofimáticas, código fuentes de

ÍTEM	TIPO DE ACTIVO	DESCRIPCIÓN
		software o sistemas lógicos, entre otros, que por su criticidad y valor organizacional (cualitativo) deben ser considerados como activos de información.
3	Parque computacional	Hace referencia a aquellos equipos de computación, impresoras y/o componentes de estos, que por su criticidad y valor organizacional (cualitativo) deben ser considerados como activos de información.
4	Servicios	Servicio que se brinda para el apoyo de las actividades de los procesos institucionales, tales como: Servicios WEB, intranet, portales organizacionales, cuentas de redes social, entre otros, que por su criticidad y valor organizacional (cualitativo) deben ser considerados como activos de información.
5	Infraestructura tecnológica	Corresponde a los elementos y/o conjuntos de recursos tecnológicos compartidos que soportan los sistemas de información y/o los servicios tecnológicos, que por su criticidad y valor organizacional (cualitativo) deben ser considerados como un activo de información.
6	Talento humano	Personas que, por su conocimiento, experiencia, prácticas de trabajo, administración del KNOW HOW, secreto industrial y/o comercial, hacen parte de la criticidad de un proceso institucional de alto valor organizacional (cualitativo) por lo cual deben ser considerados como activos de información.

ÍTEM	TIPO DE ACTIVO	DESCRIPCIÓN
7	Áreas Controladas	Espacios físicos demarcados y/o identificables, que contiene o almacenan conjuntos de activos de información, el cual amerita controlar su acceso de personas, o de factores ambientales, y que por su criticidad deben ser considerados como activos de información.

Fuente: Adaptación de conceptos del Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, 2018 y Guía para la gestión y clasificación de activos de información, Versión 5, 2016 MINTIC.

9.1.3. Valoración del activo de información

Los procesos institucionales deberán valorar el activo de información, determinando su nivel de criticidad, con los resultados obtenidos del nivel de importancia del activo de información.

El nivel de importancia se determina, calificando un nivel de valoración de 1 a 3 a cada pilar de la seguridad de la información (confidencialidad, integridad y disponibilidad), siendo:

1 = Baja

2 = Media

3 = Alta

Realizando la sumatoria de los tres pilares, conforme a la siguiente formulación:

NIA = Nivel de Importancia

C= Confidencialidad

I= Integridad

D= Disponibilidad

NIA = ∑ (C, I, D)

La representación del nivel de importancia es el insumo para determinar la criticidad de activo de información, con base en la siguiente representación:

Tabla 4. Pasos para realizar la valoración del activo de información

PRIMER PASO (identificación de la importancia del activo de información)						
Ítem	**(C) Confidencialidad**		**(D) Disponibilidad**		**(I) Integridad**	
	Escala cardinal	**Descripción cualitativa**	**Escala cardinal**	**Descripción cualitativa**	**Escala cardinal**	**Descripción cualitativa**
1.	(1)	BAJA	(1)	BAJA	(1)	BAJA
2.	(2)	MEDIA	(2)	MEDIA	(2)	MEDIA
3.	(3)	ALTA	(3)	ALTA	(3)	ALTA

Fuente: Elaboración del proceso Gestión de tecnologías de la Información de APC Colombia, septiembre 2023.

Tabla 5. Pasos para la valoración del activo de información

SEGUNDO PASO (identificación del nivel de criticidad del activo de información)			
Ítem	**Nivel de importancia ∑ C, D, I**	**Nivel de criticidad**	
	Escala cardinal	**Nivel**	**Descripción cualitativa**
1	Entre 3 y 4	BAJO	La afectación de los pilares de confidencialidad o integridad o disponibilidad sobre el activo de

SEGUNDO PASO (identificación del nivel de criticidad del activo de información)			
Ítem	**Nivel de importancia ∑ C, D, I**	**Nivel de criticidad**	
	Escala cardinal	**Nivel**	**Descripción cualitativa**
			información no ocasiona un impacto significativo en la operación de la Agencia. Asimismo, no representa riesgos de impacto económico y/o reputacional en la Agencia.
2	Entre 5 y 7	MEDIO	La afectación de los pilares de confidencialidad o integridad o disponibilidad sobre el activo de información puede ocasionar un impacto negativo en la operación del proceso, pero no representa riesgos de impacto económico y/o reputacional en la Agencia.
3	Entre 8 y 9	ALTO	La afectación de los pilares de confidencialidad o integridad o disponibilidad sobre el activo información puede ocasionar un impacto negativo que puede afectar la operación del proceso y/o también puede representar riesgos de impacto económico y/o reputacional en la Agencia.

