**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 3](#_Toc180141945)

[2. OBJETIVOS 4](#_Toc180141946)

[2.1. Objetivo general. 4](#_Toc180141947)

[2.2. Objetivos específicos. 4](#_Toc180141948)

[3. ALCANCE DEL MANUAL 4](#_Toc180141949)

[4. TÉRMINOS Y DEFINICIONES 4](#_Toc180141950)

[5. SIGLAS 5](#_Toc180141951)

[6. MARCO NORMATIVO. 5](#_Toc180141952)

[7. OBJETIVOS DEL SGSPI. 7](#_Toc180141954)

 [7.1. Objetivos Específicos del SGSPI 7](#_Toc180141955)

[8. ALCANCE DEL SGSPI 5](#_Toc180141953)

[9. IMAGEN DEL SGSPI 8](#_Toc180141956)

[10. CAPITULO I - CUMPLIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 8](#_Toc180141957)

 [10.1. Cumplimiento de revisión del sistema por la dirección 8](#_Toc180141958)

 [10.2. Indicadores del SGSPI y medición de objetivos 12](#_Toc180141959)

 [10.2.1. Plan para la medición de objetivos del SGSPI 18](#_Toc180141960)

 [10.3. Cumplimiento de relacionamiento con proveedores 18](#_Toc180141961)

 [10.4. Cumplimiento de revisión de eficacia de riesgos de seguridad de información ………………………………………………………………………………………………..20](#_Toc180141962)

[11. CAPITULO II - SEGURIDAD DIGITAL 22](#_Toc180141963)

 [11.1. Cumplimiento en el uso adecuado de medios removibles 22](#_Toc180141964)

[12. CAPITULO III - GESTIÓN DE LA COMUNICACIÓN Y DEL CONOCIMIENTO DEL SGSPI …………………………………………………………………………………………………..26](#_Toc180141965)

 [12.1. Gestión del Conocimiento 26](#_Toc180141966)

 [12.2. Plan de Comunicación del SGSPI 27](#_Toc180141967)

[13. CAPITULO IV - GESTIÓN DE PARTES INTERESADAS DEL SGSPI 33](#_Toc180141968)

 [13.1. Metodología para la identificación de Partes Interesadas 36](#_Toc180141969)

 [13.2. Instrumento Matriz de identificación de Partes Interesadas 36](#_Toc180141970)

 [13.3. Cumplimiento de la actualización del registro de Partes Interesadas 37](#_Toc180141971)

[14. PLANIFICACIÓN DE LOS CAMBIOS DEL SGSPI 37](#_Toc180141972)

[15. MARCO DE ACCIÓN PARA EL ETIQUETADO DE LA INFORMACIÓN 40](#_Toc180141973)

[16. MARCO DE ACCIÓN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 43](#_Toc180141974)

[17. CUMPLIMIENTO PARA REALIZACIÓN DE PRUEBAS Y ANÁLISIS DE VULNERABILIDADES 47](#_Toc180141975)

[18. CUMPLIMIENTO DE ESTRATEGIA PARA LA CONTINUIDAD DEL NEGOCIO 50](#_Toc180141976)

[19. CONTROL DE CAMBIOS 53](#_Toc180141977)

# 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 La Agencia Presidencial de Cooperación Internacional de Colombia, 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 se integra a la política del Sistema de Gestión de la Seguridad y Privacidad de la información (SGSPI) y habilita la capacidad de operación del Sistema, estableciendo las acciones de cumplimiento a la política interna alineado al estándar internacional Norma ISO IEC 27001:2022.

# OBJETIVO DEL MANUAL DE OPERACIONES

## **Objetivo general**

Establecer un marco de referencia que defina y documente los procedimientos, políticas y prácticas necesarias para garantizar la Seguridad y Privacidad de la información en la Agencia Presidencial de Cooperación Internacional de Colombia, APC Colombia.

## **Objetivos específicos**

* Documentar los procedimientos claros y detallados para proteger la Confidencialidad, Integridad y Disponibilidad de la información de la Agencia a través de los diferentes mecanismos de seguridad establecidos.
* **Facilitar la mejora continua** del SGSPI a través del monitoreo, revisión y ajuste de los procedimientos establecidos definidos en el presente manual.

# ALCANCE DEL MANUAL

El presente Manual de Operaciones del SGSPI es aplicable a todas las áreas, procesos, usuarios y sistemas de información de APC Colombia.

# TÉRMINOS Y DEFINICIONES

Los principales términos y definiciones se encuentran establecidos en el Documento: Política de seguridad y privacidad de la información (A-OT-011).

# SIGLAS

* **APC Colombia:** Agencia Presidencial de Cooperación Internacional de Colombia.
* **IEC:** Comisión Electrotécnica Internacional.
* **ISO:** Organización Internacional de Normalización
* **MSPI**: Modelo de Seguridad y Privacidad de la Información.
* **NIST:** National Institute of Standards and Technology.
* **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información.
* **PETI:** Plan Estratégico de Tecnologías de la Información.

# MARCO NORMATIVO

El marco normativo se encuentra establecidos en el Documento: Política de seguridad y privacidad de la información (A-OT-011).

# OBJETIVO DEL SGSPI

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 APC Colombia.

