POLÍTICA DE SEGURIDAD DE INFORMACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)EN EL FONDO ADAPTACIÓN

Código 5-PAT-P-01. Versión 3.0
Bogotá D.C. mayo de 2019

El emprendimiento es de todos
Minhacienda

Fondo Adaptación

365 Rendición

EQUIPO DIRECTIVO DEL FONDO ADAPTACIÓN:

EDGAR ORTIZ PABÓN
Gerente

ANIBAL JOSÉ PÉREZ GARCÍA
Subgerente de Gestión del Riesgo

RAFAEL EDUARDO ABUCHAIBE LÓPEZ
Subgerente de Proyectos

ANDRES AUGUSTO PARRA BELTRAN
Subgerente de Estructuración

LINA MARÍA BARRERA RUEDA
Subgerente de Regiones

MARÍA LORENA CUELLAR CRUZ
Secretaria General

VICTOR ALEJANDRO VENEGAS MENDOZA
Jefe Oficina Asesora de Planeación y Cumplimiento

Investigación y Textos:
JORGE WILLIAM ALZATE SÁNCHEZ
Asesor I Equipo de trabajo tecnología de información

Política de Seguridad del Sistema de Gestión de Seguridad de la Información (SGSI). Código 5-PAT-P-01. Versión 3
Bogotá D.C., mayo de 2019

CONTROL DE CAMBIOS Y NOMENCLATURA

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	2014/12	Documento inicial
2.0	2017/12	Complemento de las políticas que aplican al proceso de Gestión de Tecnología de acuerdo con la norma NTC/ISO 27001:2013.
3.0	2019/03	Revisión y aprobación de las políticas por parte del Comité de Gestión y Desempeño de la entidad

ACERCA DEL FONDO ADAPTACIÓN

El Fondo Adaptación nace en diciembre de 2010, como parte de la respuesta del Gobierno a la peor emergencia invernal que ha sufrido el país en toda su historia: El Fenómeno de "La Niña" 2010-2011, el cual demandó una declaratoria de emergencia económica, social y ecológica. Una tragedia que dejó cerca de 4 millones de damnificados en 1004 municipios, lo que representa un 97% del país afectado por la inundación provocada por el fenómeno natural.

El Fondo Adaptación se crea entonces para atender las inversiones públicas de largo plazo, destinadas a recuperar la infraestructura pública afectada por esta tragedia, dentro de los límites de recursos que le fueron asignados.

Tabla de contenido

1 PRESENTACIÓN

La dirección del Fondo Adaptación, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Fondo Adaptación, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

2 CONCEPTOS BÁSICOS

Los siguientes conceptos corresponden al Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el decreto 1078 de 2015 y robustecido en 2016 a través del Conpes 3854 con el fin de fortalecer las capacidades para "identificar, gestionar, tratar y mitigar los riesgos de seguridad digital" en las actividades socioeconómicas del entorno digital. La conceptualización de esta política se fundamenta en la Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27001).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

3 Política General de Seguridad y Privacidad de la Información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Fondo Adaptación con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información. Esta política orienta sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información del Fondo Adaptación, tomando como base que la efectividad de esta política depende finalmente del comportamiento de las personas, (por lo que saben, lo que sienten y que estén dispuestos a realizar) y los controles establecidos en las políticas de seguridad descritas en el presente documento, así como por medio de la generación y publicación de sus políticas, procedimientos e instructivos, de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El Fondo Adaptación, para asegurar su dirección estratégica, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Fondo Adaptación.

3.1 Justificación de la Política para la Gestión de Seguridad de la Información

El Fondo Adaptación realiza esta declaración de compromiso, justificada en que para la Entidad es muy importante contar con políticas de seguridad ya que son ellas quienes guiarán el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir. Debido a la

importancia y sensibilidad de la información, se incluye el sistema de seguridad de la información dentro del sistema de gestión de la entidad de tal forma que le permita generar la mejora continua del sistema de seguridad, basados en la gestión de riesgos y continuidad del Fondo Adaptación.

3.2 Alcance/Aplicabilidad de la Política para la Gestión de Seguridad de la Información

- Esta política define las pautas para asegurar una adecuada protección y seguridad de la información de la entidad, para el proceso de Gestión de Tecnología de Información, quien las establecerá dentro del plan estratégico de TI (PETI), y las desarrollará con los recursos asignados para su ejecución.
- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Fondo Adaptación y la ciudadanía en general.
- Aplica para todos los activos de información de la Entidad, los que incluyen: software, hardware, procesos, funcionarios, terceros, infraestructura e información en general de la entidad.

3.3 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

3.4 Políticas Generales

A continuación se establecen las políticas generales de seguridad de información que soportan el Sistema de Gestión de Seguridad de la Información del Fondo Adaptación:

- El Fondo Adaptación ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- El Fondo Adaptación protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.
- El Fondo Adaptación protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El Fondo Adaptación protegerá su información de las amenazas originadas por parte del personal.

- El Fondo Adaptación protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Fondo Adaptación controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El Fondo Adaptación implementará control de acceso a la información, sistemas y recursos de red.
- El Fondo Adaptación garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El Fondo Adaptación garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- El Fondo Adaptación garantizará la disponibilidad de sus procesos y la continuidad de su operación, basado en el impacto que pueden generar los eventos.
- El Fondo Adaptación garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

4 POLÍTICAS ESPECÍFICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Estas políticas se establecen de acuerdo con los activos de información de la entidad, los procesos y los servicios de información que presenta el Fondo Adaptación, enmarcados dentro del proceso de Gestión de TI.

