



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

**POLÍTICA DE SEGURIDAD Y  
PRIVACIDAD DE LA INFORMACIÓN**  
Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

# POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

APC-COLOMBIA

**CONTENIDO**

- 1. INTRODUCCIÓN.....4
- 2. OBJETIVO.....4
- 3. ALCANCE.....5
- 4. PREMISAS.....5
- 5. DEFINICIONES.....6
- 6. PRINCIPIOS DEL SGSI .....8
- 7. ROLES Y RESPONSABILIDADES DENTRO DEL MSPI Y SGSI..... 10
  - 7.1. ROLES..... 11
    - 7.1.1. ROL DE LA SEGURIDAD DE LA INFORMACIÓN..... 11
    - 7.1.2. ROL DE SEGURIDAD DIGITAL..... 13
- 8. RESPONSABILIDADES..... 14
  - 8.1. GENERALES..... 14
  - 8.2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO (CIGD)..... 15
  - 8.3. DIRECCIÓN GENERAL..... 16
  - 8.4. PROCESOS..... 17
    - 8.4.1. DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN..... 16
    - 8.4.2. EVALUACIÓN, CONTROL Y MEJORAMIENTO.....17
    - 8.4.3. GESTIÓN JURÍDICA.....17
    - 8.4.4. GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.....17
    - 8.4.5. GESTIÓN DE TALENTO HUMANO.....20
    - 8.4.6. GESTIÓN CONTRACUAL.....20
    - 8.4.7. GESTIÓN ADMINISTRATIVA.....20
- 9. MARCO LEGAL Y/O NORMATIVO.....21
- 10. COMPROMISO DE LA DIRECCIÓN GENERAL.....24
- 11. CUMPLIMIENTO.....25
- 12. POLÍTICA.....25
  - 12.1. POLÍTICA GENERAL..... 25

12.2. POLÍTICAS RELACIONADAS ..... 26

13. CONTROL DE CAMBIOS.....26

## 1. INTRODUCCIÓN

La Agencia Presidencial de Cooperación Internacional de Colombia APC-Colombia, para asegurar el Modelo de Seguridad y Privacidad de la Información (MSPI) debe adoptar controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el Modelo.

Este documento describe la política general y especifica la de seguridad y Privacidad de la Información por APC-Colombia. Para la definición de esta política se tomaron como base la normatividad y las regulaciones aplicables.

La política incluida en este documento se constituye en parte fundamental del Sistema de Gestión de la Seguridad de la Información (SGSI), integrado en el Sistema de Gestión Integral (SGI) de la Agencia.

## 2. OBJETIVO

Establecer los lineamientos que conduzcan a la preservación de la confidencialidad, integridad, disponibilidad de la información, a partir del establecimiento de políticas, controles, procedimientos, promoción de la cultura de privacidad y seguridad, y mediante la gestión de los riesgos de seguridad de la información para brindar confianza a las partes interesadas y grupos de valor y contribuir al logro de los objetivos de la Agencia Presidencial de Cooperación Internacional de Colombia, APC Colombia.

### 2.1. OBJETIVOS ESPECÍFICOS

Todos los procesos y los sistemas de gestión de la Agencia Presidencial de Cooperación Internacional de Colombia, APC-Colombia.

- Asegurar el cumplimiento de los requerimientos legales y regulatorios vigentes en materia de seguridad y privacidad de la información para evitar sanciones, daños a los particulares y la pérdida de imagen de APC-Colombia.
- Generar cultura de privacidad y seguridad de la información para las partes interesadas y grupos de valor demás grupos de interés, mediante la definición de una estrategia de uso y apropiación de la presente política y sus políticas relacionadas.

### **3. ALCANCE**

La presente política de seguridad y privacidad de la información debe ser aplicada por todos los procesos y los sistemas de gestión de la Agencia Presidencial de Cooperación Internacional de Colombia APC Colombia.

