PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

APC-COLOMBIA

**CONTENIDO**

[1 ALCANCE DEL PLAN 3](#_Toc60187198)

[2 OBJETIVO 3](#_Toc60187199)

[3 OBJETIVOS ESPECÍFICOS 3](#_Toc60187200)

[4 ESTRATEGIAS 4](#_Toc60187201)

[5 PROYECTOS 5](#_Toc60187202)

[5.1 REVISIÓN TÉCNICA INDEPENDIENTE 5](#_Toc60187203)

[5.2 APROPIACIÓN Y SENSIBILIZACIÓN DEL SGS 5](#_Toc60187204)

[5.3 REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 6](#_Toc60187205)

[6 METAS 7](#_Toc60187206)

[7 ACCIONES 7](#_Toc60187207)

[8 PRODUCTOS 8](#_Toc60187208)

[9 RESPONSABLES 10](#_Toc60187209)

[10 CRONOGRAMA 14](#_Toc60187210)

[11 PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN 15](#_Toc60187211)

[12 DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS 16](#_Toc60187212)

[13 MAPAS DE RIESGOS 16](#_Toc60187213)

14 CONTROL DE CAMBIOS………………………………………………………………………….........17

#

# ALCANCE DEL PLAN

Basados en la operatividad nación del modelo integrado de planeación y gestión MIPG *el comité institucional de gestión y desempeño debe articular esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política del sistema de gestión seguridad de la información. Por lo cual es necesario designar un responsable de seguridad digital o de la información, quién debe pertenecer a un área transversal que haga parte de la alta dirección. (Tomado del Manual operativo de MIPG página 53).*

Así las cosas, la implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información - SGSI, se realiza en todos los procesos de la Agencia Presidencial de Cooperación internacional APC Colombia, de acuerdo con el ciclo de mejora continua PHVA; esto incluye, las actividades de formalización de los procesos, procedimientos y documentación correspondiente al SGSI.

# OBJETIVO

Este plan tiene como objetivo determinar las acciones que se realizaran con el fin de proteger la información que la Agencia Presidencial de Cooperación internacional APC Colombia utiliza para brindar la posibilidad de consolidar un liderazgo en Colombia frente al desarrollo de nuevos instrumentos, herramientas y aportes metodológicos que logren llevar al país hacer un referente técnico y metodológico en el impulso a la cooperación Sur-Sur de excelencia, agregando valor a las iniciativas que se implementen y teniendo en cuenta los retos del desarrollo sostenible y equitativo..

# OBJETIVOS ESPECÍFICOS

* Socializar las políticas y documentos existentes del sistema de gestión de seguridad de la información a todos los servidores públicos, contratistas y terceros que puedan tener alguna responsabilidad frente a los activos de información
* Implementar los lineamientos establecidos en las políticas del sistema de gestión de seguridad la información en cuanto a la conservación de la información, su protección, permisos de acceso, responsabilidades en la administración y divulgación de la información relativa APC Colombia, esto incluye información que por sumisión reciba administre y/o almacene.
* Definición de indicadores de medición, que permitan evaluar la gestión y la implementación del sistema de gestión de seguridad de la información.
* Preparar a la agencia para una posible certificación del sistema de gestión de seguridad de la información (SGSI) teniendo en cuenta los parámetros establecidos por la norma internacional ISO 27001:2013.

# ESTRATEGIAS

Teniendo en cuenta a que la agencia se propone un trabajo conjunto entre todos los actores de la cooperación (agencia es nacionales, autoridades locales, cooperantes, sector privado y sociedad civil) en 5 ejes de acción.

Siendo conscientes que este trabajo conjunto implica compartir información, administrar información propia o de otros y al mismo tiempo velar por qué se mantenga su confidencialidad integridad y disponibilidad, es por lo que se presentan las siguientes estrategias en temas de protección de la información a adoptar en la Agencia:

* **Ampliar la visión** frente al alcance y las tendencias de la cooperación internacional para el desarrollo en el país garantizando la confidencialidad y disponibilidad de la información.
* **Fortalecer la gestión** de la cooperación bajo un enfoque de resultados, innovación y sostenibilidad, utilizando los medios más seguros para hacer de esta gestión una gestión transparente.
* **Promover el posicionamiento de Colombia** como oferente de CSS y CT, a través de una participación efectiva en los diferentes espacios como mecanismos regionales de integración y concertación, programas regionales y bilaterales de cooperación, entre otros, a través de mecanismos.
* **Implementar mecanismos de coordinación** con una gobernanza pertinente y clara.
* **Definir criterios de priorización** de la demanda y la oferta de cooperación internacional.

