PLAN DE TRATAMIENTO

DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., septiembre de 2020

**CONTENIDO**

[1 ALCANCE DEL PLAN 3](#_Toc60244219)

[2 OBJETIVO 3](#_Toc60244220)

[3 OBJETIVOS ESPECÍFICOS 3](#_Toc60244221)

[4 ESTRATEGIAS 3](#_Toc60244222)

[5 PROYECTOS 4](#_Toc60244223)

[6 METAS 4](#_Toc60244224)

[7 ACCIONES 5](#_Toc60244225)

[8 PRODUCTOS 11](#_Toc60244226)

9 RESPONSABILIDADES………………………………………………………………............18

[10 CRONOGRAMA 26](#_Toc60244227)

[11 PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN 31](#_Toc60244228)

[12 DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN 31](#_Toc60244229)

[13 MAPAS DE RIESGOS 32](#_Toc60244230)

14 CONTROL DE CAMBIOS……………………………………………………………………. 34

#

# ALCANCE DEL PLAN

Al entrar en vigor el modelo integrado de planeación y gestión (MIPG) donde se integran los sistemas de gestión de calidad y el desarrollo administrativo, y en cumplimiento de los requisitos de incluir los riesgos que afecten a los activos de información en cuanto a su confidencialidad, integridad, y disponibilidad, el presente plan se aplica para todos los riesgos de seguridad de la información identificados que puedan o no afectar a más de un proceso o en su defecto a uno solo.

Lo anterior teniendo en cuenta que toda actividad lleva implícito un riesgo en algunos casos con un mayor impacto, este es parte de cualquier área o proceso de la entidad y de alguna forma define y ayuda a poner límites.

# OBJETIVO

Este plan tiene como objetivo definir lineamientos que puedan ser tomados como metodología para la identificación análisis y evaluación los riesgos, así como determinar los roles y responsabilidades de cada uno de los servidores públicos de la entidad frente a su propia gestión.

# OBJETIVOS ESPECÍFICOS

* Determinar aspectos comunes qué pueden afectar el desarrollo de las actividades de mitigación de riesgos en APC Colombia.
* Suministrar mecanismos o metodologías que permita a todas las áreas de APC Colombia gestionar de manera efectiva los riesgos generales que afectan la protección de la información de la agencia.
* Ofrecer una herramienta para que después de haber identificado, analizado y evaluado Los riesgos de seguridad de la información, se puedan identificar roles y responsabilidades frente al tratamiento o mejora de controles de mitigación te riesgos.
* Identificar las acciones de mejora que cada control requiere para su fortalecimiento, teniendo en cuenta los lineamientos definidos para la gestión del riesgo.
* Facilitar el monitoreo y revisión de las responsabilidades y ejecución de las actividades y controles definidos para mitigar el riesgo identificado.

# ESTRATEGIAS

La estrategia definida por la agencia quiere 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.

Para lograrlo se propone un trabajo conjunto entre todos los actores de la cooperación (entidades nacionales, autoridades locales, cooperantes, sector privado y sociedad civil) En 5 ejes de acción:

* **ampliar la visión** frente al alcance y las tendencias de la cooperación internacional para el desarrollo en el país.
* **fortalecer la gestión** de la cooperación bajo un enfoque de resultados, innovación y sostenibilidad.
* **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,
* **implementar mecanismos de coordinación** con una gobernanza pertinente y clara, y
* **definir criterios de priorización** de la demanda y la oferta de cooperación internacional.

# PROYECTOS

El tratamiento de los riesgos de seguridad de la información que se identificaron comprende dos tipos de proyectos, el primero correspondiente a las mejoras de los controles existentes, el segundo a la inclusión de controles definidos por la norma ISO/IEC 27001:2013. Se requiere:

* Adquirir herramientas tecnológicas que permitan el cifrado de información incluyendo la información contenida en copias de seguridad.
* Una revisión periódica de las vulnerabilidades que pueda tener la red, los aplicativos de cara al ciudadano y los equipos que se usan para el trabajo cotidiano.
* Sesiones de sensibilización que permitan la apropiada apropiación del Sistema de Gestión de Seguridad de la Información SGSI y sus controles, por parte de todos los servidores públicos y contratistas.
* Una revisión independiente del SGSI, en el marco de una auditoría interna.

