TABLA CONTENIDO

[1. INTRODUCCIÓN 2](#_Toc133417395)

[2. ALCANCE 3](#_Toc133417396)

[3. OBJETIVO 3](#_Toc133417397)

[4. PREMISAS 3](#_Toc133417398)

[5. DEFINICIONES 4](#_Toc133417399)

[6. MARCO LEGAL Y/O NORMATIVO 10](#_Toc133417400)

[7. ROLES Y RESPONSABILIDADES DEL SGSPI 13](#_Toc133417401)

[8. CUMPLIMIENTO 18](#_Toc133417402)

[9. COMPROMISO DE LA DIRECCIÓN GENERAL 18](#_Toc133417403)

[10.1. Política general 19](#_Toc133417404)

[10.2. Políticas relacionadas 20](#_Toc133417405)

[11. CONTROL DE CAMBIOS 20](#_Toc133417406)

# INTRODUCCIÓN

El Decreto 1078 de 2015 modificado por el Decreto 767 de 2022, Establece los lineamientos generales de la Política de Gobierno Digital y subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015 con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

La Política de Gobierno Digital, es una política de Estado que ha venido evolucionando en su alcance e implementación desde su transformación de la estrategia Gobierno en Línea hasta generar en la actualidad un nuevo enfoque donde todos los actores de la sociedad son fundamentales para el desarrollo de la política. Así pues, la nueva Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos de Gobernanza, Innovación Pública Digital, Habilitadores, Líneas de Acción e Iniciativas Dinamizadoras. (MinTIC, mayo 2022).

Los Habilitadores como elemento de la Política, persiguen que los sujetos obligados como APC-Colombia, desarrollen las capacidades que les permitan ejecutar las Líneas de Acción para su implementación en el cual se encuentran: Arquitectura, Seguridad y Privacidad de la Información, Cultura y Apropiación, y Servicios Ciudadanos Digitales (Decreto 767 de 2022).

En este sentido, el presente documento habilita la capacidad del Sistema de Gestión de la Seguridad y Privacidad de la información (en adelante SGSPI) estableciendo el Marco General de los lineamientos de la Política del Sistema, que deben ser operado con aplicación de las Políticas Especificas del SGSPI y el Manual de Operación del SGSPI alineado al estándar internacional Norma ISO IEC 27001:2013 y controlados en el Sistema de Gestión Integral (SGI).

# ALCANCE

Los lineamientos establecidos de esta Política aplican para los procesos institucionales y sus usuarios de información[[1]](#footnote-1).

La especificación y detalle de los procesos institucionales se encuentra documentado en el Manual de Operación del SGSPI controlado en el SGI.

# OBJETIVO

Adoptar los lineamientos generales de la seguridad y privacidad de la información, en el marco de la Norma ISO IEC 27001:2013 y los lineamientos de la Política de Gobierno Digital del MINTIC.

**Nota:** El marco de referencia que establece los objetivos (general y específicos), así como el alcance del SGSPI se encuentran documentados en el Manual de Operación del Sistema controlado en el Sistema de Gestión Integral (en adelante SGI).

# PREMISAS

De acuerdo con el alcance definido del SGSPI que incorpora la cobertura hacia los procesos institucionales, se determinan y definen algunos principios sobre los que se van a desarrollar acciones o toma de decisiones alrededor de la protección del activo de información que estarán determinadas por las siguientes premisas:

* Identificar y valorar la criticidad de los activos de información de los procesos de la Agencia, de acuerdo con los pilares fundamentales de la seguridad de la información (confidencialidad, integridad y disponibilidad).
* Identificar, analizar y evaluar riesgos y controles; y publicar y efectuar seguimiento al mapa de riesgos de seguridad de la información para salvaguardar los activos de información, frente a posibles amenazas, tanto externas como internas, en función de la criticidad del activo de información de APC-Colombia.
* Establecer los lineamientos y definir las acciones de cumplimiento necesaria para gestionar y garantizar la seguridad y privacidad de la información.

# TÉRMINOS Y DEFINICIONES

Las definiciones son tomadas en gran parte de los lineamientos del MinTIC de la Política de Gobierno Digital, en especial del Modelo de Seguridad y Privacidad de la Información, así:

* **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia

y acceso a la información pública en posesión o bajo control de sujetos obligados (Ley 1712 de 2014, artículo 4).