Fuente: Elaboración propia del proceso Gestión de tecnologías de la información de APC Colombia, septiembre de 2023.

9.1.4. Clasificación normativa del activo de información

APC Colombia, como entidad estatal es un sujeto obligado a divulgar la información pública institucional, conforme la Ley Colombiana.

Los procesos institucionales, como productores, receptores, administradores, transformadores, y custodios de la información pública, deberán identificar las excepciones de divulgación de información de sus activos de información, conforme a las normativas de índole jurídico y legal, documentando el tipo de información del activo (información pública, información pública clasificada e información pública reservada), en el Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272, como se clasifica (según Ley 1712 de 2014).

A continuación, se ilustra un ejemplo de las definiciones del tipo de información que puede contener los activos de información, y como se clasifican, según la Ley en comento, así:

Tabla 6. Clasificación de la información según Ley 1712 de 2014

ÍTEM	NORMATIVA (Ley 1712 de 2014)	
	CLASIFICACIÓN	DESCRIPCIÓN
1	Información Pública	“Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal”.

ÍTEM	NORMATIVA (Ley 1712 de 2014)	
	CLASIFICACIÓN	**DESCRIPCIÓN**
2	Información Pública Clasificada	"Información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014".
3	Información pública reservada	Información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.

Fuente: Información tomada de la Ley 1712 de 2014 **"**Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

9.1.5. Consolidación y publicación del inventario de activos de información y de gestión de riesgos de seguridad de la información

El proceso Gestión de tecnologías de la información, es el responsable de consolidar la información de los inventarios de activos de información de cada proceso institucional y de gestionar la publicación del inventario consolidado en la sede electrónica de la Agencia

Presidencial de Cooperación internacional de Colombia - APC Colombia (portal web oficial: www.apccolombia.gov.co).

9.1.6. Lineamiento de la gestión del activo de información - Clausulado

- **Tratamiento del activo de información según su nivel de criticidad:** Los activos de información deberán tener el siguiente tratamiento según su nivel de criticidad:

Tabla 7. Lineamiento para el tratamiento de activos de información según nivel de criticidad

TRATAMIENTO DEL ACTIVO DE INFORMACIÓN SEGÚN NIVEL DE CRITICIDAD		
Ítem	**Nivel de criticidad**	**Lineamiento**
1	Alto	Los activos de información que obtengan una valoración de criticidad Alta o Media deberán tener aplicación a la gestión de riesgos de seguridad de la información por parte de los procesos institucionales.
2	Medio	
3	Bajo	Los activos de información que obtengan una valoración de criticidad baja, será opcional la aplicación de gestión de riesgos de seguridad de la información, según sean las necesidades de protección del activo de información por parte de los procesos institucionales.

Fuente: Elaboración propia del proceso Gestión de tecnologías de la información de APC Colombia, septiembre 2023.

- **Tratamiento del activo de información según clasificación de la ley 1712 de 2014:** Los activos de información deberán tener el siguiente tratamiento:

Tabla 8. Lineamiento para tratamiento de activos de información según clasificación normativa de información (Ley 1712 de 2014)

TRATAMIENTO DEL ACTIVO DE INFORMACIÓN SEGÚN NIVEL DE CLASIFICACIÓN		
Ítem	**Clasificación**	**Lineamiento de aplicación de nivel de criticidad**
1	Información Pública	Los activos de información que sean clasificados como información pública, deberán ser valorados con el nivel de importancia que determine el proceso institucional. Generalmente esta clasificación requiere valorar el pilar de integridad y disponibilidad para gestionar riesgos.
2	Información Pública Clasificada	Los activos de información se encuentren en este tipo de clasificación, deberán ser valorados con el máximo nivel de importancia y de criticidad del activo de información.
3	Información pública reservada	

Fuente: Elaboración propia del proceso Gestión de tecnologías de la información de APC Colombia, septiembre 2023.