### **4. PREMISAS**

De acuerdo con la política del SGSI, su alcance definido en el que se involucran a partes interesadas y grupos de valor, se determinan y definen algunos principios sobre los que se van a desarrollar acciones o toma de decisiones alrededor de la protección de la información que estarán determinadas por las siguientes premisas:

- Identificar y valor los activos de información de los procesos de la Agencia, de acuerdo con los principios fundamentales de la seguridad en el manejo de la información (confidencialidad, integridad y disponibilidad).



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- 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 importancia de la información de APC-Colombia.
- Aportar a la innovación tecnológica que permita proteger la información de APC-Colombia, a medida que la tecnología avanza y las necesidades de seguridad y privacidad evolucionan, permiten mejorar los productos y/o servicios para todos.
- Actualizar los lineamientos y la documentación necesaria para gestionar y garantizar la seguridad y privacidad de la información.

### 5. DEFINICIONES

**MSPI:** Modelo de Seguridad y Privacidad de la Información.

**S.I.G:** Sistema de Información Geográfica.

**SGSI:** Sistema de Gestión de Seguridad de la Información.

**Sistema de información:** Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.

**Integridad:** Hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

**Confidencialidad:** Es la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

**Disponibilidad:** Hace referencia a que la información debe permanecer accesible a elementos autorizados.

**Incidente de seguridad:** es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura de información y tecnología de APC-Colombia (sistemas de cómputo, sistemas de información, sistemas de telefonía), como pueden ser: ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, crímenes definidos en la ley 1273 de 2009 u otras normas que cobijen a la entidad.

**Incidente de seguridad computacional:** es una violación o potencial amenaza de violación de las políticas de seguridad de la información, los procedimientos de seguridad de la información o la reglamentación que cobija el uso de los servicios o equipos de información de tecnología. Algunos ejemplos de incidente computacional incluyen:

**Denegación de servicios:** un atacante envía un paquete de datos que bloquea o congestiona el servidor de páginas web y suspende el sitio web. Un atacante coordina a miles de estaciones de trabajo externas a la red para que envíen miles

de solicitudes ICMP (protocolo de control de mensajes de internet) a la red de la entidad para que se inhabiliten los servicios de red.

**Código malicioso:** un gusano informático usa archivos compartidos para contaminar cientos de estaciones dentro de la entidad. La entidad recibe un reporte del vendedor de sus antivirus en donde alerta de un virus que se dispersa a gran velocidad mediante correo electrónico por Internet. El virus aprovecha una vulnerabilidad presente en los servidores de la entidad, basado en la experiencia de la entidad en otros incidentes se estima que el virus podría afectar a los equipos en un lapso de tres horas.

**Acceso no autorizado:** un atacante utiliza una herramienta de explotación de vulnerabilidades para tener acceso al archivo de password de usuarios. Un perpetrador obtiene acceso no autorizado a nivel de administrador a un servidor y a la información confidencial que contiene y luego intimida a la víctima amenazando la de divulgar a la prensa a la información si no realiza el pago de un dinero.

**Uso inapropiado:** un usuario entrega copias de software de la entidad a personas no autorizadas. Una persona amenaza a otra vía correo electrónico.

## 6. PRINCIPIOS DEL SGSI

APC-Colombia apropia doce (12) principios en el marco del SGSI para su implementación exitosa.

- Definir, implementar, operar y mejorar de forma continua y cíclica la protección de la información en el SGSI y la soporta en lineamientos o



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

políticas claras acordes a las necesidades de la Agencia y los requerimientos normativos.