* **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización (ISO/IEC 27000).
* **Activos 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).
* **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura (Ley 594 de 2000, artículo 3).
* **Aliado Técnico**: Personal natural o jurídica que según su naturaleza intercambia o es receptor de información con APC-Colombia.
* **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).
* **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo (ISO/IEC 27000).
* **Autenticidad:** Es la condición de poder identificar que el generador o receptor (interlocutor) de la información es realmente quien dice ser.
* **Autenticación:** Provisión de una garantía de que una característica afirmada por una entidad es correcta.
* **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, artículo 3).
* **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
* **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009).
* **Ciberseguridad:** Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.
* **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
* **Confidencialidad:** se define como aquella información que siendo propiedad de un proceso, área o dependencia no puede ponerse a disposición ni tampoco puede ser revelada a individuos, entidades o procesos no autorizados (Norma ISO/IEC 27000)
* **Disponibilidad:** indica que la información debe ser accesible y utilizable cuando lo requiera área, dependencia y otra entidad autorizada (Norma ISO/IEC 27000).
* **Integridad**: consiste en toda aquella información que debe salvaguardar su exactitud y completitud (Norma ISO/IEC 27000).
* **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012, artículo 3).
* **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento (Ley 1581 de 2012, artículo 3).
* **Incidente de Seguridad de la Información**: Evento o serie de eventos inesperados, que materializa un riesgo sobre un activo de información controlado o no controlado en la Política del SGSPI que puede comprometer las operaciones de la Agencia y amenazan la Seguridad y Privacidad de la Información.
* **Incidente de Seguridad Digital sobre la información**: Evento o serie de eventos inesperados, que materializa un riesgo sobre un activo de información electrónica o digital controlado o no controlado en la Política del SGSPI que puede comprometer las operaciones de la Agencia y amenazan la Seguridad y Privacidad de la Información.
* **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014 (Ley 1712 de 2014, artículo 6).
* **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 (Ley 1712 de 2014, artículo 6).
* **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008. Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
* **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).
* **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país (Ley 1581 de 2012, artículo 25).
* **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).
* **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
* **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
* **Terceros:** Personas naturales o personas jurídicas que relacionados con el SGSPI y los procesos institucionales, son sujetos de acceder, consultar, solicitar, intercambiar, transformar, producir o archivar datos e información institucional, como, por ejemplo: i) servidores públicos de APC-Colombia u otras entidades públicas, ii) contratistas, iii) entidades privadas, iv) entidades públicas, v) pasantes, vi) aliados técnicos, vii) ciudadanos.
* **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento (Ley 1581 de 2012, artículo 3).
* **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, artículo 3).
* **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO/IEC 27000).
* **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).
* **Partes interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
* **Sistema de información:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por APC-Colombia o de origen externo ya sea adquirido por la Agencia como un producto estándar de mercado o desarrollado para las necesidades de ésta.

# GLOSARIO DE SIGLAS:

* **RACE:** Responsable de Cumplir (R), Aprueba (A), Conoce (C) y Responsable de hacer Ejecutar Procedimiento (E).
* **SGI**: Sistema de Gestión Integral.
* **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información.

# MARCO LEGAL Y/O NORMATIVO

El siguiente marco normativo aplica para el SGSPI compuesto por la Política de Seguridad y Privacidad de la Información, las Políticas Específicas del SGSPI y el Manual de Operación del SGSPI, así:

* Constitución Política de Colombia, artículo 15 y 20.
* Ley 23 de 1982 sobre Derechos de Autor. Congreso de la República.
* Ley 87 de 1993, Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
* Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
* Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
* Ley 599 de 2000, Por la cual se expide el Código Penal.
* Ley 734 de 2002, Por la cual se expide el Código Disciplinario Único.
* La Ley 850 de 2003, por medio de la cual se reglamentan las veedurías ciudadanas.
* Ley 962 de 2005, Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
* Ley 1150 de 2007, Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
* Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
* Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
* Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
* Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
* 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.
* Decreto 235 de 2010, por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
* Decreto 884 de 2012, Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
* Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.
* Decreto 886 de 2014, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
* Decreto Nacional 2573 de 2014, Estrategia de Gobierno en Línea de la República de Colombia.
* Decreto 103 de 2015, títulos I, II, III, IV, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
* Decreto 1081 de 2015, capitulo 4, por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
* Decreto 1499 del 11 de septiembre de 2017, Integración del Sistema de Gestión de Calidad y lo Sistemas de desarrollo administrativo.
* Decreto 767 de 2022, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
* Decreto 1413 del 25 de agosto de 2017, Los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos.
* Decreto 612 de 2018, Las entidades del estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), deberán integrar los planes institucionales y estratégicos al Plan de Acción de que trata el Artículo 74 de la Ley 1474 de 2011.
* Decreto 620 de 2020, Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
* Decreto 767 de 2022, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
* CONPES 3701, Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
* CONPES 3854, Política Nacional de Seguridad Digital.
* CONPES 3995, Política Nacional de Confianza y Seguridad Digital.
* Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009, Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones.
* Resolución No. 507 del 5 de diciembre de 2017 “Comité Institucional de Gestión y Desempeño de APC-Colombia”
* Norma Técnica Colombiana NTC-ISO/IEC colombiana 27001:2013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

# ROLES Y RESPONSABILIDADES DEL SGSPI

| **SGSPI** | **RACE** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **RESPONSABILIDADES** | **Dirección General (Comité Institucional de Gestión y Desempeño)** | **Dirección Administrativa y Financiera** | **Comité institucional de coordinación del sistema de control interno** | **Procesos Institucionales** | **Proceso de Gestión de TI** | **Proceso de Direccionamiento Estratégico y Planeación** | **Proceso de Gestión de Talento Humano** | **Procesos de Gestión de Comunicaciones** | **Proceso de Evaluación Control y Mejora** |
| **ROLES** |
| Conocer y adoptar la Política de la Seguridad y Privacidad de la Información. | R,A,E,C | R,C | R,C | R,C | R,E,C | R,C | R,C | R,C | R,C |
| Conocer y adoptar la política de Teletrabajo | R,A,E,C | R,C | R,C | R,C | R,C | R,C | R,E,C | R,C | R,C |
| Conocer y adoptar el Plan Estratégico de Comunicaciones | R,A,E,C | R,C | R,C | R,C | R,C | R,C | R,C | R,E,C | R,C |
| Conocer y adoptar el mapa de riesgos de seguridad de la información | R,E,C | R,C | R,A,E,C | R,C | R,C | R,C | R,C | R,C | R,E,C |
| Adoptar el plan de auditoria interna | R,A,E,C | R,C | R,C | R,C | R,C | R,C | R,C | R,C | R,E,C |
| Programar, liderar, adoptar y mantener la práctica de auditoria externa de certificación del SGSPI en la conformidad de la NTC ISO IEC 27001:2013 | R,C | R,A,E,C | R,A,E,C | R,C | R,E,C | R,C | R,C | R,C | R,C |
| Reportar los eventos e incidentes de seguridad de información y de seguridad digital que afecten los activos de información | R,C | R,C | R,C | R,C | R,E,C | R,C | R,C | R,C | R,C |
| Gestionar los eventos e incidentes de seguridad de la información y seguridad digital | R,C | R,C | R,C | R,C | R,E,C | R,C | R,C | R,C | R,C |
| **TIPO DE PARTICIPACIÓN:**  R= Responsable de Cumplir  A= Aprueba  C= Conoce  E= Responsable de hacer Ejecutar Procedimiento | | | | | | | | | |

**Fuente:** Creación del proceso Gestión de tecnologías de la información de APC-Colombia, Abril de 2023.

**Nota:** El Comité Institucional de Gestión y Desempeño (CIGD), fue creado mediante la Resolución No. 507 del 5 de diciembre de 2017, y en su artículo noveno y tiene el propósito de coordinar y apoyar la implementación del Modelo de seguridad y privacidad de la Información en APC-Colombia, conforme a la Política de Gobierno Digital, antes Gobierno en Línea del MinTIC (Decreto 767 de 2022).

# CUMPLIMIENTO

La política de seguridad y privacidad de la información contenida en este documento, las *políticas específicas del sistema de gestión de seguridad y privacidad de la información* deberán ser documentados en el Sistema de Gestión Integral (SGI), codificados, reconocidos, aceptados y cumplidos por APC-Colombia, por sus servidores públicos, y la agencia velará por el cumplimiento de las partes interesadas y grupos de valor.

APC-Colombia reglamentará los procedimientos, actividades y/o acciones de cumplimiento de la Política en su Manual de operación del SGSPI asociado al proceso de Gestión de TI.

El incumplimiento de la política de seguridad y privacidad de la información y las políticas específicas del sistema de gestión de la seguridad y privacidad de la información por parte de los servidores públicos se considerará un incidente de seguridad de la información, que según sea el caso su naturaleza, generará los siguientes eventos:

* El incidente de seguridad de la información deberá ser gestionado conforme a sus procedimientos de cumplimiento del Proceso de Gestión de TI.
* En los eventos de que el incumplimiento de estas políticas, afecte la seguridad de la información institucional en sus pilares de Integridad, Confidencialidad y Disponibilidad, de forma dolosa o por mera negligencia, APC-Colombia se reserva el derecho de iniciar el debido proceso conforme a la normatividad vigente.

# COMPROMISO DE LA DIRECCIÓN GENERAL

En el marco del Comité Institucional de Gestión y Desempeño de APC-Colombia (CIGD) se sometió la aprobación de la Política De Seguridad y Privacidad de la Información el cual se encuentra documentado y controlado en el Sistema de Gestión Integral (SGI) con participación de la alta dirección según lineamiento del comité establecido mediante Resolución No. 507 del 5 de diciembre de 2017.

APC-Colombia reglamenta el cumplimiento de revisión por la dirección general en su manual de operación. Así mismo, la instancia del CIGD y el proceso de gestión de TI analizan y determinan la oportunidad de actualización de:

* Política de seguridad y privacidad de la información
* Políticas específicas del sistema de gestión de la seguridad y privacidad de la información
* Cualquier instrumento que se incorpore al SGSPI

1. **POLÍTICA**

## Política general

APC-Colombia, se compromete a preservar la confidencialidad, disponibilidad e integridad de sus activos de información que permita a la Agencia, partes interesadas y grupos de valor, adoptar medidas de protección, mediante una eficiente y eficaz gestión de los riesgos en seguridad de la información, acorde con los lineamientos estratégicos y la misión de la Agencia, promoviendo la mejora continua en materia de seguridad y privacidad de la información.

En este sentido, APC-Colombia gestiona el SGSPI conforme al cumplimiento de la Norma ISO IEC 27001:2013 declarado en el documento A-OT-121 Declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información, reconocido en el SGI, así como sus excepciones.

## Políticas relacionadas

APC-Colombia tiene definido lineamientos específicos del SGSPI en el documento: A-OT-100 Políticas específicas del sistema de gestión de seguridad y privacidad de la información.

# CONTROL DE CAMBIOS

| **VERSIÓN** | **CÓDIGO** | **NOMBRE DEL DOCUMENTO** | **ACTO/ MECANISMO** | **DESCRIPCIÓN DEL CAMBIO** |
| --- | --- | --- | --- | --- |
| 1 | DA-D-011 | Política de seguridad y privacidad de la información | Acta, 55 Octubre 7 de 2014 | Nuevo 09/06/2014 |
| 2 | DA-D-011 | Política de seguridad y privacidad de la información | No tiene | Actualización imagen institucional 27/10/2014 |
| 3 | DA-D-011 | Política de seguridad y privacidad de la información | Acta, Julio 23 de 2015 | Se incluye nuevos controles en seguridad de las comunicaciones, seguridad de la red, seguridad física, tercerización |
| 4 | A-OT-011 | Política de seguridad y privacidad de la información | Acta, Diciembre 22 de 2015 | Cambió el código del documento. Incluyó nueva dirección de la entidad. Se ajusta la forma |
| 5 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Marzo 14 de 2017 | Se ajusta a la nueva imagen institucional |
| 6 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Octubre 30 de 2018 | Actualización de la política conforme a los nuevos lineamientos de MINTIC |
| 7 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Noviembre 13 de 2018 | Ajuste imagen institucional y versión |
| 8 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Noviembre 8 de 2019 | Ajustada la imagen institucional |
| 9 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Diciembre 30 de 2020 | Actualización de política de seguridad y privacidad de la información |
| 10 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Febrero 12 de 2022 | Se actualizó el documento en cuanto a la estructura y redacción. Se relacionaron las políticas específicas del SGSI |
| 11 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Diciembre 20 de 2022 | Actualización del logo institucional de APC-Colombia |
| 12 | A-OT-011 | Política de seguridad y privacidad de la información | Brújula, Abril 05 de 2023 | Se actualiza política de Seguridad de la información en la que se incluye el compromiso de los requisitos aplicables relacionados con seguridad y privacidad de la Información, planificación de revisión, y los objetivos de Seguridad de la Información, así como la conformidad de la Norma ISO IEC 27001:2013 |

1. Los usuarios de información de los procesos institucionales, corresponden con servidores públicos, contratistas, aliados técnicos y demás terceros que por su naturaleza usan, producen, procesan, intercambian o gestiona información institucional de APC-Colombia. [↑](#footnote-ref-1)