9.2. Metodología de la gestión de riesgos de seguridad de la información

La aplicación de la metodología de gestión de riesgos utiliza como base el modelo Planear, Hacer, Verificar y Actuar (PHVA), con el fin de establecer un proceso de gestión enfocado a la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información

SGSPI, conforme al flujo de trabajo y el marco normativo. A continuación, se presenta el marco normativo de cumplimiento para esta gestión.

9.2.1. Marco normativo

Los controles que se establezcan frente a los riesgos de seguridad de la información serán confrontados frente a la norma ISO 27001 de 2022 y su Anexo A, para alinear la conformidad.

Tabla 9. Marco normativo para la gestión de riesgos de seguridad de la información

MARCO NORMATIVO	
Estándar	ISO IEC 27001:2022, requisito 6.
Lineamiento interno de APC Colombia	• Política de gestión del riesgo, Código: E-OT-008. • Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información, Código: A-OT-125

Fuente: Elaboración propia del proceso Gestión de tecnologías de la información de APC Colombia, diciembre 2023.

Tabla 10. Cumplimiento de la gestión de riesgos de seguridad de la información

Cumplimiento	Objetivos de seguridad y privacidad de la información, en el documentado: Manual de operación del SGSPI, Código: A-OT-123.
Objetivo	Identificar y gestionar los activos de información y los riesgos de seguridad de la información que, permita dar cumplimiento a los pilares de confidencialidad, integridad y disponibilidad, sobre estos activos de información de los procesos institucionales.

Alcance	Monitorear y gestionar los activos de información y los riesgos de seguridad de la información asociados.
Proceso asociado	Procesos institucionales de APC Colombia.

Fuente: Elaboración propia del proceso Gestión de tecnologías de la información de APC Colombia, diciembre 2023.

La gestión de riesgos de seguridad de la información sobre un activo de información requiere previamente realizar el ejercicio de identificar las amenazas y vulnerabilidades que pueden afectan el activo de información. Este ejercicio de identificación de amenazas y vulnerabilidades tiene un origen y un enfoque como se registra en los siguientes apartados.

9.2.2. Identificación de amenazas

Las amenazas a las que está expuesto los activos de información, se pueden clasificar según su origen, por ejemplo:

- **Deliberadas (D):** Que, se pueden presentar de forma voluntaria o intencionada.
- **Fortuito (F):** Que, se presenten de forma inesperada y/o por casualidad.
- **Ambientales (A):** Que, puedan ser ocasionados por factores asociados al medio ambiente.

Tabla 11. Ejemplo de amenazas según origen

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A

TIPO	AMENAZA	ORIGEN
Compromiso de la información	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no Autorizadas	Uso no autorizado del equipo Copia fraudulenta del Software	D, F

Fuente: Adaptación del "Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas" (MinTIC, 2018).

9.2.3. Identificación de vulnerabilidades

A continuación, se relacionan algunos ejemplos de vulnerabilidad según el tipo de activo de información:

Tabla 12. Criterios para la identificación de vulnerabilidades

TIPO DE ACTIVO DE INFORMACIÓN	EJEMPLOS DE VULNERABILIDADES
Parque computacional	Mantenimiento insuficiente de los equipos de cómputo.
	Falta de protección de los equipos por parte de los funcionarios.
Software	Ausencia pruebas de software.
	Ausencia de registros de auditoría.
	Interfaz de usuario compleja.

	Formato de fechas incorrectas.
	Ausencia de procedimiento de registro/retiro de usuarios.
	Ausencia de Documentación.
	Ausencias de mecanismos de autenticación de usuarios.
Talento humano	Falta de apropiación en seguridad.
	Entrenamiento insuficiente.
	Ausencia de Políticas de uso aceptable.
Áreas controladas	Uso inadecuado de los controles de acceso al edificio.
	Redes eléctricas inestables.
	Ausencia de proceso para supervisión de derechos de acceso.

Fuente: Adaptación del "Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas" (MinTIC, 2018)

9.2.4. Clasificación de afectación de activos de información

La identificación de un riesgo de seguridad de la información se asocia en función de un activo de información y frente a las amenazas y vulnerabilidades a las que está expuesto. Estos riesgos de seguridad de la información, se identifican desde el enfoque de afectación del activo de información que son:

- Confidencialidad
- Integridad
- Disponibilidad

A continuación, se presenta las posibles afectaciones de un activo de información en la gestión de riesgos de seguridad de la información.