Se plantean las siguientes estrategias en la implementación del Sistema de Gestión de Seguridad de la Información:

* Fortalecer la presencia la Agencia como actor clave en el **fortalecer la gestión** de la cooperación bajo un enfoque de resultados, innovación y sostenibilidad, utilizando los medios más seguros para hacer de esta gestión, una gestión transparente.
* Fortalecer la gestión de los procesos administrativos y de apoyo de la Agencia que aportan en **promover el posicionamiento de Colombia** como oferente de CSS y CT, a través de una participación efectiva en los diferentes espacios como mecanismos regionales de integración y concertación, programas regionales y bilaterales de cooperación, entre otros.
* Sensibilizar a las diferentes áreas y procesos de la agencia sobre las responsabilidades que tienen frente a la protección y acceso a la información.
* Generar alianzas entre procesos de apoyo que administren y gestionen controles de acceso de usuarios de forma física y digital, para garantizar el cumplimiento de las directrices de control de acceso establecidas en el SGSI.
* Capacitar a los servidores públicos en la identificación y tratamiento de los riesgos de seguridad de la información y la identificación de los activos de información, así como su valoración.

# PROYECTOS

Dentro de los proyectos establecidos para seguridad de la información se encuentra la contratación de un ethical hacking, apropiación y sensibilización del SGSI a toda la agencia y la realización de una auditoría interna, con miras a que la agencia se pueda certificar en la norma ISO 27001:2013; a continuación, se especifican los requerimientos y necesidades de estos dos proyectos:

## REVISIÓN TÉCNICA INDEPENDIENTE

Contratar un experto para poder realizar un ejercicio de hacking ético, análisis de vulnerabilidades, diseño de red segura e ingeniería social que permita identificar oportunidades de mejora en:

* Puertos, servicios y direcciones IP relacionadas con la infraestructura que soporta los servicios tecnológicos expuestos en el ciberespacio la Agencia.
* Vulnerabilidades a nivel de red y sistema operativo de los servidores publicados en internet de propiedad la Agencia.
* Vulnerabilidades web sobre las aplicaciones importantes de propiedad de APC Colombia.
* Vulnerabilidades de red y sistema operativo para el 30% de las direcciones IP internas que incluye servidores, dispositivos de red y una muestra de equipos de escritorio y portátiles.
* Una prueba de ingeniería social para al menos el 30% de los usuarios de APC Colombia, que se escogerá de un conjunto de opciones posibles de acuerdo la prueba más conveniente para la agencia.

## APROPIACIÓN Y SENSIBILIZACIÓN DEL SGS

Es necesario contar con la colaboración de todo el personal esto es los servidores públicos, contratistas y/o terceros, ya que sin su colaboración los esfuerzos para implementar el sistema de gestión de seguridad de la información pueden quedarse en buenas intenciones por lo que se requiere:

* Establecer un programa continuo de concientización sobre la protección de la información que garantice llevar a todo el equipo de trabajo de menos a más en cuanto al conocimiento de los medios, mecanismos e importancia del sistema de gestión de seguridad de la información.
* El uso adecuado de un marco conceptual qué incorpore principios, ideas de protección de la información ya sea esta digital, impresa o de gestión del conocimiento.
* Mecanismos de divulgación donde se den a conocer los riesgos ocasionados por el trabajo que se desempeña y cómo minimizarlos, además como estos pueden afectar la información y por ende la operación.
* Socializar las fallas de seguridad de la información reveladas en auditorías internas, externan, ejercicios de ingeniería social o ethical hacking.
* identificar falencias o debilidades en el conocimiento de protección de la información, con el fin de fortalecer las mediante sensibilizaciones, capacitaciones o ejercicios didácticos que permitan aprender y reconocer las necesidades de protección de la información frente amenazas presentes o futuras.
* Realizar presentaciones o actividades lúdicas, con ejemplos prácticos que generen recordación.
* Esencialmente, los empleados deben comprender cómo actuar y por qué.

## REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de evitar el incumplimiento de las obligaciones frente al MINTIC, DAFP, y de acuerdo con las evaluaciones del FURAG, MIPG, así como las obligaciones legales o de reglamentación relacionadas con seguridad de la información, se plantea como proyecto y en apoyo con control interno realizar una auditoría interna al sistema de gestión de seguridad de la información.