#  Objetivos Específicos del SGSPI

* Promulgar y sensibilizar a todos los servidores, funcionarios públicos, contratistas, y personas de interés en general; en la importancia de la protección y cuidado de la información, orientado a garantizar la integridad, disponibilidad y confidencialidad que se maneja en la APC Colombia.
* Controlar, mitigar y/o reducir los riesgos asociados con la seguridad y privacidad de la información, identificando las amenazas hacia los activos determinados por la agencia y establecer el plan de tratamiento con el fin de protegerlos.
* Mantener el SGSPI a través de la implementación de las estrategias de mejora continua.

# ALCANCE DEL SGSPI

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 4.3 |

**Fuente:** Creado por el proceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

*“La Agencia Presidencial de Cooperación Internacional de Colombia, APC Colombia, adopta el Sistema de Gestión de la Seguridad y Privacidad de la Información (SGSPI), en el Sistema de Gestión Integral (SGI), con aplicación a catorce (14) procesos institucionales”.*

| SISTEMA DE GESTIÓN INTEGRAL (SGI) |
| --- |
| PROCESO: Gestión de tecnologías de la información |
| SISTEMA DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (SGSPI) |
| Proceso | Tipo de proceso |
| 1. Direccionamiento Estratégico y Planeación
 | Estratégico (transversal) |
| 1. Gestión de Comunicaciones
 | Estratégico (transversal) |
| 1. Identificación y Priorización de Cooperación Internacional
 | Misional  |
| 1. Preparación y Formulación de Cooperación Internacional
 | Misional |
| 1. Implementación y Seguimiento de Cooperación Internacional
 | Misional |
| 1. Administración de Recursos de Cooperación Internacional No Reembolsables y Donaciones en Especie
 | Misional |
| 1. Gestión de Talento Humano
 | Apoyo |
| 1. Gestión Contractual
 | Apoyo |
| 1. Gestión Administrativa
 | Apoyo |
| 1. Gestión Financiera
 | Apoyo |
| 1. Gestión de Tecnologías de la Información
 | Apoyo |
| 1. Gestión Jurídica
 | Apoyo |
| 1. Gestión de Servicio al Ciudadano
 | Apoyo |
| 1. Evaluación, Control y Mejoramiento
 | Control (transversal) |

**Fuente:** Elaboración propia del proceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# IMAGEN DEL SGSPI



**Fuente:** Imagen creada por el proceso Gestión de Comunicaciones de la APC Colombia, septiembre de 2024.

# CAPITULO I - CUMPLIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

#  Cumplimiento de revisión del sistema por la Dirección

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 9.3 |
| Lineamiento interno de la APC Colombia | Política de la seguridad y privacidad de la información, numeral 9 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **REVISIÓN POR LA DIRECCIÓN** |
| Objetivo | El Objetivo de la revisión por Dirección es asegurar la conveniencia, adecuación y eficacia continua del SGSPI de la Agencia |
| Alcance | El procedimiento de gestión de revisión parte desde el Comité Institucional de Gestión y Desempeño dando cumplimiento a la NTC ISO IEC 27001:2022, requisito 9.3 |
| Responsable | Comité Institucional de Gestión y Desempeño |
| Proceso asociado | Gestión de Tecnologías de la Información |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **FRECUENCIA** |
| --- | --- | --- | --- | --- | --- |
| 1 | Programar la revisión del sistema  | 1. Solicitar la autorización de convocatoria.
2. Preparar información del estado del SGSPI con contenido conforme a la Política
 | Proceso Gestión de tecnologías de la información  | Correo electrónico E-FO-041 Plantilla de Presentación. | Una vez por año programado por la Secretaría Técnica del Comité, o por demanda ante la necesidad de cambios significativos en el SGSPI, planificado con el comité |
| 2 | Convocar el comité institucional de gestión y desempeño (dirección) | 1. Agendar a miembros del comité y responsable del SGSPI
 | Secretaría Técnica del Comité | Correo electrónico (calendario). | Por comité |
| 3 | Sesionar el Comité | 1. Dictar orden del día
2. Verificación de Quorum
3. Inicio del Comité
 | Secretaría Técnica del Comité | Acta de comité | Por comité |
| 4 | Sensibilización al comité y medir efectividad | 1. Sensibilizar las responsabilidades frente a la revisión por la Dirección
 | Proceso Gestión de tecnologías de la información | Acta de comité | Por comité |
| 4 | Presentar el estado del SGSPI dando cumplimiento a la ISO IEC 27001:2022 | 1. Presentar las consideraciones del sistema
 | Secretaria general | Acta de registro de asistencia de revisión de Dirección | Por comité |
| 5 | Recibir retroalimentación del Comité para fortalecer el SGSPI | 1. Solicitar y documentar la retroalimentación
 | Comité | Acta de comité | Por comité |
| 6 | Cierre del Comité  | 1. Dar cierre del comité
 | Secretaría técnica del comité | Acta de comité | Por comité |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