4.1 Organización de la Seguridad de la Información

Por medio de esta política se define el comité directivo de seguridad de la información y sus objetivos. El Fondo Adaptación creará un esquema de seguridad de información donde se definan roles y responsabilidades que involucren actividades de operación, gestión y administración de la seguridad de la información.
El Comité de Desarrollo Administrativo de la entidad actuará como comité directivo de seguridad y será el ente encargado de velar por el desarrollo, aplicación, cumplimiento y mejoramiento continuo de los programas o las distintas actividades y proyectos que se desarrollen en el Sistema de Gestión de Seguridad de la Información. Así mismo debe verificar el cumplimiento de las políticas aquí definidas.

4.2 Política para uso de dispositivos móviles

Por medio de esta política se establecen las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas), entre otros suministrados por la entidad y personales que hagan uso de los servicios de información del Fondo Adaptación.

- Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (smart phones) tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.
- Los dispositivos móviles asignados por el Fondo Adaptación deben tener la configuración realizada por el Área de Tecnología, así mismo solo podrá configurarse únicamente las cuentas de correo electrónico asignadas al usuario por la entidad.
- Se autoriza el uso de WhatsApp pero no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).
- Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual.
- Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la entidad.

- Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al Equipo de Trabajo de Gestión Servicios, y continuar con el procedimiento administrativo por pérdida de elementos establecido por la entidad.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por el Fondo Adaptación con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.
- Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.
- Los usuarios de dispositivos móviles asignados por la entidad, deben evitar hacer uso de lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.
- Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).
- Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.
- En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar al comité de seguridad de la información para su aprobación.

4.3 Política de seguridad para los recursos humanos

Por medio de esta política se establecen las directrices para que los funcionarios, contratistas y demás colaboradores del Fondo Adaptación, entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores del Fondo Adaptación, adopten sus responsabilidades en relación con las políticas de seguridad de la información de la entidad y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.
- Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación al Fondo Adaptación para el tratamiento de sus datos personales de acuerdo a la Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- A la firma del contrato laboral o posesión del cargo el funcionario debe firmar un acuerdo de confidencialidad para con el Fondo Adaptación.
- Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.
- Los funcionarios del Fondo Adaptación deben cumplir con el manual de Excelencia Ética y Buen Gobierno, Resolución 390 de 2017.

- En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

4.4 Política de Gestión de Activos de Información

Estas políticas hacen referencia a los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de información. Algunas de estas políticas se encuentran definidas en la documentación del Modelo de Gestión de Información de la entidad.

- Identificación y Clasificación de los Activos de Información: Debe realizarse y mantenerse un inventario de activos de información que permita identificar lo siguiente:
  - Propiedad del activo: nombre, propietario y custodio técnico del activo
  - Acceso: Derechos de acceso sobre el activo
  - Tipo de activo: Si es información, software, físico, servicios o un intangible.
  - Valor del activo: Definida por su confidencialidad, integridad, disponibilidad.
  - Clasificación: Determinar su clasificación de acuerdo a la criticidad, sensibilidad y reserva del activo.
  - Ubicación: Establecer si la ubicación es física o electrónica y el lugar donde se encuentra.
- Propietarios de activos de información: El Fondo Adaptación es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios contratistas de la entidad, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato. Así mismo el Fondo Adaptación es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la entidad (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología de Información (TIC).

4.5 Política de Uso de Activos de Información

El objetivo de esta política es lograr mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

- Los activos de información pertenecen al Fondo Adaptación y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Área de Tecnología de Información.

- El Fondo Adaptación proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad del Fondo Adaptación, los funcionarios solo podrán realizar respaldo de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la entidad; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.
- Periódicamente, el Área de Tecnología de la Información efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considerada como una violación a las Políticas de Seguridad de la Información de la entidad.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Jefe de la dependencia al Área de Tecnología de Información.
- Estarán bajo custodia del Área de Tecnología de la Información los medios magnéticos/electrónicos (disquetes, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.
- En caso de ser necesario y previa autorización del comité de seguridad de la Información del Fondo Adaptación, los funcionarios de la entidad podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.
- Los recursos informáticos del Fondo Adaptación no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Tecnología de la Información:
    - Instalar software en cualquier equipo del Fondo Adaptación;
    - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo del Fondo Adaptación;
    - Modificar, revisar, transformar o adaptar cualquier software propiedad de la entidad;

  - Descompilar o realizar ingeniería inversa en cualquier software de propiedad del Fondo Adaptación.
  - Copiar o distribuir cualquier software de propiedad del Fondo Adaptación.
  - Cambiar la configuración de hardware de propiedad del Fondo Adaptación.
- El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información del Fondo Adaptación que tenga conocimiento y al Área de Tecnología de Información.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
- Ningún usuario deberá acceder a la red o a los servicios TIC del Fondo Adaptación, utilizando una cuenta de usuario o clave de otro usuario.
- Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc), esto compromete la seguridad de los recursos informáticos del Fondo Adaptación.
- El Área de Tecnología de Información del Fondo Adaptación, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.
- Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura TIC del Fondo Adaptación.
- Todos los archivos provenientes de equipos externos al Fondo Adaptación, deben ser revisados para detección de virus antes de su utilización dentro de la red de la entidad.
- Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios del Área de Tecnología de Información del Fondo Adaptación.
- La información del Fondo Adaptación debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información este segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.
- Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por el Fondo Adaptación en el proceso de desvinculación, de igual manera deberán documentar y entregar al Fondo Adaptación los conocimientos importantes que posee de la labor que ejecutan.