Tabla 13. Clases de afectación de un activo información

ID	CLASES DE AFECTACIONES	CONTEXTO
1	Afectación en la confidencialidad	Está afectación puede presentarse cuando la información del activo es accedida por personas no pertinentes o autorizadas.
2	Afectación en la disponibilidad	Está afectación puede presentarse cuando activo de información no se encuentre en servicio en los tiempos oportunos de la Agencia y cause una denegación de los servicios de información.
3	Afectación en la integridad	Está afectación puede presentarse cuando la información del activo sufre un cambio no pertinente, causando la perdida de atributos de fiabilidad, exactitud y/o precisión de la información.
4	Afectación en la confidencialidad y disponibilidad	Este contexto es la combinación de dos tipos de afectaciones posibles en la gestión de riesgos de seguridad de la información.
5	Afectación en la confidencialidad e integridad	
6	Afectación en la disponibilidad e integridad	
7	Afectación en la confidencialidad, disponibilidad e integridad	Este contexto es la combinación de los tres (3) tipos de afectaciones posibles en la gestión de riesgos de la seguridad de la información.

ID	CLASES DE AFECTACIONES	CONTEXTO

Fuente: Elaboración propia del Proceso de gestión de tecnologías de la información de APC Colombia, septiembre de 2023.

9.2.5. ¿Cómo describir un riesgo de seguridad de la información sobre un activo de información?

Esta descripción de riesgos de seguridad de la información deberá tener en cuenta la estructura de alto nivel definida en la Guía de función pública (última versión), lo que permite facilitar su redacción, claridad y entendimiento, como se sugiere a continuación:

Tabla 4. Sugerencia en la definición del riesgo de seguridad de la información

INICIO DE LA REDACCIÓN	¿QUÉ?	¿CÓMO?	¿POR QUÉ?
Posibilidad de	Afectación económica	Por multa y sanción del ente regulador	Debido a adquisición de bienes y servicios fuera de los requerimientos normativos.
	Impacto	Causa inmediata	Causa raíz

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

9.2.6. Valoración de riesgos de seguridad y privacidad de la información

Una vez sea identificado el riesgo de seguridad de la información, este requiere ser valorado en los niveles de “Probabilidad e Impacto”, como se enuncia a continuación:

9.2.6.1. Valoración de probabilidad del riesgo de seguridad de la información

La valoración de la probabilidad de un riesgo de seguridad de la información sobre un activo de información se debe determinar en función de la frecuencia que puede conllevar la presentación del evento del riesgo de seguridad de la información, asociando un nivel de probabilidad con una unidad de medida porcentual.

Está frecuencia se puede estandarizar por prácticas empresariales y/o por la gestión del riesgo de seguridad de la información de la Agencia.

La siguiente tabla presenta los conceptos de lineamiento definidos para aplicar la valoración de la probabilidad:

Tabla 15. Identificación del nivel de probabilidad

FRECUENCIA DE ACTIVIDAD		
Valoración de probabilidad	**Frecuencia con la que se realiza la actividad**	**Nivel de probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Adoptado de la de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

9.2.6.2. Valoración del impacto del riesgo de seguridad de la información

El impacto representa las posibles consecuencias que se pueden generar a partir de la materialización de un riesgo de seguridad de la Información, y para ello, la Agencia adopta los siguientes criterios para medir el grado de afectación. La siguiente tabla identifica los criterios para identificar el nivel de impacto:

Tabla 16. Identificación del nivel de Impacto

VALORACIÓN DEL NIVEL DE IMPACTO			
Valoración del impacto a nivel económico		**Valoración del impacto a nivel reputacional**	**Nivel de impacto cuantitativo**
Cualitativa	**Posible afectación económica expresado en SMLMV**	**Posible afectación de la reputación**	
Leve	No se monetiza directamente en términos económicos, pero se expresa en reprocesos internos. (No aplica).	El riesgo afecta la imagen interna de alguna dependencia de la Agencia.	20%
Menor	No se monetiza directamente en términos económicos, pero se expresa en reprocesos internos. (No aplica).	El riesgo afecta la imagen de la entidad internamente en dos o más dependencias de la Agencia.	40%
Moderado	Menor a 10 SMLMV.	El riesgo afecta la imagen de la entidad frente al logro de los objetivos y puede transcender a nivel de junta directiva.	60%