#  Indicadores del SGSPI y medición de objetivos

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito  |
| Lineamiento interno de la APC Colombia | Política de la seguridad y privacidad de la información |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** | **FECHA INICIO - FIN** | **ACTIVIDADES** | **RECURSOS REQUERIDOS** | **RESPONSABLE** | **INDICADOR ASOCIADO** | **META** | **FRECUENCIA DE REVISIÓN** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Promulgar y sensibilizar a todos los servidores públicos, contratistas, y personas de interés en general; en la importancia de la protección y cuidado de la información, orientado a garantizar la integridad, disponibilidad y confidencialidad que se maneja en la agencia presidencial para la cooperación internacional de la La APC Colombia | Anual | Actualización del Programa de Concientización en Seguridad y privacidad de la información.Ejecución del Programa de Concientización | Recursos Humanos.Materiales de apoyo.Recurso financiero.  | Proceso Gestión de tecnologías de la información | Número de campañas realizadas  | 100% | Trimestral  |
| Controlar, mitigar y/o reducir los riesgos asociados con la seguridad y privacidad de la información, identificando las amenazas hacia los activos determinados por la agencia y establecer el plan de tratamiento con el fin de protegerlos. | Anual | Identificar nuevos riesgos de Seguridad y privacidad de la Información. Realizar seguimiento sobre los riesgos relacionados con seguridad y privacidad de la Información | Recursos Humanos.Materiales de apoyo.Recursos Financieros | Procesos institucionales  | Número de incidentes de seguridad controladosdiariamente | 100% | mensual |
| Mantener el SGSPI a través de la implementación de las estrategias de mejora continua. | Anual | Programar el seguimiento del estado de las acciones de mejora sobre el sistema determinando un muestreo. Ejecutar el seguimiento del estado de las acciones de mejora sobre el sistema determinando un muestreo  | Recursos Humanos.Recursos Financieros | Proceso Gestión de tecnologías de la información | Número de estrategias de mejora continua implementadas | 100% | Bimestral |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# Plan para la medición de objetivos del SGSPI

* El proceso Gestión de tecnologías de la información incorporará el resultado de la medición de los objetivos en un informe controlado por el Sistema de Gestión Documental dispuesto para tal fin, conforme a los indicadores del sistema y su frecuencia de medición.
* El proceso Gestión de tecnologías de la información realizará un consolidado del resultado de esta medición para presentarlo a la revisión de la Dirección General y recibir retroalimentación.

# Cumplimiento de relacionamiento con proveedores

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito A.15 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, Código: A-OT-100, Numeral 7.12 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **RELACIONAMIENTO CON PROVEEDORES** |
| Objetivo | Asegurar la protección de los activos de la organización que sean accesibles a los proveedores (contratistas y aliados técnicos)  |
| Alcance | Monitoreo al cumplimiento de la Política de seguridad y privacidad de la información |
| Proceso asociado | Gestión de tecnologías de la informaciónGestión contractual |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **FRECUENCIA** |
| --- | --- | --- | --- | --- | --- |
| 1 | Programar una selección aleatoria de revisión de expedientes contractuales  | Requerir al proceso de Gestión contractual mediante comunicación oficial  | Proceso Gestión de tecnologías de la información | Correo electrónico  | Una vez por año |
| 2 | Identificar cumplimiento de los requisitos de la Política | Revisar el cumplimiento de la Política del SGSPI y los acuerdos de confidencialidad | Proceso Gestión de tecnologías de la información | Reporte para incorporar al informe de seguridad de la información para presentar a instancia superior  | Una vez por año  |
| 3 | En el evento de identificar un incidente por no cumplimiento de la política: Gestionar el incidente de seguridad de la información | Requerir el cumplimiento de la política del SGSPI | Proceso Gestión de tecnologías de la informaciónA Supervisores de contratos | Reporte para incorporar al informe de seguridad de la información para presentar a instancia superior | Una vez por año |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

#  Cumplimiento de revisión de eficacia de riesgos de seguridad de información

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 6.1.1 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.13 y 7.14 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **MONITOREO EFICACIA DE RIESGOS DE SEGURIDAD DE INFORMACIÓN** |
| Objetivo | Medir indicador de objetivo del SGSPI  |
| Alcance | Monitoreo sobre la eficacia de los Riesgos |
| Proceso asociado | Gestión de tecnologías de la información.Gestión contractual |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **FRECUENCIA** |
| --- | --- | --- | --- | --- | --- |
| 1 | Dar recepción y documentar los incidentes de seguridad de la información provenientes de materialización de riesgos en los procesos institucionales | Recibir incidentes por los canales de la mesa de servicios Consultar de forma planificada sobre la materialización de riesgos a los procesos institucionales  | Proceso Gestión de tecnologías de la información  | Correo electrónico,Sistema de mesa de servicios  | Diario  |
| 2 | Gestionar los incidentes de seguridad de la información relacionado con la materialización de riesgos del SGSPI | Gestionar y superar la incidencia de seguridad de la información  | Proceso Gestión de tecnologías de la información Procesos institucionales donde se materialice el riesgo | SGSPI, informes (varios) | Por demanda |
| 3 | Evaluar la eficacia de los controles de los riesgos del SGSPI y actualizar herramientas de gestión de riesgos | Documentar los cambios y actualizar el mapa de riesgos de seguridad de la información y los activos de información (si aplica)  | Proceso Gestión de tecnologías de la información A Supervisores de contratos | Reporte para incorporar al informe de seguridad de la información para presentar a instancia superior | Por demanda |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