- Establecer las responsabilidades de la protección de la información, las cuales son aceptadas y publicadas por y para todas las partes interesadas y grupos de valor.
- Proteger la información generada, administrada, procesada o custodiada por los procesos, su infraestructura y los controles de acceso.
- Proteger la información creada, procesada, transmitida o en custodia con el fin de minimizar los impactos de la materialización de los riesgos que afectan los principios de seguridad y privacidad de la información.
- Sensibilizar al personal de la Agencia, partes interesadas y grupos de valor, con el propósito de prevenir ataques provenientes de amenazas externas y/o internas.
- Establecer y socializar los lineamientos necesarios para proteger las instalaciones de procesamiento electrónico de datos y de infraestructura tecnológica que soporte la información crítica de la Agencia.
- Garantizar la seguridad y privacidad de la información en la operación de los recursos tecnológicos y las redes de telecomunicación.
- Definir e implementar controles de acceso a la información para los sistemas de información y recursos de red.
- Garantiza la inclusión de la seguridad de la información en el ciclo de vida del desarrollo de los sistemas de información.
- Garantizar la adecuada gestión de los eventos de seguridad y privacidad de la información y su socialización a los organismos de vigilancia y control.
- Garantizar la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueda generar.

- Fomentar el cumplimiento de las obligaciones legales y los requisitos regulatorios y contractuales que se establezcan en el marco de la protección de la información.

## **7. ROLES Y RESPONSABILIDADES DENTRO DEL MSPI Y SGSI**

Con el fin de dar dirección y apoyo gerencial que permita realizar la gestión y el desarrollo de las iniciativas sobre seguridad y privacidad de la información, en el marco de la Estrategia de Gobierno Digital, en cumplimiento de la legislación vigente y la gestión efectiva de los riesgos de seguridad de la información.

APC-Colombia establece los siguientes roles y responsabilidades:

- Aplicar los lineamientos definidos en la norma técnica colombiana NTC ISO/IEC 27001:2013, que describe cómo gestionar la seguridad de la información en una empresa.
- Informar a la Dirección Administrativa y Financiera sobre el desempeño de la gestión de la seguridad y privacidad de la información, mediante informe remitido mediante las herramientas: Sistema de Gestión Documental de Orfeo o Correo electrónico o el Sistema de Gestión Integral de Brújula.
- Analizar, identificar, gestionar, evaluar, controlar y publicar los riesgos de seguridad y privacidad de la información.
- Proteger los activos de seguridad y privacidad de la información.
- Ejecución de procesos de seguridad y privacidad específicos.

A continuación, se describen las responsabilidades definidas:



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

### **7.1. ROLES**

#### **7.1.1. ROL DE LA SEGURIDAD DE LA INFORMACIÓN**

- Diseñar, implementar y realizar seguimiento a planes de tratamiento de los riesgos de seguridad de la información.
- Identificar, seleccionar e implementar mecanismos, controles y herramientas tecnológicas necesarias para realizar el tratamiento de riesgos de seguridad de la información.
- Diseñar, revisar o actualizar políticas y lineamientos en materia de seguridad de la información.
- Apoyar a APC-Colombia en las actividades de divulgación y promoción de la importancia del SGSI, los beneficios de la seguridad de la información para la Agencia y las implicaciones de la no conformidad con los requisitos del SGSI.
- Participar en la implementación de los controles de seguridad de la información requeridos por la Agencia para el cumplimiento de sus objetivos.
- Atender las mediciones de la efectividad de los controles de seguridad de la información implementados.
- Elaborar y socializar propuestas de programas de toma de conciencia y formación en seguridad de la información.
- Verificar el cumplimiento de las normas y políticas de seguridad informática de APC-Colombia, mediante revisiones periódicas del estado de la seguridad de los diferentes servicios, sistemas de información y componentes de tecnología que permiten el tratamiento de la información de la Agencia.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Verificar el cumplimiento de la seguridad a nivel de operación, desarrollo e implementación de los sistemas de información y las bases de datos.
- Coordinar las acciones necesarias para identificar, controlar, reducir y evaluar incidentes de seguridad de la información.
- Participar activamente en la construcción, actualización, publicación, socialización y difusión de la documentación que soporta el SGSI de APC-Colombia.
- Aplicar los controles y realizar el seguimiento necesario a los riesgos en intervalos periódicos para determinar la efectividad de los controles implementados, las oportunidades de mejora y las acciones correctivas necesarias.
- Apoyar a las diferentes direcciones / dependencias de APC-Colombia en la identificación, valoración y tratamiento de los riesgos de seguridad de la información (revisión periódica del panorama de los riesgos: descripción, definición de criterios, implementación de variables y aceptación de riesgos y controles de seguridad de la información).
- Apoyar a APC-Colombia en las actividades de implementación del MPSI de la estrategia establecida por el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC).
- Elaborar informes del estado de la seguridad y privacidad de la información, la efectividad de los controles, indicar alertas para toma de decisiones, análisis de recomendaciones / sugerencias para implementar medidas, acciones preventivas o correctivas sobre la gestión de la seguridad y privacidad de la información.
- Preparar la información necesaria para realizar la revisión periódica del estado de la seguridad y privacidad de la información y acompañar a APC-Colombia en el fortalecimiento, implementación y seguimiento del SGSI conforme a las necesidades de la Agencia.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Recolectar, organizar y presentar a la dirección general la información sobre el desempeño del SGSI para la preparación de las auditorías internas y la revisión por parte de la Alta Dirección del estado del Subsistema de SGSI., esta deberá ser presentada en Comité institucional de gestión y desempeño
- Proponer, diseñar y fomentar la implementación de mejoras a los controles y herramientas tecnológicas necesarias para el fortalecimiento de la seguridad y privacidad de la información en la Agencia.
- Formular los planes de mejoramiento y realizar seguimiento a las acciones correctivas o preventivas para responder a incidentes de seguridad y privacidad de la información detectados, medir su efectividad y socializar las acciones adelantadas a los interesados y partes pertinentes.

### **7.1.2. ROL DE SEGURIDAD DIGITAL**

- Atender eventos e incidentes de seguridad de la información que sean identificados y coordinar a los recursos dispuestos por la Agencia para la identificación, control y recuperación de la Infraestructura de Tecnología de Información y Comunicaciones de la Agencia.
- Formular los planes de mejoramiento y realizar seguimiento a las acciones correctivas o preventivas para responder a incidentes de seguridad digital detectados, medir su efectividad y socializar las acciones adelantadas a los interesados y partes pertinentes.
- Investigar, evaluar y recomendar el uso de herramientas de última tecnología que permitan proteger la infraestructura informática de la Agencia.
- Elaborar y ejecutar los planes operativos anuales y de mejoramiento relacionados con la seguridad informática, de acuerdo con la metodología diseñada por la Agencia.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Verificar el cumplimiento de la seguridad a nivel de operación de los sistemas de comunicaciones (Red LAN – WAN).
- Participar activamente en la evaluación de los cambios a nivel de infraestructura de tecnología de información y comunicaciones para determinar los riesgos de seguridad, las medidas de mitigación y las acciones correctivas en caso de incidentes de seguridad de la información.
- Gestionar y realizar análisis de vulnerabilidades técnicas, plan de remediaciones y presentar el informe al responsable de la seguridad de la información.
- Apoyar a APC-Colombia en las actividades de implementación de la estrategia de ciberdefensa definida por el Ministerio de Defensa Nacional.
- Realizar la ejecución y seguimiento de las responsabilidades del proceso de Gestión de Tecnologías de la Información, asociadas con la seguridad informática.
- Realizar la identificación, análisis y tratamiento de los riesgos de seguridad informática.
- Verificar y analizar que los desarrollos de software de la Agencia, cumplan con criterios y estándares de software seguro.
- Realizar análisis y pruebas a base de datos para conexiones seguras y gestionar la actualización de los sistemas operativos.

## 8. RESPONSABILIDADES

### 8.1. GENERALES

- Apoyar y velar por la formación de Auditores Internos en NTC ISO 27001:2013.

- Apoyar la identificación de los activos de información de APC-Colombia y la definición de las responsabilidades de protección apropiadas, de acuerdo con lo estipulado en el Anexo A.8.
- Asegurar la privacidad y protección de los datos personales como se exige en la ley 1581 de 2012 con el apoyo de las diferentes áreas de la entidad, de acuerdo con lo estipulado en A.18.1.4.
- Identificar clasificar y valorar los activos de información.
- Identificar la información que contiene datos personales, teniendo en cuenta la ley 1581 de 2012.

## **8.2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO (CIGD)**

Que el CIGD fue creado mediante la Resolución No. 507 del 5 de diciembre de 2017, y en su Artículo Noveno. Políticas de Gestión y Desempeño. Adoptar las políticas de gestión y desempeño, que se describen a continuación:

- Gobierno Digital, antes Gobierno en Línea
- Seguridad Digital<sup>1</sup>.

Por medio de las cuales se dan lineamientos y estándares para:

- Coordinar y apoyar la implementación del Modelo de seguridad y privacidad de la Información en APC-Colombia.
- Revisar y aprobar las actualizaciones y los nuevos lineamientos en materia de seguridad de la información

<sup>1</sup> <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Presentar a la alta dirección los requerimientos presupuestales para la implementación y mantenimiento del Modelo de seguridad y privacidad de la información en APC-Colombia.
- Evaluar y aprobar los planes de tratamiento de riesgos de seguridad de la información.
- Aprobar los programas de pruebas y análisis de vulnerabilidades de la infraestructura tecnológica.
- Verificar el cumplimiento de las políticas de seguridad y emitir recomendaciones sobre la materia.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Realizar revisiones periódicas del Sistema de Gestión de Seguridad de la Información- SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

### **8.3. DIRECCIÓN GENERAL**

- La dirección general debe mostrar liderazgo y compromiso frente al SGSI, asegurando que se establezca la política del Sistema de Gestión de Seguridad de la Información y los objetivos de este, siendo estos definidos de acuerdo con la misión y visión de la Agencia.
- Apoyar la integración del SGSI con los procesos de la Agencia, garantizando recursos económicos y de personal, así como impulsar y asegurar que todos los servidores públicos y contratista conozcan y apliquen las políticas y procedimientos establecidos en temas de seguridad de la información.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Asegurarse de hacer seguimiento a la implementación del SGSI y que este logre los resultados previstos con eficacia.
- Definir, asignar, notificar, publicar y socializar las responsabilidades y los roles de seguridad y privacidad de la información, velar por su cumplimiento de acuerdo con lo estipulado en el A.6.1.1.

### 8.4. PROCESOS

#### 8.4.1. DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN

- Integrar la seguridad de la información en la gestión por proyectos, independientemente del tipo de proyecto, así tratara los riesgos de seguridad de la información, de acuerdo con lo estipulado en el Anexo A.6.1.5.
- Definir un control para los cambios en APC-Colombia aplicados en los procesos, en las instalaciones y en el Sistema de Gestión Integral que afectan la seguridad de la información, de acuerdo con lo estipulado en el Anexo A.12.1.2.

#### 8.4.2. EVALUACIÓN CONTROL Y MEJORAMIENTO

- Apoyar en la revisión independiente de la seguridad de la Información (Contratar un externo para auditorías internas de conformidad con el numeral 9.2 de la NTC ISO 27001:2013 “(…)La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información (…)”).
- Formar Auditores Internos en NTC ISO 27001:2013



### **8.4.3. GESTIÓN JURÍDICA**

- Brindar asesoría jurídica frente al régimen aplicable para el manejo y seguridad de la información.
- Emitir concepto sobre el régimen aplicable a los acuerdos de confidencialidad. O no divulgación teniendo en cuenta las necesidades de APC-Colombia.
- Asesorar con el fin de evitar el incumpliendo en las obligaciones legales o contractuales relacionadas con la seguridad de la información.