Mayor	Entre 10 y 100 SMLMV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sectorial, nacional, departamental o municipal.	80%
Catastrófico	Mayor a 100 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido que puede trascender a nivel internacional.	100%

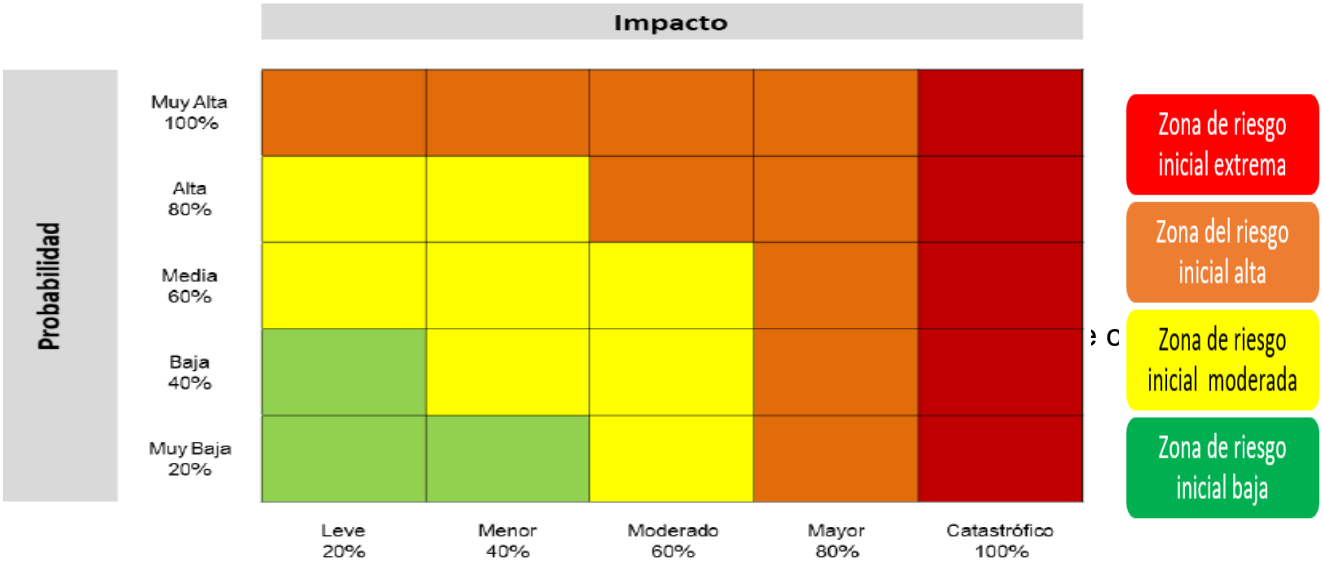
Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

9.2.7. Identificación de la zona del riesgo inherente.

La aplicación de las valoraciones de la probabilidad y del impacto, permite ubicar la zona de magnitud o severidad en el riesgo inicial o inherente.

El nivel de severidad de un riesgo se determina a partir del análisis de la probabilidad y su impacto en la herramienta Mapa de calor, donde se puede identificar las zonas de magnitud o severidad del riesgo inherente atenuado en un color, como se ilustra en la siguiente imagen:

Ilustración 3. Mapa de calor para la evaluación de riesgos de seguridad de la información



9.2.8. Lineamiento para la gestión del riesgo inherente - Clausulado:

- El tratamiento del riesgo inicial según la zona de ubicación en el mapa de calor se aplica conforme a la siguiente tabla:

Tabla 7. Tratamiento de riesgos de seguridad de la información sobre activos de información sugeridos del SGSPI

SEGÚN SEVERIDAD DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN					
Ítem	**Severidad del riesgo**	**Tratamiento sugerido**	**Modos de tratamiento**	**Modos de aplicación de tratamientos**	
1	Zona de riesgo	Reducir o evitar		Reducir: (Mitigar)	• Aplicación de controles internos y/o