Se proyecta que dentro de la formación al grupo de auditores internos se incluya el sistema de gestión de seguridad de la información SGSI y su respectiva auditoría.

# METAS

Dentro de las metas planteadas en la implementación del Sistema de Gestión de Seguridad de la Información y acordes al MSPI se definen las siguientes metas:

* Servidores públicos y contratistas de la agencia conocen sus responsabilidades frente a la protección y acceso a la información que administran y generan en su cotidianidad.
* Integración entre los procesos de apoyo que administran y gestionan controles de acceso físico y digital, con el fin de garantizar el cumplimiento de las directrices de control de acceso establecidas en el sistema de gestión de seguridad de la información.
* Los servidores públicos y contratistas tienen la capacidad de identificar y documentar los riesgos de seguridad de la información a partir del inventario de activos de información valorado y clasificado.

# ACCIONES

Las acciones se encuentran especificadas por temas de acuerdo con el avance de la implementación del SGSI y se presentan a continuación:

**Tema 1: Socialización y planificación**

* Presentación de proyecto a Comité institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI.
* Asumir compromiso por parte la Agencia para la implementación y certificación de SGSI.
* Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI.
* Implementación de la documentación al interior de los procesos y planes operativos de la agencia para cumplir con la implementación y certificación de SGSI.
* Diagnosticar y Analizar la situación de la agencia frente a Seguridad de la información.

**Tema 2: Implementación de SGSI**

* Documentación formalizada de Procedimientos e instructivos requeridos para la implementación de SGSI.
* Generar un plan de acción para la definición de arquitecturas o componentes redundantes.
* Depuración de usuarios y permisos de acceso
* Alianzas entre procesos de apoyo que administran y gestionan controles de acceso de usuarios de forma física y digital, para garantizar el acceso seguro a áreas restringidas.
* Implementar un sistema de cifrado acorde a las necesidades de la información clasificada como, pública clasificada o pública reservada.
* Evaluación de documentación implementada
* Ajustes a implementación de SGSI

**Tema 3: Revisión independiente de la seguridad de la información**

* Revisión del cumplimiento técnico
* Implementación de Mejoras
* Socialización de resultados

**Tema 4: Evaluación y Certificación**

* Formación de auditores internos en ISO/IEC 27001:2013
* Auditoría Interna
* Revisión por la Dirección
* Solicitud de certificación
* Certificación de SGSI implementado

# PRODUCTOS

El principal producto del presente plan será el Sistema de Gestión de la Seguridad de la Información certificado bajo la norma ISO/IEC 27001:2013

A continuación, se presentan los entregables durante el desarrollo del proyecto

**Tema 1: Socialización y planificación**

| **ACCIÓN** | **ENTREGABLES** |
| --- | --- |
| Presentación de proyecto a Comité institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI. | Documentación existente del SGSI, presentación power point y Acta |
| Asumir compromiso por parte la Agencia para la implementación y certificación de SGSI. | Acta |
| Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI | Campaña de comunicaciones |
| Implementación de la documentación al interior de los procesos y planes operativos de la agencia para cumplir con la implementación y certificación de SGSI | Documentación revisada y actualizada |
| Diagnosticar y Analizar de la situación de la agencia frente a Seguridad de la información | Documento de diagnóstico del SGSI |
| Planificación de implementación de SGSI | Documento Plan del SGSI |

**Tema 2: Implementación de SGSI**

| **ACCIÓN** | **ENTREGABLES** |
| --- | --- |
| Documentación de Procedimientos e instructivos requeridos para la implementación de SGSI. | Estructura documental de SGSI |
| Generar un plan de acción para la definición de arquitecturas o componentes redundantes. | Plan de Recuperación de Desastres |
| Depuración de usuarios y permisos de acceso | Directorio activo acorde con listado de planta y contratistas activos. |
| Alianzas entre procesos de apoyo que administran y gestionan controles de acceso de usuarios de forma física y digital, para garantizar el acceso seguro a áreas restringidas. | Inventario áreas segurasPlan de implementación controles físicos de acceso |
| Implementar un sistema de cifrado acorde a las necesidades de la información clasificada como, pública clasificada o pública reservada. | Herramienta para el cifrado de la información, socializada y en funcionamiento |
| Evaluación de documentación implementada  | Documentación revisada |
| Ajustes a implementación de SGSI | Documentación aprobada y socializada |

**Tema 3: Revisión independiente de la seguridad de la información**

|  |  |
| --- | --- |
| **ACCIÓN** | **ENTREGABLES** |
| Revisión del cumplimiento técnico | Informes de resultados de la revisión técnica (Ethical hacking) |
| Implementación de Mejoras | Acciones de mejora implementadas y documentadas |
| Socialización de resultados | Acta |

**Tema 4: Evaluación y Certificación**

|  |  |
| --- | --- |
| **ACCIÓN** | **ENTREGABLES** |
| Formación de auditores internos en ISO 27001:2013 | Auditores formados |
| Auditoría Interna | Informe de Auditoría |
| Revisión por la Dirección | Acta |
| Solicitud de certificación  | Documentación pertinente |
| Certificación de SGSI implementado | Certificado del ente certificador |

# RESPONSABLES

En la definición de los responsables y responsabilidades se identificaron para el plan las siguientes

**Tema 1: Socialización y planificación**

| **ACCIÓN** | **ENTREGABLES** | **RESPONSABLE** |
| --- | --- | --- |
| Presentación de proyecto a Comité institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI. | Documentación existente del SGSI, presentación power point y Acta | Grupo de trabajo de Tecnologías de la Información |
| Asumir compromiso por parte la Agencia para la implementación y certificación de SGSI | Acta | Comité institucional de Gestión y Desempeño |
| Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI | Campaña de comunicaciones | Grupo de trabajo de Tecnologías de la Información |
| Implementación de la documentación al interior de los procesos y planes operativos de la agencia para cumplir con la implementación y certificación de SGSI | Documentación revisada y actualizada | Responsable de seguridad de la información asignado por el Comité institucional de Gestión y Desempeño |
| Diagnosticar y Analizar de la situación de la agencia frente a Seguridad de la información | Documento de diagnóstico del SGSI | Responsable de seguridad de la información asignado por el Comité institucional de Gestión y Desempeño |
| Planificación de implementación de SGSI | Documento Plan del SGSI | Responsable de seguridad de la información asignado por el Comité institucional de Gestión y Desempeño |

**Tema 2: Implementación de SGSI**

| **ACCIÓN** | **ENTREGABLES** | **RESPONSABLE** |
| --- | --- | --- |
| Documentación de Procedimientos e instructivos requeridos para la implementación de SGSI. | Estructura documental de SGSI | Responsable de seguridad de la información asignado por el Comité institucional de Gestión y Desempeño |
| Generar un plan de acción para la definición de arquitecturas o componentes redundantes. | Plan de Recuperación de Desastres | Grupo de trabajo de Tecnologías de la Información |
| Depuración de usuarios y permisos de acceso | Directorio activo acorde con listado de planta y contratistas activos. | Grupo de trabajo de Tecnologías de la Información |
| Alianzas entre procesos de apoyo que administran y gestionan controles de acceso de usuarios de forma física y digital, para garantizar el acceso seguro a áreas restringidas. | Inventario áreas segurasPlan de implementación controles físicos de acceso | Gestión AdministrativaGrupo de trabajo de Tecnologías de la InformaciónResponsable de seguridad de la información |
| Implementar un sistema de cifrado acorde a las necesidades de la información clasificada como, pública clasificada o pública reservada. | Herramienta para el cifrado de la información, socializada y en funcionamiento | Grupo de trabajo de Tecnologías de la Información |
| Evaluación de documentación implementada  | Documentación revisada | Responsable de seguridad de la información asignado por el Comité institucional de Gestión y Desempeño |
| Ajustes a implementación de SGSI | Documentación aprobada y socializada | Responsable de seguridad de la información asignado por el Comité institucional de Gestión y Desempeño |

**Tema 3: Revisión independiente de la seguridad de la información**

| **ACCIÓN** | **ENTREGABLES** | **RESPONSABLE** |
| --- | --- | --- |
| Revisión del cumplimiento técnico | Informes de resultados de la revisión técnica (Ethical hacking) | Contrato con tercero Seguimiento por parte del Responsable de seguridad de la información |
| Implementación de Mejoras | Acciones de mejora implementadas y documentadas | Contrato con tercero Seguimiento por parte del Responsable de seguridad de la información |
| Socialización de resultados | Acta | Contrato con tercero Seguimiento por parte del Responsable de seguridad de la información |

**Tema 4: Evaluación y Certificación**

|  |  |  |
| --- | --- | --- |
| **ACCIÓN** | **ENTREGABLES** | **RESPONSABLE** |
| Formación de auditores internos en ISO 27001:2013 | Auditores formados | Control Interno |
| Auditoría Interna | Informe de Auditoría | Control Interno |
| Revisión por la Dirección | Acta | Comité institucional de Gestión y Desempeño |
| Solicitud de certificación  | Documentación pertinente | Comité institucional de Gestión y Desempeño |
| Certificación de SGSI implementado | Certificado del ente certificador | Comité institucional de Gestión y Desempeño |

Es importante mencionar que todas las áreas y procesos son responsables del cumplimiento de las políticas de seguridad de la información, además de ser responsables de la identificación de los activos de información, su valoración e identificación de riesgos.

Además, todas las áreas y procesos son responsables de la protección de la información, por lo cual velan por su confidencialidad integridad y disponibilidad.

Con el fin de dar dirección y apoyo gerencial que permita realizar la gestión y desarrollo de las iniciativas sobre seguridad de la información, en el marco de la Estrategia de Gobierno Digital, el cumplimiento de la legislación vigente, en materia de seguridad de la información y la gestión adecuada de riesgos de seguridad de la información, APC COLOMBIA establece roles y responsabilidades para:

* Asegurar, que el sistema de gestión de la calidad preserva la seguridad de la información y es conforme con los requisitos de la norma técnica colombiana NTC ISO/IEC 27001:2013.
* Informar a la dirección sobre el desempeño de la gestión de la seguridad de la información y los controles que la apoyan.
* Gestionar los riesgos de seguridad de la información.
* Proteger los activos de seguridad de la información.
* Ejecución de procesos de seguridad específicos.

A continuación, se describen a groso modo las responsabilidades definidas:

**Dirección General / Comité institucional de Gestión y Desempeño:** Aprobar los lineamientos de seguridad de la información, apoyar en su divulgación e implementación.

**Gestión de Talento Humano:** Garantizar compromisos de protección de la información por parte de los servidores públicos antes, durante y al terminar su relación laboral con la agencia**.**

**Gestión Contractual:** Garantizar compromisos de protección de la información por parte de los contratistas antes, durante y al terminar su contrato con la agencia**.**

**Planeación:** Garantizar la inclusión del Sistema de Gestión de Seguridad de la Infomración en la integración al sistema, la gestión de riesgos y su tratamiento, socialización y planeación estratégica

**Gestión Administrativa:** Apoyar en la administración de recursos físicos que almacenen información, el acceso seguro a las instalaciones y acceso físico restringido a áreas seguras.

**Gestión Documental:**  Apoyar en la identificación de activos de información, implementar el etiquetado de Infomración y definir tiempos de conservación física y digital.

**Jurídica:** Apoyar a las áreas y procesos en la identificación y sustentación jurídica de los activos clasificados o de reserva y en velar por el cumpliendo en las obligaciones legales o contractuales relacionadas con la seguridad de la información

**Control Interno:** Realizar las auditorías internas al Sistema de Gestión de seguridad de la Información

**Director Administrativo y Financiero con funciones de Control Interno Disciplinario:** velar por el cumplimiento de los lineamientos y políticas para la protección de la información y de ser necesario tomar acciones de cumplimiento disciplinario

# CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma con vigencia del 2020-2022.

**Tema 1: Socialización y planificación**

| **ACCIÓN** | **FECHA****DD / MM / AAAA** |
| --- | --- |
| **INICIO** | **FIN** |
| Presentación de proyecto a Comité institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI. | 01/12/2020 | 15/12/2020 |
| Asumir compromiso por parte la Agencia para la implementación y certificación de SGSI. | 15/12/2020 | 15/12/2020 |
| Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI | 01/12/2020 | 31/12/2021 |
| Implementación de la documentación al interior de los procesos y planes operativos de la agencia para cumplir con la implementación y certificación de SGSI | 01/10/2020 | 31/12/2021 |
| Diagnosticar y Analizar la situación de la agencia frente a Seguridad de la información | Dos veces al año |
| Planificación de implementación de SGSI | 15/01/2021 | 05/02/2021 |

**Tema 2: Implementación de SGSI**

| **ACCIÓN** | **FECHA****DD / MM / AAAA** |
| --- | --- |
| **INICIO** | **FIN** |
| Documentación de Procedimientos e instructivos requeridos para la implementación de SGSI. | 01/07/2020 | 30/03/2021 |
| Depuración de usuarios y permisos de acceso | 01/02/2021 | 30/06/2021 |
| Revisión entre procesos de apoyo que administran y gestionan controles de acceso de usuarios de forma física y digital, para garantizar el acceso seguro a áreas restringidas. | 15/01/2020 | 30/06/2021 |
| Evaluación de documentación implementada  | 01/06/2020 | 01/03/2022 |
| Ajustes a implementación de SGSI | 15/01/2020 | 02/05/2022 |

**Tema 3: Revisión independiente de la seguridad de la información**

|  |  |
| --- | --- |
| **ACCIÓN** | **FECHA****DD / MM / AAAA** |
| **INICIO** | **FIN** |
| Revisión del cumplimiento técnico | 15/08/2020 | 30/12/2021 |
| Implementación de Mejoras | 16/05/2021 | 15/09/2021 |
| Socialización de resultados | 16/08/2021 | 15/12/2021 |

**Nota:** Esta revisión deberá hacerse cada 2 años

**Tema 4: Evaluación y Certificación**

| **ACCIÓN** | **FECHA****DD / MM / AAAA** |
| --- | --- |
| **INICIO** | **FIN** |
| Formación de auditores internos en ISO/IEC 27001:2013 | 01/10/2020 | 31/12/2020 |
| Auditoría Interna | 01/07/2021 | 15/07/2021 |
| Revisión por la Dirección | 16/07/2021 | 20/08/2021 |
| Solicitud de certificación  | 01/09/2021 | 01/09/2021 |
| Certificación de SGSI implementado | 01/10/2021 | 15/11/2021 |

# PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN

Dentro de los planes de adquisiciones se encuentran los siguientes temas:

* Realizar pruebas de vulnerabilidades para corregir o minimizar posibles fallas en los controles de seguridad.
* Realizar la auditoría interna.
* Realizar la auditoría externa.

# DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS

La distribución presupuestal de los proyectos de inversión es la siguiente:

|  |  |
| --- | --- |
| **ACCIÓN** | **COSTO APROXIMADO** |
| Dentro del proyecto Fortalecimiento de la arquitectura tecnológica y los procesos asociados a la gestión de las tecnologías de la información y comunicaciones nacional incluye el ethical hacking | $ 24.000.000 |
| Adquisición de dispositivos de seguridad perimetral. | $ 120.000.000 |
| Adquisición de dispositivos de seguridad física (cámaras, CCTV, XVR,etc) |  $ 54.000.000 |
| Prestación de servicios para apoyo profesional para la implementación del SGSI |  $ 31.000.000 |
| Curso de formación para auditores internos (6 auditores) |  $ 25.000.000 |

# MAPAS DE RIESGOS

**Descripción del Riesgo:** Incumplimiento de las acciones de implementación de una o varias actividades descritas en el presente plan de Seguridad de la información.

**Causas:**

* Mecanismos insuficientes en la socialización de los controles a Implementar por parte del responsable de seguridad de la información hacia los propietarios, responsables o custodios de la información.
* Demoras en la Aprobación de presupuesto o personal que apoye la implementación de las acciones descritas en el presente plan de seguridad de la información.
* Indisponibilidad del personal al momento de cumplir o hacer cumplir los lineamientos y políticas definidos en el sistema de gestión de seguridad de la información.
* No contar con el apoyo de la dirección por desconocimiento en temas de seguridad y protección de la información de acuerdo con los modelos establecidos por el estado colombiano.
* Falta de personal responsable de hacer seguimiento al plan de seguridad de la información

**Consecuencias**:

* Posible materialización de riesgos Que afecten la confidencialidad integridad y/o disponibilidad de la información.
* Incumplimientos y valoraciones bajas en herramientas como MIPG y Política de Gobierno Digital.
* Atraso en la ejecución de actividades e implementación de controles qué prevengan la materialización de los riesgos de seguridad de la información.
* Afectación de la imagen institucional.
* Incumplimientos qué ocasionen sanciones legales o penales.



**Tipo de riesgo** Estratégico

**Probabilidad de**

**ocurrencia** Probable

**Impacto** Moderado

**Zona de riesgo** Alta

**14 CONTROL DE CAMBIOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versión** | **Código** | **Nombre** | **Aprobación** | **Control de cambios** |
| 1 |  A-OT-101 | Plan de Seguridad y Privacidad de la Información | Brújula, Diciembre 30 de 2020. | Creación documento. |