#  CAPITULO II - SEGURIDAD DIGITAL

#  Cumplimiento en el uso adecuado de medios removibles

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 8.1.1 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.13 y 7.14 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **CONTROL EN EL USO DE MEDIOS REMOVIBLES** |
| Objetivo | Realizar las actividades necesarias para el control de los medios de almacenamiento removibles con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información de la APC Colombia  |
| Alcance | Este procedimiento se encuentra alineado con las Políticas específicas del sistema de gestión de seguridad y privacidad de la información y aplica para todos los usuarios que requieran gestionar medios de almacenamiento removibles en los que se pueda extraer o que contenga información de la Entidad, tales cintas, CD’s, DVD’s, dispositivos personales “USB”, token de firma digital, discos externos a la estación de trabajo, celulares, entre otros |
| Proceso asociado | Gestión de tecnologías de la información |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

* La APC Colombia, gestiona el uso adecuado de medios removibles mediante los documentos de control: A-FO-260 Control del uso de medios removibles y A-FO-261 Control de asignación del uso de medios removibles.
* El proceso Gestión de tecnologías de la información deniega la habilitación de los puertos USB, para evitar el uso de medios removibles no autorizados en las estaciones de trabajo del parque computacional.
* El proceso de Gestión de tecnologías de la información habilita el puerto USB para el uso de medios removibles a las excepciones autorizadas con criterio funcional y documenta un registro de las exenciones.
* Estas operaciones se controlan con el siguiente cumplimiento:

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1 | Solicitud de habilitar puertos USB  | Tarea 1: Todo funcionario y/o contratista que requiera utilizar medios removibles, deberá solicitar la respectiva aprobación para que se habiliten los puertos respectivos. está solicitud deberá ser realizada por medio de la herramienta de la mesa de servicios disponible | Servidor y/o Contratista | Correo electrónico y/o sistema de la mesa de servicios.Formato usuarios con medios removibles  | Por demanda |
| Tarea 2. Definir el periodo de tiempo de acceso a los puertos |
| Tarea 3: Se revisará si es aprobada la solicitud |
| 2 | Habilitar puertos | Tarea 1: El proceso Gestión de tecnologías de la información, procederá con la habilitación de los puertos una vez sea aprobada dicha solicitud | Proceso Gestión de tecnologías de la información | Por demanda |
| Tarea 2: Se informará el estado de la solicitud por intermedio de las herramientas correspondientes |
| 3 | Inhabilitar puertos | El proceso Gestión de tecnologías de la información, tendrá generada política para inhabilitar los puertos que no están autorizados, y se realizará monitoreo periódico sobre las estaciones | Proceso Gestión de tecnologías de la información | Por demanda |
| 4 | Registro de accesos a medios removibles | El proceso Gestión de tecnologías de la información, llevará control de los usuarios con acceso autorizado a medios removibles como lista de excepción | Proceso Gestión de tecnologías de la información |
| 5 | Clasificación de la información | El funcionario y/o contratista dará uso adecuado de la información según la clasificación de la información definida por la APC Colombia  | Servidor y/o Contratista |
|  6 | Escaneo de Malware |  Proceso automatizado de la herramienta de antivirus  | Proceso Gestión de tecnologías de la información  |
| 7 | Seguimiento uso de medios removibles | Se revisará y solicitará acta de uso de adecuado de medios removibles, definido según el formato uso adecuado de medios removibles. Con las respectivas responsabilidades sobre el uso de memorias USB, Discos, Cintas entre otros | Proceso Gestión de tecnologías de la información |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# CAPITULO III - GESTIÓN DE LA COMUNICACIÓN Y DEL CONOCIMIENTO DEL SGSPI

#  Gestión del conocimiento

| MARCO NORMATIVO |
| --- |
| Lineamiento interno de la APC Colombia | 7.17. Política de la gestión del conocimiento del SGSPI, numeral 7.17 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **GESTIÓN DEL CONOCIMIENTO DEL SGSPI** |
| Objetivo | Habilitar y promover las acciones que conlleven al conocimiento de los lineamientos del sistema  |
| Alcance | Cumplimiento de actividades de entrenamiento y conocimiento del SGSPI |
| Proceso asociado | Gestión de tecnologías de la informaciónGestión de talento humano |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

* El proceso Gestión de tecnologías de la información habilitará la herramienta tecnológica disponible para la publicación de contenidos del SGSPI.
* El proceso Gestión de tecnologías de la información habilitará el curso o entrenamiento del SGSPI de forma transitoria para la toma de los usuarios.
* El proceso Gestión de tecnologías de la información y el proceso Gestión de talento humano articularán el curso o entrenamiento del SGSPI mediante los lineamientos de la inducción y reinducción institucional asegurando la toma del curso por todos los servidores públicos y el proceso Gestión de tecnologías de la información habilitará el curso o entrenamiento del SGSPI de forma transitoria para la toma de los usuarios y contratistas de la Agencia.
* El proceso Gestión de tecnologías de la información y el proceso Gestión de talento humano realizarán el monitoreo del cumplimiento de la toma del curso o entrenamiento conforme a los lineamientos de estos procesos. Así como, la efectividad de la sensibilización de estos conocimientos.

#  Plan de comunicación del SGSPI

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 7.4 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.16E-OT-037 Plan estratégico de comunicacionesE-OT-040 Matriz seguridad de la información en la política de comunicacionesE-OT-026 Matriz de comunicaciones |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

La APC Colombia mediante los procesos Gestión de tecnologías de la información y Gestión de Comunicaciones ejecutaran las actividades del siguiente plan de comunicaciones del sistema conforme al lineamiento interno de la APC Colombia:

* **Primer Semestre**

| **No.** | **ACTIVIDAD PROGRAMADA** | **ENERO** | **FEBRERO** | **MARZO** | **ABRIL** | **MAYO** | **JUNIO** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| 1 | Contexto Organizacional y Partes Interesadas |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Política de Seguridad de la Información |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Políticas generales de Seguridad de la Información |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 4 | Requisitos legales y contractuales  |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 5 | Objetivos de Seguridad de la Información |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 6 | Responsabilidades y Autoridades frente al SGSPI |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 7 | Plan de Tratamiento de riesgos |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 8 | Resultados de la Revisión por la dirección |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 9 | Acciones correctivas y de mejora |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 10 | Necesidades de capacitación frente al SGSPI |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 11 | Bloqueo de Sesión  |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 12 | Ingeniería Social, Spoofing, Spam |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |   |   |   |   |   |
| 14 | Manejo de Contraseñas |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 15 | Ransomware |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 16 | Seguridad Informática |   |   |   |  |   |   |   |   |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |
| 17 | Protección de datos |   |   |   |  |   |   |   |   |   |   |   |   |   |   |  |   |   |   |  |   |   |   |   |   |
| 18 | Elementos de Seguridad Antivirus |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |   |
| 19 | Controles de Accesos |   |   |   |  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

* **Segundo Semestre**

| **No.** | **ACTIVIDADES PROGRAMADAS** | **JULIO** | **AGOSTO** | **SERPTIEMBRE** | **OCTUBRE** | **NOVIEMBRE** | **DICIEMBRE** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| 1 | Contexto Organizacional y Partes Interesadas |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Política de Seguridad de la Información  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Políticas generales de Seguridad de la Información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 4 | Requisitos legales y contractuales  |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 5 | Objetivos de Seguridad de la Información |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 6 | Responsabilidades y Autoridades frente al SGSPI |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 7 | Plan de Tratamiento de riesgos |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 8 | Resultados de la Revisión por la dirección |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 9 | Acciones correctivas y de mejora |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 10 | Necesidades de capacitación frente al SGSPI |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 11 | Bloqueo de Sesión |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 12 | Ingeniería Social, Spoofing, Spam |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 14 | Manejo de Contraseñas |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 15 | Ransonware |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 16 | Seguridad Informática |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 17 | Protección de datos |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 18 | Elementos de Seguridad Antivirus |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 19 | Controles de Accesos |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

* La APC Colombia mediante el proceso Gestión de tecnologías de la información, evaluará la efectividad de la difusión y comunicación del Sistema.
* La APC Colombia mediante el proceso Gestión de tecnologías de la información, realizará un informe consolidado con la frecuencia del indicador de los objetivos del sistema, frente al resultado de la ejecución del plan de comunicaciones.
* La APC Colombia mediante el proceso Gestión de tecnologías de la información, realizará un informe consolidado anual para presentación de la revisión por la Dirección General, frente al resultado de la ejecución del plan de comunicaciones.

#

#  CAPITULO IV - GESTIÓN DE PARTES INTERESADAS DEL SGSPI

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 4.2 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.18 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **GESTIÓN DEL REQUISITOS DE SEGURIDAD DE PARTES INTERESADAS**  |
| Objetivo | Identificar las partes interesadas, grupos de interés o autoridades con los cuales la Agencia Presidencial de Cooperación Internacional de Colombia interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectados por la seguridad y privacidad de la Información |
| Alcance | Inicia desde la identificación de los requisitos y partes interesadas, continúa con las necesidades y expectativas y termina con la consolidación de las partes |
| Proceso asociado | Responsable de liderar la acción de cumplimiento: Gestión de tecnologías de la informaciónResponsable de ejecutar la acción de cumplimiento: Todos los procesos institucionales |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1 | Planificar y hacer ejecutar la gestión sobre la identificación de las partes interesadas | Dentro de la planeación se realiza análisis con el fin de determinar cuáles son las partes interesadas que aplican a la APC Colombia y que afectan la seguridad y privacidad de la Información | Proceso  | Matriz de Partes interesadas | Anual |
| 2 | Identificación de las partes interesadas | Identificar las partes interesadas y su aplicación en la misión de la APC Colombia | Procesos institucionales | Matriz de Partes interesadas  | Anual |
| 3 | Definición de las partes interesadas | Definir las partes interesadas y su propósito con la APC Colombia  | Procesos institucionales | Matriz de Partes interesadas  | Anual |
| 4 | Definición de los requisitos de Seguridad de la Información de las partes interesadas | Definir los requisitos de Seguridad de la Información de cada una de las partes interesadas  | Procesos institucionales | Matriz de Partes interesadas | Anual |
| 4 | Identificar las necesidades de las partes interesadas | Determinar cuáles son las necesidades que tiene la APC Colombia frente a estas partes interesadas | Procesos institucionales | Matriz de Partes interesadas  | Anual |
| 5 | Identificar las expectativas de las partes interesadas | Recopilar información que permita identificar las expectativas de las partes interesadas | Procesos institucionales | Matriz de Partes interesadas | Anual |
| 6 | Divulgar la matriz de las partes interesadas y sus requisitos | Publicar en el canal autorizado  | Proceso Gestión de tecnologías de la informaciónProceso Gestión de comunicaciones  | Canal de comunicación (intranet) | Por actualización |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