SEGÚN SEVERIDAD DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN					
Ítem	**Severidad del riesgo**	**Tratamiento sugerido**	**Modos de tratamiento**	**Modos de aplicación de tratamientos**	
	inicial extrema		Reducir: (Mitigar o Transferir)		• Plan de contingencia interno.
2	Zona de riesgo inicial alta			Reducir: (Transferir)	• Tercerizar con aplicación de controles a riesgos del tercero.
			Evitar	Evitar	• El proceso debe contar o desarrollar las capacidades suficientes para anular la actividad que genera el riesgo inherente.
3	Zona de riesgo inicial moderada	Reducir o evitar	Reducir: (Mitigar)	Reducir: (Mitigar)	• Aplicación de Controles internos. • Plan de contingencia interno.
4	Zona de riesgo inicial baja	Aceptar	Aceptar	Aceptar	• Después de analizar el riesgo, el mismo se asume con las consecuencias a

SEGÚN SEVERIDAD DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN					
Ítem	**Severidad del riesgo**	**Tratamiento sugerido**	**Modos de tratamiento**	**Modos de aplicación de tratamientos**	
					partir de su posible materialización.

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

- La toma de decisión de aceptar un riesgo inicial solo aplica cuando este se encuentre en zona de riesgo bajo, teniendo como precedente que el mismo no representa una posible afectación económica.
- La toma de decisión de evitar un riesgo inicial solo es posible cuando el proceso cuenta con las capacidades para anular la actividad que genera el riesgo inherente.
- El riesgo inherente que se encuentre en la zona extrema, alta o moderada, solo puede aplicar la decisión de reducir o evitar el riesgo.
- Los líderes y responsables de los procesos institucionales deben decidir el tratamiento más conveniente para: i) proteger su activo de información con su capacidad propia o la gestión de capacidades con terceros, ii) contar con un protocolo o plan de contingencia para hacer frente a una eventual materialización de riesgos, conforme a este lineamiento.
- La gestión de controles sobre los riesgos iniciales de información debe conducir el riesgo hacia una ubicación en una zona tolerable del riesgo residual, según las necesidades del proceso, relacionada con la protección del activo de información, como se define en los siguientes apartados.

9.2.9. Mitigación del riesgo de seguridad de la información por gestión de controles

Uno de los soportes que propicia el logro de los objetivos de los procesos institucionales, se enfoca en las actividades de control que previenen la materialización de los riesgos de seguridad de la información. La valoración de los controles se obtiene así:

- **Valoración de controles según tipología:** A continuación, se define la siguiente valoración de controles según su tipología:

Tabla 18. Tipología del control del riesgo y su valoración

ÍTEM	TIPO DE CONTROL	DESCRIPCIÓN TIPO DE CONTROL	VALORACIÓN (1) DEL CONTROL V1 UNIDAD DE MEDIDA (%)
1	Preventivo	Control realizado antes que se materialice la actividad originadora de riesgo.	25%
2	Detectivo	Detecta que algo puede ocurrir, y se establecen los efectúan los controles preventivos.	15%
3	Correctivo	Control ejecutado después de haberse materializado el riesgo.	10%

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

- **Valoración de controles según su forma:** A continuación, se define la siguiente valoración de controles según su forma:

Tabla 19. Forma del control del riesgo y su valoración

ÍTEM	IMPLEMENTACIÓN DEL CONTROL	DESCRIPCIÓN	VALORACIÓN (2) DEL CONTROL V2 UNIDAD DE MEDIDA (%)
1	Automático	Se tiene herramienta definida para ejercer el control.	25%
2	Manual	El control es realizado de forma manual.	15%

Fuente: Adaptado de la guía para administración del riesgo y el diseño de controles entidades públicas, versión 6, DAFP, noviembre de 2022.