### **8.4.4. GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

- Garantizar las configuraciones seguras que permitan prevenir los riesgos que se puedan presentar por el uso de dispositivos móviles de acuerdo con lo estipulado en el Anexo A.6.2.1.
- Implementar medidas de aseguramiento a la información que se acceda a través del teletrabajo de acuerdo con lo estipulado en el Anexo A.6.2.2.
- Definir procedimientos para la gestión de medios removibles cuando se reutilicen, se den de baja y proteger la información que contienen, acuerdo con lo estipulado en el Anexo A.8.3.1.
- Limitar el acceso a la información y a las instalaciones de procesamiento de la información con base en los requisitos de APC-Colombia y de Seguridad de la Información, apoyados por los responsables o coordinadores de cada área, contractual y talento humano de acuerdo con lo estipulado en el Dominio A.9.
- Asegurar el uso apropiado y eficaz para proteger la confidencialidad, autenticidad y/o la integridad de la información mediante el cifrado de la información, apoyados por los responsables o coordinadores de cada área, de acuerdo con lo estipulado en el Dominio A.10.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Prevenir la pérdida, daño o robo de equipos que puedan comprometer la información o la operación de APC-Colombia de acuerdo con lo estipulado en el Anexo A.11.2.
- Definir ambientes separados desarrollo, pruebas y operación con el fin de reducir los riesgos de acceso o cambios no autorizados en la operación de los sistemas de información de acuerdo con lo estipulado en el Anexo A.12.1.4.
- Realizar seguimiento al uso de los recursos, ajustar y proyectar los requisitos de capacidad futura con el fin de asegurar el desempeño requerido del o los sistemas de acuerdo con lo estipulado en el Anexo A.12.1.3.
- Asegurar la información y las instalaciones de procesamiento de información se encuentren protegidas contra código malicioso de acuerdo con lo estipulado en el Anexo A.12.2.
- Proteger contra la pérdida de datos, mediante respaldos de la información, software e imágenes de los sistemas, y ponerlas a pruebas regularmente, apoyados por los responsables o coordinadores de cada área, de acuerdo con lo estipulado en el Anexo A.12.3.
- Registrar, conservar y revisar los registros acerca de actividades del usuario para generar evidencias de excepciones, fallas y eventos de seguridad de la información de acuerdo con lo estipulado en el Anexo A.12.4.
- Implementar procedimientos para controlar la instalación Software Operacional en los sistemas operativos de acuerdo con lo estipulado en el Anexo A.12.5.1.
- Prevenir el aprovechamiento de cualquier vulnerabilidad técnica que se pueda presentar mediante la gestión de la vulnerabilidad técnica de acuerdo con lo estipulado en el Anexo A.12.6.



- Planificar y acordar cuidadosamente auditorías que involucren la verificación de los sistemas operativos de acuerdo con lo estipulado en el Anexo A.12.7.
- Asegurar que la Seguridad de la Información se integre durante todo el ciclo de vida en el proceso de desarrollo y soporte de sistemas de información incluyendo los sistemas de información que prestan servicios sobre redes públicas de acuerdo con lo estipulado en el Dominio A.14.
- Asegurar la protección de la información en las redes, sus instalaciones de proceso, protegiéndola al ser transferida mediante cualquier medio de acuerdo con lo estipulado en el Anexo A.13.

#### **8.4.5. GESTIÓN DE TALENTO HUMANO**

- Implementar políticas de aseguramiento a la información que se acceda a través del teletrabajo.
- Asegurar, que los empleados comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, tomando conciencia de sus responsabilidades en la protección de la información y las cumplan.

#### **8.4.6. GESTIÓN CONTRACTUAL**

- Asegurar, que los contratistas y proveedores comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, tomando conciencia de sus responsabilidades en la protección de la información.
- Definir y documentar junto con los responsables de la información, acuerdos sobre transferencia segura de información.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- Identificar, revisar regularmente y documentar junto con los responsables de la información, los requisitos para los acuerdos de confidencialidad o no divulgación teniendo en cuenta las necesidades de APC-Colombia.
- Identificar y definir documentar junto con los responsables de la información, los mecanismos para asegurar la protección de la información que sea accesible a los proveedores.