4.6 Política de Uso de estaciones cliente

El objetivo de esta política es garantizar que la seguridad es parte integral de los activos de información y la correcta utilización por los usuarios finales.

- La instalación de software en los computadores suministrados por el Fondo Adaptación, es una función exclusiva del Área de Tecnología de Información, la cual mantendrá una lista actualizada del software autorizado para instalar en los computadores.
- Los usuarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.
- En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.
- Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación cliente asignada por el Fondo Adaptación y deberán ubicar copias y documentos finales en las carpetas de Drive de Google y en Mis Documentos para garantizar la copia de respaldo que se hace diariamente al equipo.
- El préstamo de equipos de cómputo, computadores portátiles se debe hacer a través de la mesa de ayuda de TI con anticipación y se proveerá de acuerdo a la disponibilidad.
- Los equipos que ingresan temporalmente al Fondo Adaptación que son de propiedad de terceros, deben ser registrados en los controles de acceso de la entidad para poder realizar su retiro; posteriormente el Fondo Adaptación no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
- El Área de Tecnología de la Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean del Fondo Adaptación.

4.7 Política de seguridad de equipos de propiedad de contratistas

Por medio de esta política se dictan los lineamientos para el uso de equipos de propiedad de contratistas que se conectan a la infraestructura tecnológica del Fondo Adaptación.

- Antes de conectar por primera vez un computador de propiedad de un contratista de la entidad deberá reportarse al Área de Tecnología de Información quien se encargará de analizar el equipo e ingresarlo a la base de datos de control de equipos de terceros que usan la infraestructura tecnológica de la entidad.
- Estos equipos deberán tener un nombre de equipo que permita identificar claramente a quién pertenece. Esta identificación se hace con el fin de tener rastro del equipo en la red del Fondo Adaptación. Si esta identificación no es clara se le debe pedir al contratista que haga el cambio de nombre del equipo.
- Estos equipos deben tener instalado un antivirus debidamente actualizado y licenciado. Además deben tener la política de actualización automática del sistema operativo y del software de antivirus.

- Los contratistas propietarios de estos equipos deben seguir las políticas asociadas al uso de los puntos de red de datos, las políticas de uso de impresoras y del servicio de impresión, la política de uso de internet y las políticas específicas para usuarios del Fondo Adaptación.
- El Área de Tecnología de la Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a estos equipos.
- El software instalado en los equipos de contratistas debe ser software legal con sus respectivas licencias de uso.
- El Fondo Adaptación no se hace responsable por la pérdida, daño o hurto del equipo dentro de las instalaciones de la entidad o de daños que se presenten en estos equipos producto de la conexión a las redes eléctricas y de datos del Fondo Adaptación.
- Los contratistas son responsables de la información que se procesa y almacena en estos equipos, por lo tanto el Fondo Adaptación no hará respaldo de esta información. Si existiera la necesidad de respaldar información presente en uno de estos equipos debe solicitarse expresamente al Área de Tecnología de Información la necesidad quien evaluará el mecanismo de respaldo dependiendo del tipo de equipo, su ubicación, el tamaño de la información y la frecuencia con que debe respaldarse.
- Los contratistas que hacen uso de los servicios de impresión se les creará una cuenta de usuario en el directorio activo del Fondo Adaptación con el fin que pueda autenticarse en la red de datos de la entidad. Esta cuenta de usuario no crea ninguna responsabilidad de la entidad con la seguridad y uso del equipo la cual seguirá siendo exclusivamente del contratista.
- Está prohibido la instalación de software propiedad del Fondo Adaptación en estos equipos. Sólo se podrá instalar siempre y cuando el contrato con la entidad así lo estipule.
- El Área de Tecnología de Información podrá verificar en cualquier momento que los equipos de los contratistas estén siguiendo las políticas de seguridad aquí establecidas. En caso de no cumplirlas podrán exponerse a las sanciones administrativas y legales pertinentes.

4.8 Política de Uso de Internet

Por medio de esta política se establecen los lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

- La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad del Fondo Adaptación, por lo tanto se reserva el derecho de monitorear el tráfico de internet y el acceso a la información.
- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas del Fondo Adaptación o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el Fondo Adaptación. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del comité de seguridad de la Información de la entidad.
- El Área de Tecnología de Información administrará la autorización de navegación a los usuarios del Fondo Adaptación, previa solicitud del Jefe de la dependencia.
- El Área de Tecnología de Información implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.
- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.
- Los usuarios de los activos de información del Fondo Adaptación tienen prohibido el acceso a redes sociales, sistemas de mensajería instantánea y cuentas de correo no institucional.

4.9 Política de disposición de información, medios y equipos

El objetivo de esta política es contrarrestar las interrupciones en las actividades del Fondo Adaptación, proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna, permitiendo la confidencialidad, integridad y disponibilidad de la información.

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
- Se debe realizar la aplicación del procedimiento de borrado seguro definido por el Fondo Adaptación.
- Está restringido del uso de medios removibles de almacenamiento, por lo cual se deshabilita la funcionalidad de los puertos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través Comité de Seguridad de la Información y enviada al área de Tecnología de Información.
- Se debe implementar el procedimiento para la transferencia de medios físicos.

4.10 Política de control de acceso

El objetivo de esta política es asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática del Fondo Adaptación, así como el uso de medios de computación móvil.