- **Otras formas de los controles:** Una forma de gestionar un control corresponde con la documentación del mismo; se sugiere que la documentación de un control sea reconocida en el Sistema de Gestión Integral (SGI). A continuación, se presenta la siguiente tabla que del estado de documentación de un control:

Tabla 20. Documentación del control

ÍTEM	DOCUMENTACIÓN DEL CONTROL	DESCRIPCIÓN	VALORACIÓN DEL CONTROL
1	Documentado	Se cuenta con evidencia documental dentro del proceso (manuales, procedimientos, guías, políticas, formatos, o cualquier documento propio del proceso.	(Sin valoración)
2	Sin documentar	Controles ejecutados en el proceso que no se encuentran documentados. Las actividades y forma de ejecución o aplicación del control son de conocimiento de personas y el proceso puede estar en riesgo de perder la información de cómo se ejecuta o se gestiona el control.	(Sin valoración)

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

La aplicación o ejecución de un control debe generar el registro de evidencias. A continuación, se presenta la siguiente tabla del estado de registro de evidencias de un control

Tabla 21. Registro de evidencias de controles

ÍTEM	EVIDENCIA DEL CONTROL	DESCRIPCIÓN	PESO DEL CONTROL
1	Con registro	Se cuenta con registro de la ejecución del control.	-
2	Sin registro	No se tiene registros de la ejecución del control.	-

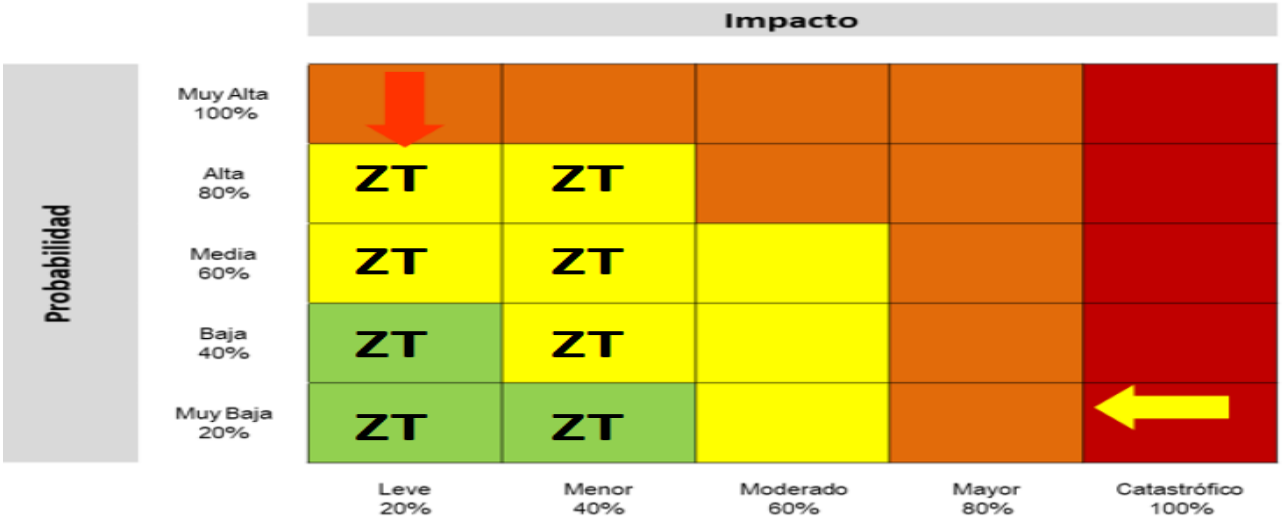
Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

- **Ecuación para la valoración del control:** El resultado de la valoración de un control es insumo inicial para medir la efectividad en función de identificar el riesgo residual. Esta valoración se expresa en una unidad de medida porcentual con la siguiente formulación:
  VC = ∑ (V1, V2)
  Dónde: VC= Valoración control, V1= Valoración 1, V2=Valoración 2.
  Una vez se obtenga la valoración del control aplicado al riesgo inicial (inherente) de seguridad de información, este riesgo obtiene una nueva ubicación en el mapa de calor.

9.2.10. Identificación del riesgo residual.

La implementación de controles frente a un riesgo inherente (inicial), permite reducirlo. Esa reducción del riesgo inherente determina un nivel de riesgo residual, que subsiste a partir de la implementación de los controles (probabilidad residual y/o impacto residual). A continuación, se presenta el movimiento del mapa de calor de un riesgo.

Ilustración 4. Zona de tolerancia de riesgos de seguridad de la información



Fuente: Adoptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, 2022, DAFP.