### **8.4.7. GESTIÓN ADMINISTRATIVA**

- Garantizar la verificación de entrega por parte de los servidores públicos y contratistas de todos los activos asociados con la información e instalaciones de procesamiento.
- Prevenir el acceso físico no autorizado a las áreas identificadas como críticas por la información que contienen, administran o generan.
- Identificar y definir documentar junto con los responsables de la información, los mecanismos para asegurar la protección de la información que sea accesible a los proveedores.
- Implementar y documentar un procedimiento para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por APC-Colombia.
- Proteger contra el acceso no autorizado, uso indebido o corrupción durante el transporte los medios que contienen información.

## **9. MARCO LEGAL Y/O NORMATIVO**

- Constitución Política de Colombia, artículo 15 y 20.
- Ley 23 de 1982, sobre Derechos de Autor. Congreso de la República.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- 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



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

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, capítulo 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 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.



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

- 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 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Decreto 620 de 2020, Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- 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.
- NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

### **10. COMPROMISO DE LA DIRECCIÓN GENERAL**

La alta dirección aprueba esta política como parte de su compromiso y apoyo en el diseño e implementación del Modelo de Seguridad y Privacidad de la Información para garantizar la seguridad y privacidad de la información de APC-Colombia.

## 11. CUMPLIMIENTO

La política de seguridad y privacidad de la información contenida en este documento y las *políticas específicas del sistema de gestión de seguridad y privacidad de la información*, deberán ser reconocidas aceptadas y cumplidas por APC-Colombia y las partes interesadas y grupos de valor.

El incumplimiento de esta se considerará un incidente de seguridad, que, de acuerdo con el caso, podrá dar lugar a un proceso disciplinario para los servidores públicos, y se podrá convertir en un incumplimiento del contrato respecto a los contratistas, que pueda dar lugar a la imposición de sanciones e incluso a la terminación del contrato, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

## 12. POLÍTICA

### 12.1. POLÍTICA GENERAL

APC-Colombia, se compromete a preservar la confidencialidad, disponibilidad e integridad de sus activos de información que permita a APC-Colombia, 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 caso de incumplimiento de la política general seguridad y privacidad de la información, APC-Colombia iniciará las investigaciones disciplinarias correspondientes, conforme a lo dispuesto en la Ley 734 del 2002.

**12.2. POLÍTICAS RELACIONADAS**

A continuación, se mencionan las políticas que se encuentran en el documento políticas específicas del SGSI y que se relacionan con el presente documento:

- Política para Dispositivos móviles
- Política de Trabajo en casa
- Política Uso aceptable de activos
- Política de Usos tecnológicos de comunicación y acceso a Internet
- Política de Control de acceso
- Política Uso de controles criptográficos - gestión de llaves
- Política Escritorio y pantalla limpios
- Política Copias de respaldo
- Política Transferencia de información
- Política Desarrollo seguro
- Política de Relación con proveedores

**13.CONTROL DE CAMBIOS**

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO	CONTROL DE CAMBIOS
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	No tiene	Actualización imagen



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO	CONTROL DE CAMBIOS
		la Información		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 comunicacione s, seguridad de la red, seguridad física, tercerización
4	A-OT-011	Política de Seguridad y Privacidad de la Información	Acta, Diciemb re 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



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO	CONTROL DE CAMBIOS
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



El futuro  
es de todos

APC Colombia  
Agencia Presidencial de  
Cooperación Internacional

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: A-OT-011 - Versión: 10 - Fecha: Febrero 10 de 2022

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO	CONTROL DE CAMBIOS
		la Información		redacción. Se relacionaron las políticas específicas del SGSI