- El Equipo de Trabajo de Gestión Servicios definirá el procedimiento de acceso físico (Funcionarios, visitantes, contratistas, proveedores) a las instalaciones de la entidad en coordinación el Área de Tecnología de Información.
- El Equipo de Trabajo de Gestión Servicios, establecerá un programa de mantenimiento integral de los sistemas de control de acceso y sistema de video seguridad (Circuito cerrado de televisión CCTV), así mismo administrará estas plataformas.
- El Área de Tecnología de Información establecerá el procedimiento para establecer los niveles de acceso para usuarios de los servicios y sistemas de información del Fondo Adaptación.
- El Área de Tecnología de Información establecerá las configuraciones de las políticas en los sistemas de tecnología y comunicaciones para el control de acceso a los activos de información.
- El Fondo Adaptación proporcionará a los funcionarios todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tabletas, enrutadores, agendas electrónicas, celulares inteligentes, access point, el Área de Tecnología de Información podrá realizar la mencionada conexión previa solicitud del interesado, y evaluará la pertinencia y necesidad de la conexión del dispositivo.
- El Fondo Adaptación suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.
- Es responsabilidad del usuario el manejo apropiado a las claves asignadas de los servicios de red y de acceso a la red. Estas claves de acceso y usuarios son personales e intransferibles.
- Solo usuarios designados por el Área de Tecnología de Información estarán autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones del Fondo Adaptación, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software maliciosos.
- Todo trabajo a realizarse en los servidores del Fondo Adaptación con información de la entidad, por parte de sus funcionarios o contratistas, se debe realizar en las instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del Jefe del Área de Tecnología de Información del Fondo Adaptación.
- El Área de Tecnología de Información establecerá el procedimiento de registro, cancelación y periodicidad de revisión y ajuste a permisos de acceso a la red y servicios de red, asignados a los usuarios de los sistemas de información y comunicaciones del Fondo Adaptación, tomando como base los múltiples factores de riesgo existentes en la seguridad de la información.
- La conexión remota a la red de área local del Fondo Adaptación debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

4.11 Política de establecimiento, uso y protección de claves de acceso

El objetivo de esta política es controlar el acceso a la información.

- Se debe concientizar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.
- Los usuarios deben tener en cuenta los siguientes aspectos:
    - No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
    - El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
    - Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
    - Se bloqueara el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo sistema informático, en forma consecutiva por cinco veces.
    - La clave de acceso será desbloqueada luego de la solicitud formal al área de Tecnología de Información por parte del responsable de la cuenta.

Las claves o contraseñas deben:

- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Nunca utilice sus contraseñas personales en el entorno laboral.
- Tener mínimo ocho caracteres alfanuméricos y caracteres especiales.
- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Cambiarse obligatoriamente cada 40 días, o cuando lo establezca el Área de Tecnología de Información.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.

- No ser reveladas a ninguna persona, incluyendo al personal del Área de Tecnología de Información.
- No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

4.12 Política de uso de discos de red o carpetas virtuales

El objetivo de esta política es asegurar la operación correcta y segura de discos de red o carpetas virtuales.

- Para que los usuarios tengan acceso a la información ubicada en los discos de red, el jefe inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, a la mesa de ayuda del Área de Tecnología de Información del Fondo Adaptación. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
- La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a las carpetas de Google Drive o a los discos de red por ser información institucional.
- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
- Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tabletas, celulares inteligentes, etc. o en los discos de red.
- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
- Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
- La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo del Área de Tecnología de la Información.
- La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones del Fondo Adaptación, estará a cargo del Área de Tecnología de la Información.

4.13 Política de uso de puntos de red de datos (red de área local – LAN)

El objetivo de esta política es asegurar la correcta y segura operación de los puntos de red.

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales o equipos de contratistas debidamente autorizados.

- Los equipos de visitantes, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y redes WIFI definidos por el Área de Tecnología de Información de la entidad.
- La instalación, activación y gestión de los puntos de red es responsabilidad del Área de Tecnología de Información.

4.14 Política de uso de impresoras y del servicio de impresión

El objetivo de esta política es asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

- Cada usuario del servicio de impresión le será asignado un PIN o clave para que pueda hacer uso del servicio. Es responsabilidad del usuario mantener en forma secreta este código.
- Cada usuario le será asignada una cuota de impresión que consiste en un número de impresiones, escaneos y copias al mes. Es responsabilidad del usuario administrar debidamente su cuota. El Equipo de Trabajo de Gestión Servicios será el encargado de administrar las cuotas de los usuarios.
- Los documentos que se impriman en las impresoras del Fondo Adaptación deben ser de carácter institucional.
- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Equipo de Trabajo de Gestión Servicios o al área de Tecnología de Información.
- Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

4.15 Política de Seguridad Física

El objetivo de esta política consiste en implementar un programa de seguridad física para el acceso a las instalaciones, centros de datos y centros de cableado que permita fortalecer la integridad, disponibilidad e integridad de la información.

- El Equipo de Trabajo de Gestión Servicios debe implementar un sistema de seguridad física para las instalaciones del Fondo Adaptación.
- El Equipo de Trabajo de Gestión Servicios y el Área de Tecnología de Información deben implementar barreras y sistemas de control de acceso a las instalaciones, centros de datos y centros de cableado del Fondo Adaptación, así como la asignación de niveles de acceso.