#  Metodología para la identificación de partes interesadas

La APC Colombia establece la metodología de identificación de partes interesadas mediante los documentos:

* E-OT-027 Portafolio de servicios características y partes interesadas de la APC Colombia
* A-OT-084 Caracterización de partes interesadas y grupos de valor

#  Instrumento matriz de identificación de partes interesadas

El proceso Gestión de tecnologías de la información define la siguiente estructura como instrumento para la identificación de partes interesadas:

**Fuente: Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

#  Cumplimiento de la actualización del registro de partes interesadas

El proceso Gestión de tecnologías de la información documentará los registros del instrumento de la matriz de partes interesadas y realizará su custodia en el archivo de gestión conforme a los lineamientos del sistema de gestión documental.

#  PLANIFICACIÓN DE LOS CAMBIOS DEL SGSPI

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, requisito 6.3 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.18 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

|  |  |
| --- | --- |
| **CUMPLIMIENTO** | **PLANIFICACIÓN DE LOS CAMBIOS DEL SGSPI** |
| Objetivo | Establecer la metodología apropiada para planificar, identificar, evaluar y controlar el impacto de los cambios internos o externos que se puedan generar sobre el SGSPI de la APC Colombia. |
| Alcance | El presente alcance de la planificación de cambios aplica para todos los procesos institucionales, sistemas y recursos de la entidad, que tienen relación con el SGSPI y que puedan verse afectados por cualquier acción de modificación. |
| Proceso asociado | Responsable de liderar la acción de cumplimiento: proceso Gestión de tecnologías de la informaciónResponsable de ejecutar la acción de cumplimiento: Todos los procesos institucionales. |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1. | Identificación del cambio | Identificar la necesidad o el motivo del cambio en el SGSPI | Proceso Gestión de tecnologías de la información | A-FO-277 Formato de Planificación de cambios | Por demanda |
| 2. | Evaluación del cambio | Evaluar el impacto potencial del cambio, correspondientes a los procedimientos internos de la entidad. | Proceso Gestión de tecnologías de la información | A-FO-277 Formato de Planificación de cambios | Por demanda |
| 3. | Diseño y planificación del cambio  | Diseñar un plan detallado para implementar los cambios específicos del SGSPI, incluidas las actividades, los plazos, los recursos necesarios y los responsables de la ejecución | Proceso Gestión de tecnologías de la información | A-FO-277 Formato de Planificación de cambios | Por demanda |
| 4. | Aprobación de los cambios | Obtener la aprobación de las partes interesadas pertinentes  | Comité Institucional de Gestión y DesempeñoDireccionamiento estratégico y planeación | Acta de revisión por dirección.A-FO-277 Formato de Planificación de cambios | Por demanda |
| 5. | Implementación del cambio | Implementar las actividades necesarias para efectuar el cambio, según el plan diseñado | Proceso Gestión de tecnologías de la información | A-FO-277 Formato de Planificación de cambios | Por demanda |
| 6. | Comunicación y participación del cambio | Informar a todas las partes interesadas pertinentes sobre los cambios planificados en el SGSPI para su respectiva divulgación y conocimiento | Proceso Gestión de comunicacionesProcesos institucionales | Correo electrónico institucional Intranet Mi Agencia | Por demanda |
| 7. | Evaluación posterior de la Implementación de los cambios | Evaluar la efectividad de los cambios y sus efectos | Proceso Gestión de tecnologías de la información | A-FO-277 Formato de planificación de los cambios | Por demanda |
| 8. | Revisión y documentos | Documentar registros del proceso de planificación y cambio | Proceso Gestión de tecnologías de la información | A-FO-277 Formato de planificación de los cambios | Por demanda |

**Fuente: Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

#  MARCO DE ACCIÓN PARA EL ETIQUETADO DE LA INFORMACIÓN

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, Control 5.13 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.12 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1. | Consulta de Marco Normativo para Clasificación de la información | Identificar y clasificar la información según su nivel de criticidad y riesgo para dar lineamientos | Proceso de Gestión de tecnologías de la Información | A-OT-125 Lineamiento metodológico de Gestión de activos de información y de riesgos de seguridad de la Información y Ley 1712 de 2014 | Anual |
| 2. | Definición de Etiquetas de Seguridad | Crear el concepto de las etiquetas y niveles de seguridad para categorizar la información como lineamiento | Proceso de Gestión de tecnologías de la Información | A-OT-100 – Políticas específicas de Seguridad de la Información | Anual |
| 3 | Implementación de políticas de etiquetado de la información | Establecer directrices claras sobre cómo debe aplicarse el etiquetado de la información | Proceso de Gestión de Tecnologías de la Información | A-OT-100 – Políticas específicas de Seguridad de la Información | Anual |
| 4 | Identificar la información a etiquetar | Seleccionar la información a etiquetar, de acuerdo con su nivel de criticidad | Procesos institucionales | A-FO-272 Inventario de activos de Información y Sistema de Gestión de Archivo Electrónico Digital (SGAED) | Anual |
| 5. | Asignación de etiquetas de la información | Aplicar las etiquetas correspondientes a cada tipo de información según su clasificación y nivel de criticidad | Procesos institucionales | Información generada por los procesos institucionales.Documentos A-FO-272 Inventario de activos de Información y SGAED | Anual |
| 6. | Capacitar al personal sobre el uso y aplicación del etiquetado de la Información | Dar a conocer la importancia del etiquetado adecuado de la información y sus respectivos lineamientos de seguridad | Proceso de Gestión de Tecnologías de la Información | E-FO-010 - Acta de reunión y seguimiento a compromisos | Por demanda |
| 7. | Monitoreo y seguimiento | Realizar seguimiento periódico para verificar el cumplimiento de las políticas de etiquetado de la información | Proceso de Gestión de Tecnologías de la Información | E-FO-010 - Acta de reunión y seguimiento a compromisos | Por demanda |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# MARCO DE ACCIÓN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, Control 5.24 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.20 |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1 | Preparación | Definir el conjunto de políticas y procedimientos para el manejo de incidentes de seguridad  | Proceso Gestión de tecnologías de la información | A-OT-100 Políticas específicas de Seguridad de la Información. A-OT-123 Manual de operaciones del SGSPI  | Anual |
| 2. | Detección | Identificar y detectar los eventos e incidente de seguridad de la información y contacto con autoridades pertinentes | Proceso Gestión de tecnologías de la información | Formato reporte de incidentes de seguridad de la información | Por demanda |
| 3. | Evaluación y clasificación | Evaluar inicialmente el evento y/o incidente para determinar su naturaleza y gravedad.Clasificar la acción como evento o incidente de Seguridad de la Información | Proceso Gestión de tecnologías de la información | Formato reporte de incidentes de Seguridad de la Información.A-OT-100 Políticas específicas de seguridad de la información | Por demanda |
| 4. | Activación del equipo de respuesta. (notificación y reporte) | Activar el equipo de respuestas a incidentes de seguridad de la Información o equipo designado para el manejo de estas situaciones | Equipo de respuesta a incidentes de seguridad de la información (CSIRT)Proceso Gestión de seguridad la información | Formato de reporte de incidentes de seguridad de la información  | Por demanda |
| 5. | Contención y Mitigación | Implementación de medidas y controles para contener el incidente de seguridad y mitigar el daño | Proceso de Gestión de Tecnologías de la Información | Formato de reporte de incidentes de Seguridad de la Información | Por demanda. |
| 6. | Investigación, recolección de evidencia y análisis forense | Investigación que permita determinar la causa que ocasionó el incidente de Seguridad de la Información. Recopilación de evidencia digital | Equipo de respuesta a incidentes de seguridad de la información (CSIRT)Proceso Gestión de tecnologías de la información | Formato de Reporte de incidentes de Seguridad de la Información.Discos extraíbles | Por demanda |
| 7. | Erradicación del incidente | Eliminar por completo la amenaza (eliminación de malware, pruebas de vulnerabilidad)Implementar medidas de seguridad | Proceso Gestión de tecnologías de la información | Herramientas Tecnológicas | Por demanda |
| 8. | Resolución y recuperación | Restaurar los servicios y sistemas de información afectados y confirmación de la solución del incidente | Proceso Gestión de tecnologías de la información | Copias de seguridad de la información | Por demanda |
| 9. | Post incidente (análisis posterior y lecciones aprendidas) | Realizar el análisis posterior para identificar las lecciones aprendidas y recomendaciones de mejora | Proceso Gestión de tecnologías de la información | Formato de Reporte de incidentes de Seguridad de la Información.Informe del incidente | Por demanda |
| 10. | Documentación y Cierre del incidente | Documentar el detalle del incidente y su respectivo cierre | Proceso Gestión de tecnologías de la información  | Formato de Reporte de incidentes de Seguridad de la Información.Informe del incidenteInforme de gestión de incidente de Seguridad | Por demanda |
| 11. | Revisión y mejora continua | Revisión de los procesos y políticas internas de seguridad de la Información  | Proceso de gestión de tecnologías de la Información | A-OT-123 Manual de operacionesA-OT-100 Políticas de Seguridad de la Información | Por demanda |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# CUMPLIMIENTO PARA REALIZACIÓN DE PRUEBAS Y ANÁLISIS DE VULNERABILIDADES

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, Control 8.8 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.20A-OT-128 Plan de pruebas y análisis de vulnerabilidades |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1 | Planificación de las pruebas y análisis de vulnerabilidades | Definición del alcance y objetivos que incluye (sistemas información y/o aplicativos, redes y servidore | Proceso de gestión de tecnologías de la Información | A-OT-128 Plan de pruebas y análisis de vulnerabilidades | Anual.  |
| 2. | Recopilar la información para las pruebas y análisis de vulnerabilidades | Identificar los sistemas y aplicaciones a revisar y evaluar | Proceso de gestión de tecnologías de la Información | Matriz de inventario de activos críticos | Anual |
| 3. | Desarrollo de las pruebas y análisis de vulnerabilidades  | Escanear los sistemas en busca de nuevas vulnerabilidades.Realizar pruebas de penetración en determinados sistemas tecnológicos de la Agencia | Proveedor de servicios tercerizados | Informe de pruebas y análisis de vulnerabilidades | Anual |
| 4. | Informe y priorización | Presentar informe con información de los resultados de las pruebas realizadas | Proveedor de servicios tercerizados | Informe de pruebas y análisis de vulnerabilidades | Anual |
| 5. | Remediación de las vulnerabilidades encontradas | Ejecución de acciones para mitigar los riesgos y puesta en marcha de nuevas soluciones | Proveedor de servicios tercerizados | Informe de las pruebas de análisis de vulnerabilidades | Anual |
| 6. | Implementación de soluciones. | Montaje de nuevas soluciones de tecnología para contener cualquier amenaza del entorno tecnológico | Proceso de gestión de tecnologías de la Información | Herramientas tecnológicas | Por demanda |
| 7. | Documentación y respectivo cierre | Desarrollo de toda documentación obtenida como parte del ejercicio de pruebas y análisis de vulnerabilidades | Proceso de gestión de tecnologías de la Información | Informe de las pruebas de análisis de vulnerabilidades | Anual |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# CUMPLIMIENTO DE ESTRATEGIA PARA LA CONTINUIDAD DEL NEGOCIO

| MARCO NORMATIVO |
| --- |
| Estándar | ISO IEC 27001:2022, Control 5.30 |
| Lineamiento interno de la APC Colombia | Políticas específicas del sistema de gestión de seguridad y privacidad de la información, numeral 7.22A-OT-065 Estrategia de continuidad de tecnologías de la información |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

| **No.** | **ACTIVIDAD** | **TAREA** | **RESPONSABLE** | **REGISTRO** | **TIEMPO** |
| --- | --- | --- | --- | --- | --- |
| 1 | Definición de la estrategia de continuidad de negocio (BCP) | Establecer el plan y estrategia de continuidad de negocio que permita garantizar la operación de la entidad frente a cualquier amenaza del entorno tecnológico | Proceso de Gestión de Tecnologías de la Información  | A-OT-065 Estrategia de continuidad de tecnologías de la información. | Anual |
| 2. | Análisis de impacto y riesgos | Identificar los activos críticos de la entidad ya sean sistemas de información y/o aplicativos, redes y servidores  | Proceso de Gestión de tecnologías de la Información  | Matriz de inventario de activos críticos | Anual  |
| 3. | Desarrollo de estrategias de continuidad de negocio | Desarrollar las estrategias de continuidad de negocio para todos los procesos críticos de la Agencia  | Proceso de Gestión de tecnologías de la Información | A-OT-065 Estrategia de continuidad de tecnologías de la informaciónPlan de pruebas de continuidad de negocio | Por demanda  |
| 4.  | Implementación del plan de pruebas de continuidad de negocio | Implementar las medidas y controles para mitigar los riesgos de seguridad de la Información | Proceso de Gestión de tecnologías de la Información | Informe de resultados de pruebas | Por demanda |
| 5. | Desarrollo de pruebas y ejercicios  | Planificar la ejecución de pruebas y ejercicios de continuidad del negocio | Proceso de Gestión de Tecnologías de la Información | Plan de pruebas de continuidad de negocio.Informe de resultados de pruebas | Por demanda |
| 6. | Revisión y actualización de la estrategia de Continuidad del Negocio | Revisar y actualizar la estrategia de continuidad del negocio conforme a las nuevas amenazas del entorno | Proceso de Gestión de Tecnologías de la Información | A-OT-065 Estrategia de continuidad de tecnologías de la informaciónPlan de pruebas de continuidad de negocio.Informe de resultados de pruebas | Por demanda |

**Fuente:** Elaboración propia delproceso Gestión de tecnologías de la información de la APC Colombia, octubre de 2024.

# CONTROL DE CAMBIOS

| **VERSIÓN** | **CÓDIGO** | **NOMBRE DEL DOCUMENTO** | **ACTO/ MECANISMO** | **DESCRIPCIÓN DEL CAMBIO** |
| --- | --- | --- | --- | --- |
| 1 | A-OT-123 | Manual de operación del SGSPI  | Brújula, Abril 26 de 2023 | Creación del documento. Se determinan actividades, evidencias, soportes y frecuencias de las actividades enmarcadas en las políticas general y especificas del SGSPI. |
| 2  | A-OT-123 | Manual de operación del SGSPI  | Brújula, Octubre 22 de 2024 | Se revisó y actualizó la estructura y el contenido del documento, acorde con lo establecido en el Manual de imagen de la APC Colombia, en cumplimiento de la Ley 2345 del 30-12-2023 “Chao Marcas”, y siguiendo los lineamientos dados por Presidencia.Además, se incluye la planificación de los cambios del SGSPI y marco de acción para el etiquetado de la información y la gestión de incidentes de seguridad de la información, marco de acción para pruebas y análisis de vulnerabilidades, y marco de acción de estrategia de continuidad de negocio, adicional a ello se incluyeron objetivos generales y específicos, definición del alcance, términos y definiciones, siglas, marco normativo, ente otros. |