9.2.11. Lineamiento del riesgo residual y la zona de tolerancia - Clausulado:

- La toma de decisión de mitigar un riesgo inicial (inherente) para reducirlo, debe dar como resultado un riesgo residual. La ubicación final del riesgo residual en el mapa de calor es aceptada únicamente en la siguiente zona de tolerancia.
- Los responsables de mitigar un riesgo inherente con la aplicación de controles deberán incorporar el número de controles suficientes y solventes para tener como resultado un riesgo residual en la zona de tolerancia establecida.
- Los responsables de mitigar los riesgos sobre los activos de información, podrán aplicar otros métodos de evaluación de la eficacia de riesgos, sin eximir la reducción del mismo al riesgo residual en la zona de tolerancia.

En las otras formas de evaluar la eficacia de controles, se presentan los siguientes ejemplos:

- Aplicación de un pentesting: penetración a un ambiente de red para evaluar controles y/o determinar fallos en seguridad digital.
- Saturación de un ambiente de infraestructura tecnológica para medir la capacidad de concurrencia y performance de un sistema.
- Simulación de salida de un equipo de cómputo sin autorización de la Agencia de forma controlada en la prueba.

9.13. Lineamiento para el monitoreo y la revisión de la gestión por el esquema de las líneas de defensa - Clausulado:

- El monitoreo y revisión a la gestión de activos de información y la gestión de riesgos de seguridad por líneas de defensa se define conforme a la siguiente tabla:

Tabla 22. Líneas de defensa y acciones de operación

ID	LÍNEA	ACCIÓN DE LA OPERACIÓN
1	Línea estratégica	En este nivel se define el marco general de la gestión de riesgo y se asegura el cumplimiento de los planes de la Agencia.
2	Primera línea de defensa	Esta línea se encarga del mantenimiento efectivo de los activos de información, la gestión de los riesgos asociados, y la implementación de los controles sobre los riesgos de seguridad de información, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.

ID	LÍNEA	ACCIÓN DE LA OPERACIÓN
3	Segunda línea de defensa	• Responsable el proceso Gestión de tecnologías de la información. • Realizar la planeación y la programación de actividades y acciones para orientar a los procesos institucionales en la ejecución de la gestión de activos de información y de riesgos de seguridad de la información en el documento: Plan de seguridad y privacidad de la información, Código: A-OT-101 • Orientar a los procesos institucionales y ofrecer acompañamiento técnico para el desarrollo de las actividades de la gestión de activos de información y la gestión de riesgos de seguridad. • Realizar el monitoreo y el seguimiento al cumplimiento de los procesos institucionales frente a la ejecución de actividades de la gestión de activos de información y la gestión de riesgos de seguridad por parte del proceso. • Presentar información a la Dirección Administrativa y Financiera, Dirección General, y demás instancias de la Alta Dirección de la Agencia, sobre la gestión de activos de información y de riesgos de seguridad de la información. • Emitir los certificados sobre el número de activos de información, riegos de seguridad de la información y controles, por cada proceso institucional. • Publicar el Inventario de activos de información y de gestión de riesgos de seguridad de la información, Código: A-FO-272, en la sede

ID	LÍNEA	ACCIÓN DE LA OPERACIÓN
		electrónica. Asimismo, en la carpeta red de proceso Gestión de tecnologías de la información. • Publicar el documento: Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información, Código: A-OT-125 que, equivalen al Plan de tratamiento de riesgos de seguridad y privacidad de la información de que, trata el Decreto 612 de 2018 "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".*
4	Tercera línea de defensa	A cargo del Asesor con funciones de Control Interno y su equipo de trabajo, quienes evalúan de manera independiente y objetiva la efectividad y cobertura de los controles de la 2ª línea de defensa.

Fuente: Adaptado de la Política de gestión del riesgo de APC Colombia.

10. CONTROL DE CAMBIOS

Tabla 23. Control de Cambios

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO/ MECANISMO	DESCRIPCIÓN DEL CAMBIO
1	A-OT-125	Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información	Brújula, Diciembre 15 de 2023	Creación del documento.
2	A-OT-125	Lineamiento metodológico de gestión de activos de información y de riesgos de seguridad de la información	Brújula, Diciembre 15 de 2023	Actualización de la imagen institucional de APC Colombia, en cumplimiento de la directriz del DAPRE, con motivo del cambio de Gobierno “CHAO MARCAS”