- El Equipo de Trabajo de Gestión Servicios debe mantener actualizado el programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las barreras de seguridad (Perimetrales e internas) de las instalaciones pertenecientes a la Entidad.
- El Equipo de Trabajo de Gestión Servicios, implementará y mantendrá en operación sistemas de control de incendio, así como planes integrales a las instalaciones para prevenir inundaciones o humedad en los centros de datos y centros de cableado.
- El Área de Tecnología de Información, deberá implementar protecciones que eviten ó mitiguen daños causados por incendios, inundaciones y otros desastres naturales o generados por el hombre a los centros de datos y centros de cableado.
- No está permitido el uso de equipo fotográfico, de video, de audio u otro dispositivo de grabación de audio o video al interior de los centros de datos, centros de cableados, centros de control.

4.16 Política de Seguridad del centro de datos y centros de cableado

El objetivo de esta política es asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- El Área de Tecnología y Sistemas de la Información deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de un funcionario y/o contratista del Área de Tecnología de la Información del Fondo Adaptación. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
- En las instalaciones del centro de datos o de los centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales inflamables o combustibles que generen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
- El centro de datos debe estar provisto de:
    - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
    - Pisos elaborados con materiales no combustibles.
    - Sistema de refrigeración por aire acondicionado.

  - Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
  - Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el comité de seguridad de la Información y exclusivamente con fines institucionales.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario y/o contratista autorizado del Fondo Adaptación.
- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

4.17 Política de Seguridad de los Equipos

El objetivo de esta política es asegurar la protección de la información en los equipos.

4.17.1 Instalación de equipos de procesamiento y almacenamiento

- Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el Área de Tecnología de Información.

4.17.2 Protecciones en el suministro de energía

- A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el área Administrativa. El Área Administrativa del Fondo Adaptación debe implementar sistemas redundantes de alimentación eléctrica, como por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro de un proveedor de energía

4.17.3 Seguridad del cableado

- Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- Deben existir planos que describan las conexiones del cableado.
- El acceso a los centros de cableado (Racks), debe estar protegido.
- El Área de Tecnología de Información establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

4.17.4 Mantenimiento de los Equipos

- El Fondo Adaptación debe mantener contratos de soporte y mantenimiento de los equipos críticos.
- Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
- Los equipos que requieran salir de las instalaciones del Fondo Adaptación para reparación o mantenimiento, deben estar debidamente autorizados por el Fondo Adaptación y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo a los niveles de clasificación de la información pública reservada o información pública clasificada (privada o semiprivada).
- Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos de la entidad, teniendo en cuenta los diferentes riesgos que se pueden presentar al trabajar en un ambiente que no cuenta con las protecciones ofrecidas al interior del Fondo Adaptación.
- Los equipos retirados de la entidad deben ser protegidos, no se deben dejar sin vigilancia en lugares públicos, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos y la conexión con los sistemas de información del Fondo Adaptación debe cumplir con la política de control acceso.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del Área de Tecnología de Información, así mismo debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

4.17.5 Ingreso y retiro de activos de información de terceros.

- El retiro e ingreso de todo activo de información de propiedad de los usuarios del Fondo Adaptación, utilizados para fines laborales o personales, se realizará mediante los procedimientos establecidos por el sistema de seguridad física. El Fondo Adaptación no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica del Departamento.
- El retiro e ingreso de todo activo de información de los visitantes que presten servicios al Fondo Adaptación (consultores, pasantes, visitantes, etc.) será registrado e inspeccionado en los controles de accesos de las instalaciones de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.
- El traslado entre dependencias del Fondo Adaptación de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

4.17.6 Normas de protección

- Los funcionarios que hagan uso de los equipos del Fondo Adaptación, no deben dejar desatendidos los equipos de cómputo en sitios públicos y deben transportarlos en lugares visibles bajo medidas que le provean seguridad física.
- Siempre deben asegurarse con la guaya que se brinda con el equipo para evitar el hurto del mismo.
- Los computadores portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos, y prevenir la perdida y/o hurto.

4.18 Política de Escritorio y pantalla limpia

El objetivo de esta política es definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

- El personal del Fondo Adaptación debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El personal del Fondo Adaptación debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información y comunicaciones del Fondo Adaptación deberán cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Los usuarios a los que el Fondo Adaptación les asigne equipos móviles como computadores, teléfonos inteligentes, tabletas, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.

- Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.
- La información pública reservada o información pública clasificada (privada o semiprivada) que se encuentre en medio físico, debe permanecer almacenada en una caja fuerte o gabinete de seguridad.

4.19 Política de adquisición, desarrollo y mantenimiento de sistemas de información

El objetivo de esta política es garantizar que la seguridad es parte integral de los sistemas de información de la entidad.

- Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de seguridad de la información.
- En caso de desarrollos propios el Área de Tecnología de Información debe separar los ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
- El Área de Tecnología de Información deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
- El Área de Tecnología de Información desarrollará y/o adquirirá el software requerido por el Fondo Adaptación; de manera coordinada con el Área que manifieste la necesidad del software, el Área de Tecnología de Información establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.
- Se debe verificar que los desarrollos de la entidad estén completamente documentados, igualmente todas las versiones de los desarrollos se deben preservar adecuadamente en varios medios y guardar copia de respaldo externa a la entidad.
- Desarrollar estrategias para analizar la seguridad en los sistemas de información, como no usar datos sensibles en ambientes de prueba y usar diferentes perfiles para pruebas y producción.
- Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica del Fondo Adaptación, por cualquier dependencia o proyecto del Fondo Adaptación, deberá ser gestionado por el Área de Tecnología de Información para su correcto funcionamiento.
- La compra de una licencia de un programa permitirá al Fondo Adaptación realizar una copia de seguridad, para ser utilizada en caso de que el medio se averíe.

- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- El Área de Tecnología de Información será la única dependencia autorizada para realizar copia de seguridad del software original.
- La instalación del software en los activos informáticos del Fondo Adaptación, se realizará únicamente a través del Área de Tecnología de Información.
- El Área de Tecnología de Información implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información del Fondo Adaptación.
- El software proporcionado por el Fondo Adaptación no puede ser copiado o suministrado a terceros.
- En los equipos del Fondo Adaptación solo se podrá utilizar el software licenciado por el Área de Tecnología de Información y el adquirido o licenciado por los proyectos o programas que se encuentran en el Fondo Adaptación.
- Para la adquisición y actualización de software, es necesario efectuar la solicitud al Área de Tecnología de Información con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
- El software que se adquiera a través de proyectos o programas, debe quedar licenciado a nombre del Fondo Adaptación.
- Se debe establecer los lineamientos para la supervisión y seguimiento a las actividades de desarrollo contratado, los cuales deben quedar inmersos en las clausulas y/o especificaciones técnicas de los contratos a ejecutar por el Fondo Adaptación.
- Se encuentra prohibido el uso e instalación de juegos en los computadores del Fondo Adaptación.
- Se presentarán para dar de baja el software de acuerdo con los lineamientos dados por la Entidad.
- El Área de Tecnología de Información debe implementar actividades para la protección contra códigos maliciosos y de reparación.
- El Área de Tecnología de Información debe implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo de software seguro, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
- El Área de Tecnología de Información debe implementar y aplicar metodologías que permitan proteger las transacciones de los servicios de aplicaciones del Fondo Adaptación.
- Se debe implementar el procedimiento de control de cambios de los sistemas de información del Fondo Adaptación, basados en el ciclo de vida, asegurando la integridad desde las primeras etapas de diseño, pasando por mantenimiento.

4.20 Política de respaldo y restauración de información

El objetivo de esta política es proporcionar los medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

- La información de cada sistema debe ser respaldada sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, etc.
- Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación); de igual manera el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
- Las copias de respaldo se guardaran únicamente con el objetivo de restaurar el sistema luego de la infección de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
- Debe ser desarrollado un plan de emergencia para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
- Semanalmente los administradores de infraestructura del Fondo Adaptación, verificarán la correcta ejecución de los procesos de respaldo.
- El Área de Tecnología de Información debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del Fondo Adaptación.

4.21 Política para la realización de copias en los computadores de usuario final

El objetivo de esta política es asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

- De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación a la Entidad pública correspondiente, en este caso al Fondo Adaptación, son de propiedad de ésta con las excepciones que la misma ley han señalado.

- En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Talento Humano, el Área de Tecnología de Información generará una copia de la información contenida en el equipo asignado al perfil del usuario (C:\usuarios\nombre-usuario), a una unidad de almacenamiento.
- Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, debe realizar solicitud al Área de Tecnología de Información, quien escalará la solicitud ante el comité de seguridad de la Información, quien evaluara la pertinencia de la copia.
- Se debe seguir el procedimiento de Borrado Seguro para equipos Final, a fin de garantizar la copia de la información para la entidad y la eliminación de la información almacenada en el disco local.
- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB.
- En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar a la mesa de ayuda del Área de Tecnología de Información y en caso de requerirse copia de la información, ésta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.
- Ningún usuario debe utilizar equipo diferente al asignado para copiar algún tipo de archivo, excepto al autorizado por jefe inmediato.
- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales como Google Drive para la optimización del uso de los recursos de almacenamiento que entrega el Fondo Adaptación a los usuarios.

4.22 Política de seguridad de las comunicaciones

El objetivo de esta política es implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento del Fondo Adaptación.

- El Área de Tecnología de Información debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red del Fondo Adaptación.
- El Área de Tecnología de Información debe crear los estándares técnicos de configuración de la Red del Fondo Adaptación y configuración de seguridad y de dispositivos de seguridad.
- El Área de Tecnología de Información debe implementar sistemas de protección entre las redes del Fondo Adaptación y las redes externas no administradas por la entidad.
- El Área de Tecnología de Información debe identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.
- El Área de Tecnología de Información debe segmentar la red, de modo que permita separar los grupos de servicios de información.

4.23 Política para la transferencia de Información

El objetivo de esta política es proteger la información transferida al interior y exterior del Fondo Adaptación.

- El Área de Tecnología de Información debe implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior del Fondo Adaptación, contra interceptación, copiado, modificación, enrutado y destrucción.
- El Área de Tecnología de Información, deberá controlar las acciones para reenvío automático de correo electrónico a direcciones de correo externo.
- Los funcionarios del Fondo Adaptación que traten temas o información clasificada como información pública reservada o información pública clasificada (privada o semiprivada), lo deberán hacer en lugares seguros y/o por medios de comunicación seguros.
- Se debe establecer el procedimiento para la transferencia de información en medios físicos a nivel interno, externo del Fondo Adaptación y a terceros.

4.24 Política de uso del correo electrónico

El objetivo de esta política es definir las pautas generales para asegurar una adecuada protección de la información del Fondo Adaptación, en el servicio y uso del servicio de correo electrónico por parte de los usuarios autorizados.