#  METAS

Dentro de las metas propuestas a medida que se ejecute el plan de tratamiento de riesgos se propone lo siguiente:

* Trabajo conjunto de todas las áreas en la ejecución de las actividades necesarias para la mitigación de riesgos en APC Colombia.
* Riesgos de seguridad de la información gestionados de forma efectiva utilizando los mecanismos como la guía del DAFP.
* Roles y responsabilidades definidos en el marco de la gestión de los riesgos de seguridad de la información (digital) identificados.
* Mejoras de controles definidos y valorados como débiles o moderados, con el fin de fortalecerlos.

#  ACCIONES

Las acciones para mitigar los riesgos se ejecutarán teniendo en cuenta dos aspectos muy importantes

* Acciones de mejora de los controles que al ser evaluados su solidez fue diferente a fuerte
* Nuevos controles que se deben implementar y apoyan la mitigación de los riesgos.

Listado de controles identificados que, por su valoración en solidez, requieren un plan de mejora:

| **CONTROL** | **PLAN DE MEJORA / ACCIONES** |
| --- | --- |
|
|  |
| Identificación y valoración de los activos de información | Concienciación de la información que administran y genera cada una de las áreas y procesos de APC.Realizar ejercicios periódicos de actualización e identificación de activos de informaciónRealizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice |
| Aplicación de controles de acceso de acuerdo con perfiles definidos | Generar la documentación de perfiles de acceso para cada una de las áreas de APC.Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos.Implementar las directrices de seguridad para el acceso a la información |
| Control de uso de puertos USB | Identificación automática en el uso de dispositivo USB no autorizados.Definición de mecanismos tecnológicos y procedimientos de autorización para extraer informaciónSocialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer informaciónAcciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.Implementar las directrices de seguridad para el acceso a la información |
| Definición y socialización de las rutas digitales para el almacenamiento de la información | Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología. |
| Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información. | Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo.Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles.Aplicar política de seguridad para las copias de respaldo |
| Parámetros de seguridad aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes. | Crear acuerdos de confidencialidad y uso de información antes, durante y después de la vinculación laboral.Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadasContar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimosImplementar las directrices de seguridad para el acceso a la información |
| Revisión de calidad documental por el responsable de la información. | Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico |
| Mantenimientos preventivos | Generar un documento que puede ser anexado a la hoja de vida de los equipos |
| Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales | Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractualesDocumentar los resultados de las pruebas y dejar evidencias de estas.Documentar seguimientos de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales. |

**Nuevos controles y sus acciones**

A continuación, se presentan los riesgos con los nuevos controles propuestos y las actividades a ejecutar para estos controles:

| **RIESGO** | **DESCRIPCIÓN** | **NUEVO CONTROL** | **ACCIONES** |
| --- | --- | --- | --- |
|
|  |
| Pérdida de confidencialidad de la información valorada como de reserva o clasificada, en uno o varios procesos | Acceso no autorizado a la información que sea confidencial o de reserva. | Aplicación de la política de control de Acceso | Aplicar los controles técnicos necesarios para controlar el acceso a la información clasificada o de reservaSocializar la Política de control de acceso a todos los servidores y contratistas de la entidad. |
| Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información  |
| Poner en conocimiento de todos los empleados los procesos disciplinarios | Mediante charlas informativas socializar el proceso disciplinario y las responsabilidades de cada servidor público frente a la protección de la información clasificada o de reserva. |
| Acuerdos de confidencialidad | Firmar acuerdos de confidencialidad entre servidores públicos y la agencia, así como los contratistas la agencia  |
| Pérdida de información de uno o varios procesos | Imposibilidad de recuperación de información importante para un proceso o área, que se elimine o dañe. | Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información |
| Procedimientos para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes  |
| Pruebas de vulnerabilidad periódicas | Cada dos años realizar pruebas de vulnerabilidad a los aplicativos, la red, estaciones de trabajo y pruebas de ingeniería social  |
| Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información | Realizar un sondeo al año frente a temas de seguridad y protección de la informaciónEncuestas se seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información |
| Etiquetado y manejo de información acorde a niveles de clasificación | De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información  |
| Aplicar la política y el procedimiento de gestión de usuarios  | Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo |
| Pérdida de integridad de la información importante para uno o varios procesos | La veracidad de la información contenida en el activo de información se encuentra comprometida. | Etiquetado y manejo de información acorde a niveles de clasificación | De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información |
| Aplicar la política y el procedimiento de gestión de usuarios  | Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo |
| Procedimientos para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes  |
| Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información | Realizar un sondeo al año frente a temas de seguridad y protección de la información.Encuestas se seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información |
| Indisponibilidad de la información contenida en los sistemas de información | El sistema de información presenta fallas asociadas al funcionamiento o comunicación con él. | Procedimientos para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes |
| Pruebas de vulnerabilidad periódicas | Ejecución de pruebas de vulnerabilidad a los sistemas de información al menos una vez cada dos años. |

**Nota:** Es importante aclarar que los riesgos identificados aplican para todas las áreas y procesos por ende la ejecución de los controles dependerá de manera conjunta entre los responsables mencionados y los jefes de todas las áreas con su equipo de trabajo. En especial se aplica para todas las áreas qué han identificado activos de información en un nivel alto o muy alto de confidencialidad, integridad o disponibilidad.

# PRODUCTOS

Dentro de los productos que se deben generar en el transcurso de la aplicación del plan de tratamiento de riesgos de seguridad de la información se encuentran

* Mejoras definidas para los controles que su nivel de solidez fue diferente a fuerte, con su respectiva evidencia que a continuación se listan
* controles nuevos diseñados, generando las actividades previstas y con las evidencias o productos que a continuación se listan

**Productos esperados de las acciones de mejora de los controles que su nivel de madurez fue débil o moderado:**

| **CONTROL** | **PLAN DE MEJORA** | **RESPONSABLES** | **EVIDENCIA DE LO ESPERADO** |
| --- | --- | --- | --- |
|
| Identificación y valoración de los activos de información | Concienciación de la información que administran y genera cada una de las áreas y procesos de APC.Realizar ejercicios periódicos de actualización e identificación de activos de informaciónRealizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice | Responsables de Áreas y procesos de APC | Inventario de Activos de Información debidamente diligenciado y con las valoraciones correspondientes por parte de todas las áreas de APC. |
| Aplicación de controles de acceso de acuerdo con perfiles definidos | Generar la documentación de perfiles de acceso para cada una de las áreas de APC.Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimosImplementar las directrices de seguridad para el acceso a la información | Responsables de Áreas y procesos de APC | - Perfiles definidos por área- Protocolo de configuraciones de acceso a la información implementado para todos los servidores públicos y contratistas |
| Control de uso de puertos USB | Identificación automática en el uso de dispositivo USB no autorizados.Definición de mecanismos tecnológicos y procedimientos de autorización para extraer informaciónSocialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer informaciónAcciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.Implementar las directrices de seguridad para el acceso a la información | Oficina de Tecnologíajefes de áreasTodos los servidores públicos y contratistasPersona asignada con las responsabilidades de Seguridad de la Información | - USB bloqueadas y alertas configuras por intentos de descarga, debidamente documentadas y socializadas con las áreas y procesos- Política de control de Acceso- Socialización de implicaciones disciplinarias o jurídicas frente al uso de información privilegiada sin el debido proceso y autorización |
| Definición y socialización de las rutas digitales para el almacenamiento de la información | Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología. | Oficina de Tecnologíajefes de áreasTodos los servidores públicos y contratistas | - Información de la entidad almacenada en los repositorios definidos |
| Identificación y valoración de los activos de información | Concienciación de la información que administran y genera cada una de las áreas y procesos de APC.Realizar ejercicios periódicos de actualización e identificación de activos de informaciónRealizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice | Responsables de Áreas y procesos de APC | Inventario de Activos de Información debidamente diligenciado y con las valoraciones correspondientes por parte de todas las áreas de APC. |
| Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información. | Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo.Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles.Aplicar política de seguridad para las copias de respaldo | Oficina de TecnologíaResponsables de información (jefes de área, servidores públicos y contratistas) | - Pruebas de restauración debidamente documentadas y realizadas con los propietarios de la información- Plan de copias de seguridad donde se incluya al menos una prueba de restauración con cada área en el año. |
| Parámetros de seguridad aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes. | Crear acuerdos de confidencialidad y uso de información antes, durante y después de la vinculación laboral.Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadasContar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimosImplementar las directrices de seguridad para el acceso a la información | ContractualTalento HumanoOficina de Tecnología | - Acuerdos de confidencialidad debidamente firmados- Acuerdos de transferencia de información debidamente firmados- Usuarios activos conforme a planta y contratistas en funcionamiento |
| Revisión de calidad documental por el responsable de la información. | Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico | Responsables de área que deben publicar, transferir o compartir información. | - Modificaciones en el proceso de publicación, donde se evidencie la revisión de calidad- Seguimientos documentados por parte de control de cambios en la documentación. |
| Mantenimientos preventivos | Generar un documento que puede ser anexado a la hoja de vida de los equipos | Tecnología | - Información documentada de los mantenimientos realizados en el año, por cada equipo. |
| Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales | Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractualesDocumentar los resultados de las pruebas y dejar evidencias de estas.Documentar seguimientos de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales | Oficina de Tecnología | - Plan de seguimientos y pruebas a proveedores de servicios esenciales en tecnología- Documentación de las pruebas realizadas a la prestación por parte de terceros de servicios esenciales en Tecnología |

**Productos esperados de las acciones para los nuevos controles definidos**

| **NUEVO CONTROL** | **ACCIONES** | **EVIDENCIA DE LO ESPERADO** |
| --- | --- | --- |
|
| Aplicación de la política de control de Acceso | Aplicar los controles técnicos necesarios para controlar el acceso a la información clasificada o de reservaSocializar la Política de control de acceso a todos los servidores y contratistas de la entidad. | Política de Control de AccesoControles aplicadosListados de asistenciaPiezas de divulgación |
| Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información   | Política para el uso de controles criptográficosAplicativo configuradoListados de asistenciaPiezas de divulgación |
| Poner en conocimiento de todos los empleados los procesos disciplinarios | Mediante charlas informativas socializar el proceso disciplinario y las responsabilidades de cada servidor público frente a la protección de la información clasificada o de reserva. | Listados de asistenciaPiezas de divulgación |
| Acuerdos de confidencialidad | Firmar acuerdos de confidencialidad entre servidores públicos y la agencia, así como los contratistas la agencia  | Acuerdos firmados por todos los servidores públicos y contratistas o proveedores |
| Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información | Política para el uso de controles criptográficosAplicativo configuradoListados de asistenciaPiezas de divulgación |
| Procedimiento para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes  | Procedimiento para reporte y atención de incidentesAplicativo configuradoListados de asistenciaPiezas de divulgaciónIncidentes documentados |
| Pruebas de vulnerabilidad periódicas | Cada dos años realizar pruebas de vulnerabilidad a los aplicativos, la red, estaciones de trabajo y pruebas de ingeniería social  | Pruebas planificadas ejecutadas y documentadasPlanes de remediación y ejecución de estos |
| Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información | Realizar un sondeo al año frente a temas de seguridad y protección de la informaciónEncuestas se seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información | Plan de sensibilización en temas de seguridad de la informaciónListados de asistenciaPiezas de divulgaciónEncuestas de sondeo y seguimiento diligenciadas y documentadas |
| Etiquetado y manejo de información acorde a niveles de clasificación | De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información  | Procedimiento de etiquetado socializadoDocumentos con marca de agua, de forma impresa o digitalArchivadores y carpetas etiquetados |
| Aplicar la política y el procedimiento de gestión de usuarios  | Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo | Política de gestión de usuariosProcedimiento de gestión de usuariosUsuarios actualizados en el directorio activo |

**9 RESPONSABILIDADES**

Todas las áreas y procesos son responsables de aplicar los controles necesarios para la protección de la información, en este sentido los riesgos identificados, las mejoras en sus controles existentes y la implementación de los nuevos controles tienen como responsables directos a todos los servidores públicos, contratistas o terceros que tengan acceso a la información por razón de sus funciones.



Cada control cuenta con su responsable definido de acuerdo con la autoridad que éste tiene y a la segregación de funciones definida en la agencia, en la descripción de las actividades se menciona la periodicidad de la implementación de cada uno de los controles qué actividades se deben realizar y las evidencias del control.

Responsables de acciones para los planes de mejora de los controles:

| **CONTROL** | **PLAN DE MEJORA / ACCIONES** | **RESPONSABLES** |
| --- | --- | --- |
|
|  |
| Identificación y valoración de los activos de información | Concienciación de la información que administran y genera cada una de las áreas y procesos de APC.Realizar ejercicios periódicos de actualización e identificación de activos de informaciónRealizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice | Responsables de Áreas y procesos de APC |
| Aplicación de controles de acceso de acuerdo con perfiles definidos | Generar la documentación de perfiles de acceso para cada una de las áreas de APC.Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos.Implementar las directrices de seguridad para el acceso a la información | Responsables de Áreas y procesos de APC |
| Control de uso de puertos USB | Identificación automática en el uso de dispositivo USB no autorizados.Definición de mecanismos tecnológicos y procedimientos de autorización para extraer informaciónSocialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer informaciónAcciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.Implementar las directrices de seguridad para el acceso a la información | Oficina de Tecnologíajefes de áreasTodos los servidores públicos y contratistasPersona asignada con las responsabilidades de Seguridad de la Información |
| Definición y socialización de las rutas digitales para el almacenamiento de la información | Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología. | Oficina de Tecnologíajefes de áreasTodos los servidores públicos y contratistas |
| Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información. | Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo.Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles.Aplicar política de seguridad para las copias de respaldo | Oficina de TecnologíaResponsables de información (jefes de área, servidores públicos y contratistas) |
| Parámetros de seguridad aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes. | Crear acuerdos de confidencialidad y uso de información antes, durante y después de la vinculación laboral.Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadasContar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimosImplementar las directrices de seguridad para el acceso a la información | ContractualTalento HumanoOficina de Tecnología |
| Revisión de calidad documental por el responsable de la información. | Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico | Responsables de área que deben publicar, transferir o compartir información. |
| Mantenimientos preventivos | Generar un documento que puede ser anexado a la hoja de vida de los equipos | Oficina de Tecnología |
| Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales | Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractualesDocumentar los resultados de las pruebas y dejar evidencias de estas.Documentar seguimientos de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales. | Oficina de Tecnología |

**Responsables de la implementación de los nuevos controles**

| **RIESGO** | **DESCRIPCIÓN** | **NUEVO CONTROL** | **ACCIONES** | **RESPONSABLE** |
| --- | --- | --- | --- | --- |
|
|  |
| Pérdida de confidencialidad de la información valorada como de reserva o clasificada, en uno o varios procesos | Acceso no autorizado a la información que sea confidencial o de reserva. | Aplicación de la política de control de Acceso | Aplicar los controles técnicos necesarios para controlar el acceso a la información clasificada o de reservaSocializar la Política de control de acceso a todos los servidores y contratistas de la entidad. | Oficina de Tecnología |
| Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información  | Oficina de Tecnología |
| Poner en conocimiento de todos los empleados los procesos disciplinarios | Mediante charlas informativas socializar el proceso disciplinario y las responsabilidades de cada servidor público frente a la protección de la información clasificada o de reserva. | Oficina de Control Interno |
| Acuerdos de confidencialidad | Firmar acuerdos de confidencialidad entre servidores públicos y la agencia, así como los contratistas la agencia  | Talento Humano / Contractual |
| Pérdida de información de uno o varios procesos | Imposibilidad de recuperación de información importante para un proceso o área, que se elimine o dañe. | Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información | Oficina de Tecnología |
| Procedimientos para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes  | Oficina de Tecnología / Responsable de seguridad de la información |
| Pruebas de vulnerabilidad periódicas | Cada dos años realizar pruebas de vulnerabilidad a los aplicativos, la red, estaciones de trabajo y pruebas de ingeniería social  | Oficina de Tecnología |
| Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información | Realizar un sondeo al año frente a temas de seguridad y protección de la informaciónEncuestas se seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información | Responsable de seguridad de la información |
| Etiquetado y manejo de información acorde a niveles de clasificación | De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información  | Gestión documental / Todas las áreas y procesos |
| Aplicar la política y el procedimiento de gestión de usuarios  | Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo | Oficina de Tecnología / Todas las áreas y procesos |
| Pérdida de integridad de la información importante para uno o varios procesos | La veracidad de la información contenida en el activo de información se encuentra comprometida. | Etiquetado y manejo de información acorde a niveles de clasificación | De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información | Gestión documental / Todas las áreas y procesos |
| Aplicar la política y el procedimiento de gestión de usuarios  | Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo | Oficina de Tecnología / Todas las áreas y procesos |
| Procedimientos para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes  | Oficina de Tecnología / Responsable de seguridad de la información |
| Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información | Realizar un sondeo al año frente a temas de seguridad y protección de la informaciónEncuestas se seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información | Responsable de seguridad de la información |
| Indisponibilidad de la información contenida en los sistemas de información | El sistema de información presenta fallas asociadas al funcionamiento o comunicación con él. | Procedimientos para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes | Oficina de Tecnología / Responsable de seguridad de la información |
| Pruebas de vulnerabilidad periódicas | Ejecución de pruebas de vulnerabilidad a los sistemas de información al menos una vez cada dos años. | Oficina de Tecnología |

# CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma con vigencia al 2021.

 **Plan de mejora para los controles que su nivel de solidez es débil o moderado**

| **CONTROL** | **PLAN DE MEJORA** | **RESPONSABLES** | **FECHAS DE****IMPLEMENTACIÓN** |
| --- | --- | --- | --- |
| **INICIO** | **FIN** |
| Identificación y valoración de los activos de información | Concienciación de la información que administran y genera cada una de las áreas y procesos de APC.Realizar ejercicios periódicos de actualización e identificación de activos de informaciónRealizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice | Responsables de Áreas y procesos de APC | 01/11/2020 | 30/10/2021 |
| Aplicación de controles de acceso de acuerdo con perfiles definidos | Generar la documentación de perfiles de acceso para cada una de las áreas de APC.Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimosImplementar las directrices de seguridad para el acceso a la información | Responsables de Áreas y procesos de APC | 01/11/2020 | 31/12/2021 |
| Control de uso de puertos USB | Identificación automática en el uso de dispositivo USB no autorizados.Definición de mecanismos tecnológicos y procedimientos de autorización para extraer informaciónSocialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer informaciónAcciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.Implementar las directrices de seguridad para el acceso a la información | Oficina de Tecnologíajefes de áreasTodos los servidores públicos y contratistasPersona asignada con las responsabilidades de Seguridad de la Información | 01/06/2021 | 31/12/2021 |
| Definición y socialización de las rutas digitales para el almacenamiento de la información | Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología. | Oficina de Tecnologíajefes de áreasTodos los servidores públicos y contratistas | 01/11/2020 | 301/12/2020 |
| Identificación y valoración de los activos de información | Concienciación de la información que administran y genera cada una de las áreas y procesos de APC.Realizar ejercicios periódicos de actualización e identificación de activos de informaciónRealizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice | Responsables de Áreas y procesos de APC | 01/11/2020 | 30/10/2021 |
| Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información. | Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo.Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles.Aplicar política de seguridad para las copias de respaldo | Oficina de TecnologíaResponsables de información (jefes de área, servidores públicos y contratistas) | 01/03/2021 | 31/12/2021 |
| Parámetros de seguridad aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes. | Crear acuerdos de confidencialidad y uso de información antes, durante y después de la vinculación laboral.Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadasContar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimosImplementar las directrices de seguridad para el acceso a la información | ContractualTalento HumanoOficina de Tecnología | 01/11/2020 | 30/10/2021 |
| Revisión de calidad documental por el responsable de la información. | Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico | Responsables de área que deben publicar, transferir o compartir información. | 01/03/2021 | 31/12/2021 |
| Mantenimientos preventivos | Generar un documento que puede ser anexado a la hoja de vida de los equipos | Tecnología | 01/12/2020 | 31/01/2021 |
| Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales | Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractualesDocumentar los resultados de las pruebas y dejar evidencias de estas.Documentar seguimientos de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales | Oficina de Tecnología | 01/03/2021 | 31/12/2021 |

 **Plan de implementación de nuevos controles**

| **NUEVO CONTROL** | **ACTIVIDADES** | **FECHAS** |
| --- | --- | --- |
| **INICIO** | **FIN** |
| Aplicación de la política de control de Acceso | Aplicar los controles técnicos necesarios para controlar el acceso a la información clasificada o de reservaSocializar la Política de control de acceso a todos los servidores y contratistas de la entidad. | 30/11/2020 | 30/11/2021 |
| Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información  | 01/03/2021 | 31/12/2021 |
| Poner en conocimiento de todos los empleados los procesos disciplinarios | Mediante charlas informativas socializar el proceso disciplinario y las responsabilidades de cada servidor público frente a la protección de la información clasificada o de reserva. | 30/11/2020 | 01/02/2021 |
| Acuerdos de confidencialidad | Firmar acuerdos de confidencialidad entre servidores públicos y la agencia, así como los contratistas la agencia  | 02/01/2021 | 02/03/2021 |
| Aplicación de la política para el uso de controles criptográficos | Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información | 01/03/2021 | 31/12/2021 |
| Procedimiento para reporte y atención de incidentes | Socializar, divulgar y aplicar el procedimiento de atención de incidentes  | 01/11/2020 | 02/03/2021 |
| Pruebas de vulnerabilidad periódicas | Cada dos años realizar pruebas de vulnerabilidad a los aplicativos, la red, estaciones de trabajo y pruebas de ingeniería social  | 01/02/2021 | 31/12/2021 |
| Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información | Realizar un sondeo al año frente a temas de seguridad y protección de la informaciónEncuestas se seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información | 01/02/2021 | 31/12/2021 |
| Etiquetado y manejo de información acorde a niveles de clasificación | De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información  | 01/02/2021 | 31/12/2021 |
| Aplicar la política y el procedimiento de gestión de usuarios  | Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo | 30/11/2020 | 30/11/2021 |

# 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:

* Adquisición de un software que permita el cifrado de la información
* Ethical hacking que compruebe aplicaciones internas, red, pc de escritorio y pruebas de ingeniería social
* Plan de adquisiciones para copias de seguridad

# DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

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

|  |  |  |  |
| --- | --- | --- | --- |
| **PLAN DE COMPRAS** | **CONTROL AL QUE SOPORTA** | **ENTREGABLE** | **COSTO APROXIMADO MERCADO** |
| Adquisición de un software que permita el cifrado de la información | Aplicación de la política para el uso de controles criptográficos | Aplicación de cifrado a información catalogada como confidencial o de reserva. |  |
| Ethical hacking que compruebe aplicaciones internas, red, pc de escritorio y pruebas de ingeniería social | Pruebas de vulnerabilidad periódica | Planes de remediacionesInforme de vulnerabilidades |  |
| Plan de adquisiciones para copias de seguridad  | Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información. | Documentación de seguimiento sobre pruebas restauración de las copias de seguridad realizadas |  |

# 13 MAPAS DE RIESGOS

**Descripción del Riesgo:**

Incumplimiento de las acciones de implementación para los controles descritas en el plan de tratamiento de riesgos de seguridad de la información

**Causas:**

* Mecanismos insuficientes en la socialización de los controles a los propietarios de la información
* Demoras en la aplicación de los controles por parte de los custodios, responsables y propietarios de la información
* Demoras en los tiempos de contratación
* Falta de personal responsable de hacer seguimiento al plan de tratamiento de riesgos de seguridad de la información

**Consecuencias:**

* Posible materialización de riesgos de seguridad de la información
* 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-103 | Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.  | Brújula, Diciembre 30 de 2020. | Creación documento. |