- Los funcionarios del Fondo Adaptación deberán hacer uso del correo electrónico institucional suministrado por el Área de Tecnología de Información, para desarrollar las actividades oficiales inherentes al cargo asignado.
- EL correo electrónico que usa la entidad es el correo Gmail, del proveedor de servicios en la nube Google y para ello tiene un dominio oficial fondoadaptacion.gov.co.
- La cuenta de correo oficial para el cumplimiento de las funciones desempeñadas para el Fondo Adaptación, es la cuenta de correo electrónico institucional suministrado por el Área de Tecnología de Información.
- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC del Fondo Adaptación se consideran bajo el control de la entidad.
- El servicio de correo electrónico debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el Fondo Adaptación y no debe utilizarse para ningún otro fin.
- No está autorizado el envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red.

- No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.
- Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire del Fondo Adaptación, su cuenta de correo será desactivada.
- Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo las áreas de Recursos Humanos y de Contratación son las responsables de solicitar la modificación o cancelación de las cuentas electrónicas al Área de Tecnología de Información del Fondo Adaptación.
- Las cuentas de correo electrónico son propiedad del Fondo Adaptación, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal de planta, en comisión permanente, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Entidad y no debe utilizarse para ningún otro fin.
- Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por el Fondo Adaptación.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta soportetecnologia@fondoadaptacion.gov.co con la frase "correo sospechoso" en el asunto.
- El único servicio de correo electrónico autorizado en la entidad es el asignado por el Área de Tecnología de Información.
- En el momento de retiro de un funcionario, además de la desactivación de su cuenta, se hará un respaldo de la cuenta de correo y quedará almacenada en el medio físico de almacenamiento que tenga dispuesto el área de TI. Esta acción se ejecuta en el momento que el área de Recursos Humanos de la entidad envía la notificación de retiro del Funcionario.

4.25 Políticas específicas para funcionarios y contratistas del Área de Tecnología y Sistemas de la Información.

El objetivo de esta política es definir las pautas generales para asegurar una adecuada protección de la información del Fondo Adaptación por parte de los funcionarios y contratistas de TI de la entidad.

- El personal del Área de Tecnología de la Información no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Jefe del Área de Tecnología y de la Información.

- Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnología de la Información son de uso personal e intransferible.
- El personal del Área de Tecnología de la Información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Jefe del Área de Tecnología de Información o el Asesor para la de Seguridad de la Información.
- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Ej: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- Los funcionarios del Área de Tecnología de Información no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe del Área de Tecnología de Información y el registro en el sistema de la mesa de ayuda.
- Los funcionarios del Área de Tecnología de Información se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- Los funcionarios del Área de Tecnología de Información no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
- La copia de programas o documentación, requiere tener la aprobación escrita del Fondo Adaptación y del proveedor si éste lo exige.
- El personal del Área de Tecnología de Información debe velar por que se cumpla con el registro en la bitácora de acceso a los centros de datos o de cableado, de las personas que ingresen y que hayan sido autorizadas previamente por la jefatura del área o por quien ésta delegue.
- Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de seguridad de la Información.
- Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información, deben ser aprobados oficialmente

por la entidad, a través del Comité de seguridad de la Información y deben ser asegurados mediante controles que permitan la preservación de la seguridad de la información.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
- Las pruebas de laboratorio o piloto deben ser autorizadas por el Comité de Seguridad de la Información, para sistemas de información, de software tipo freeware o shareware o de sistemas que necesiten conexión a internet; estas deben ser realizadas sin conexión a la red LAN de la entidad y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

4.26 Política de Tercerización u Outsourcing.

El objetivo de esta política es mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

- Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
- Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información del Fondo Adaptación, las cuales deben ser divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.
- En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.
- Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por el Fondo Adaptación.
- El Área de Tecnología de la Información deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información del Fondo Adaptación.
- Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.
- Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas al Fondo Adaptación. El resultado del análisis de riesgos será la base para el establecimiento de los

controles y debe ser presentado al Comité de seguridad de la Información antes de iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.

- Los funcionarios del Fondo Adaptación que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.
- Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

4.27 Política de Gestión de los Incidentes de la Seguridad de la Información

El objetivo de esta política es asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas.

- El Fondo Adaptación establecerá responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar su repetición, así mismo debe escalar los incidentes de acuerdo con la criticidad del mismo.
- El único canal acreditado para reportar incidentes de seguridad ante las autoridades y el pronunciamiento oficial ante entidades externas del Fondo Adaptación es la Secretaria General o el funcionario que esta delegue.
- El Fondo Adaptación designa al CSIRT de Gobierno (Computer Security Incident Response) Equipo de respuesta a incidentes de seguridad informática del Gobierno y al Área de Tecnología de Información para responder a los eventos o incidentes de seguridad de la información; debe generarse el procedimiento de respuesta.
- El CSIRT de Gobierno (Computer Security Incident Response) Equipo de respuesta a incidentes de seguridad informática debe establecer el procedimiento para la recolección de evidencia, siguiendo los lineamientos jurídicos vigentes en Colombia y estándares internacionales.

4.28 Política para la Gestión de la Continuidad de Seguridad de la Información

El objetivo de esta política es asegurar la continuidad de la seguridad de la información en situaciones de crisis o desastres.

- El Fondo Adaptación establecerá el Plan de Continuidad del Negocio para la entidad, este debe incluir el plan de recuperación de desastres.

- Se debe generar el plan de continuidad de seguridad de la información, documentado e implementando procesos y procedimientos para asegurar la continuidad requerida por la Entidad.
- El Área de Tecnología de Información elaborará el plan de recuperación de desastres para los sistemas de información y comunicación del Fondo Adaptación, el cual debe incluir mínimo procedimientos, condiciones de seguridad, recuperación y retorno a la normalidad.
- El plan de continuidad del negocio de la entidad se debe verificar, revisar y evaluar, por la Oficina de Control Interno durante el desarrollo del plan anual de auditorías.
- El Fondo Adaptación propenderá por la implementación de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad necesarios para la Entidad, así como programación y ejecución de pruebas de funcionalidad de esta.
- El Área de Tecnología de Información debe analizar y establecer los requerimientos mínimos de redundancia para los sistemas de información críticos del Fondo Adaptación junto con la plataforma tecnológica que los soporta, de igual forma deberá investigar, evaluar y probar las soluciones de tecnología que supla la necesidad de la Entidad.

4.29 Políticas específicas para usuarios del Fondo Adaptación

Definir las pautas generales para asegurar una adecuada protección de la información del Fondo Adaptación por parte de los usuarios de la entidad.

El Fondo Adaptación suministra la herramienta de Google Drive para el almacenamiento de la información que crea importante. Así mismo podrá almacenar la información en la carpeta de Mis Documentos del sistema operativo. Sobre estas dos ubicaciones se hará copia de seguridad diaria para garantizar la disponibilidad de la información ante una falla del equipo de cómputo.

- El Fondo Adaptación instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización del Fondo Adaptación (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que ésta práctica no está autorizada.
- Todo el software usado en la plataforma tecnológica del Fondo Adaptación debe tener su respectiva licencia y acorde con los derechos de autor.
- El Fondo Adaptación no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.
- El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son

susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal e individual del Comité de Seguridad de la Información.

- Los programas instalados en los equipos, son de propiedad del Fondo Adaptación, la copia no autorizada de programas o de su documentación, implica una violación a la política general del Fondo Adaptación. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por el Fondo Adaptación o las sanciones que especifique la ley.
- El Fondo Adaptación se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la entidad. Se incluirá valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.
- Los recursos tecnológicos y de software asignados a los funcionarios del Fondo Adaptación son responsabilidad de cada funcionario.
- Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información institucional, de acuerdo con la guía de clasificación de la información.
- Los usuarios solo tendrán acceso a los datos y recursos autorizados por el Fondo Adaptación, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
- Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.
- Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.
- Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente al Área de Tecnología de la Información del Fondo Adaptación o al CSIRT Gobierno (Computer Security Incident Response) Equipo de respuesta a incidentes de seguridad informática.
- Los jefes de las diferentes áreas del Fondo Adaptación, en conjunto con el comité de seguridad de la Información propiciarán actividades para concienciar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial cuando se hace una llamada telefónica, que pueda ser interceptada mediante acceso físico a la línea o al auricular o ser escuchada por personas que se encuentren cerca. Lo anterior debe aplicar también cuando el funcionario, contratista o colaborador se encuentre en sitios públicos como restaurantes, transporte público, ascensores, etc.
- Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.

4.30 Política de uso de mensajería instantánea y redes sociales.

El objetivo de esta política es definir las pautas generales para asegurar una adecuada protección de la información del Fondo Adaptación, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

- El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
- No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador del Fondo Adaptación, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
- Toda información distribuida en las redes sociales que sean originadas por la entidad deben ser autorizadas por el área de Comunicaciones y por los jefes de área para ser socializadas y con un vocabulario institucional.
- No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

5 PROCESO DISCIPLINARIO

Dentro de la estrategia de seguridad de la información del Fondo Adaptación, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores del Fondo Adaptación violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de Gestión Disciplinaria.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por el Fondo Adaptación:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al Comité de Seguridad o al Área de Tecnología de Información.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, "documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)".
- No guardar la información digital, producto del procesamiento de la información perteneciente al Fondo Adaptación.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas al Fondo Adaptación, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.

- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de Tecnología de Información del Fondo Adaptación.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización Área de Tecnología de Información del Fondo Adaptación.
- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por el Fondo Adaptación o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias del Fondo Adaptación.
- No cumplir con las actividades designadas para la protección de los activos de información del Fondo Adaptación.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca al Fondo Adaptación o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de Fondo Adaptación, sin la debida autorización.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos del Fondo Adaptación para beneficio personal.
- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad del Fondo Adaptación.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones del Fondo Adaptación, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información del Fondo Adaptación.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica del Fondo Adaptación.
- El que viole datos personales de las bases de datos del Fondo Adaptación.

- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por el Fondo Adaptación.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información del Fondo Adaptación o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos del Fondo Adaptación a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador del Fondo Adaptación o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por el Fondo Adaptación.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones del Fondo Adaptación, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento del Fondo Adaptación, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen del Fondo Adaptación o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica del Fondo Adaptación.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de Tecnología de Información del Fondo Adaptación.
- Copiar sin autorización los programas del Fondo Adaptación, o violar los derechos de autor o acuerdos de licenciamiento.

6 CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, personal en comisión permanente, contratistas y otros colaboradores del Fondo Adaptación. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, el Fondo Adaptación tomará las acciones disciplinarias y legales correspondientes. El Manual de la Política de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

7 CONTROLES

El Manual de la Política de Seguridad de la Información del Fondo Adaptación esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología del Fondo Adaptación pueden consultar los procedimientos a través del Área de Tecnología de Información.

8 MARCO LEGAL Y REQUISITOS

MARCO LEGAL

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional"
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea"
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- CONPES 3701 de 2011 Lineamientos de Política para Ciber-seguridad y Ciber-defensa
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.

REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad.