El emprendimiento es de todos

Minhacienda

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Impulsando el desarrollo sostenible del país,
a través de la adaptación al cambio climático

5-GOS-P-01. Versión 4.0, marzo de 2021

Fondo Adaptación

Equipo Directivo 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

ILIANA MARGARITA GARZÓN
Subgerente de Regiones

DIANA PATRICIA BERNAL PINZÓN
Secretaria General

VICTOR ALEJANDRO VENEGAS MENDOZA
Jefe Oficina Asesora de Planeación y Cumplimiento

Investigación y textos:

EQUIPO DE TRABAJO
E. T. de Tecnología de Información

Política de Seguridad de la Información.
Versión 4.0 marzo de 2021, Bogotá D.C.

CONTROL DE CAMBIOS Y NOMENCLATURA

VERSIÓN	FECHA	DESCRIPCIÓN
1	2014/12	Documento Inicial
2	2017/12	Complemento de las políticas que aplican al proceso de Gestión de Tecnología de acuerdo con la norma NTC/ISO 27001:2013.
3	2019/03	Revisión y aprobación de las políticas por parte del Comité de Gestión y Desempeño de la entidad
4	2021/03	Revisión y ajustes conforme a la estrategia de Transformación Digital para Todos. Aprobación por parte del Comité de Gestión y Desempeño de la entidad

Tabla de contenido

INTRODUCCIÓN

La Gerencia del Fondo Adaptación, ha encaminado los esfuerzos al fortalecimiento de la gestión de TI de la entidad, implementando nuevas herramientas y fortaleciendo las existentes, ampliando la capacidad de la infraestructura tecnológica de la entidad, e implementando el modelo de seguridad digital, acatando las recomendaciones y lineamientos establecidos desde el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

En particular y entendiendo la importancia de una gestión segura de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información conforme al Modelo de Seguridad y Privacidad de la Información como marco de trabajo del habilitador transversal de seguridad de la Política de Gobierno Digital, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, dando estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Fondo Adaptación, la protección y salvaguarda de la información busca la disminución del impacto generado sobre sus activos de información, por las situaciones no deseadas que afecten negativamente el logro de los objetivos misionales y estratégicos.

CONCEPTOS BÁSICOS

Los siguientes conceptos corresponden al Modelo de Seguridad y Privacidad de la Información, 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 esta (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.

Activo de información es todo recurso por medio del cual se almacena, procesa, transmite, divulga, comunica, intercambia, presenta y genera la información, de igual manera la información en sí misma es un activo de información solo que esta se vale de algún medio o recurso para su gestión.
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: Efecto de la incertidumbre sobre los objetivos.
Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.
Los objetivos pueden tener diferentes aspectos y categorías (por ejemplo: financieros, salud y seguridad, y metas ambientales) y se pueden aplicar a niveles diferentes (estratégico, en toda la organización, en proyectos, productos y procesos).

A menudo el riesgo está caracterizado por la referencia a los eventos potenciales y las consecuencias o a una combinación de ellos.

Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.[1]

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas:

ISO/IEC 27000 - 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.

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).

Transformación Digital para Todos (TDxT): Es la estrategia del Ministerio de las TIC que busca acompañar a las entidades públicas del orden nacional y territorial para impulsar su nivel de madurez digital a través de la adopción de soluciones tipo y en consecuencia, su capacidad de entregar los servicios del Estado de manera efectiva a los ciudadanos.

https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1542226781163&download=true

1 ROLES Y RESPONSABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN

El Representante por la Alta Dirección del Fondo Adaptación ante el Sistema de Gestión de Seguridad de la Información es el jefe Oficina Asesora de Planeación y Cumplimiento. En sus responsabilidades están:

- Presentar al Comité Institucional de Gestión y Desempeño los cambios y nuevas propuestas de alto impacto a la entidad para su análisis y aprobación.
- Representar y atender al ente certificador cuando se realicen ejercicios de auditoría de tercera parte.
- Liderar la definición de la estrategia institucional en seguridad de la información.
- Realizar la revisión por la Dirección al SGSI al menos una vez al año.
- Presidir las reuniones en donde se traten aspectos estratégico y tácticos relevantes del Sistema de Gestión de Seguridad de la Información.

El **Responsable de Seguridad de la Información** es el líder del Equipo de Trabajo de Tecnología de la Información quien a su vez se apoya en expertos técnicos para la implementación, implantación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información. Este rol tiene las siguientes responsabilidades:

- Velar por la implementación, puesta en marcha y mantenimiento del Sistema de Gestión de Seguridad de la Información.
- Velar por la revisión de la estructura (políticas, procedimientos, instructivos, roles, responsables y responsabilidades) del Sistema de Gestión de Seguridad de la Información.
- Hacer seguimiento al plan de trabajo que permita el logro de los objetivos específicos de seguridad de la información del Fondo
- Presentar los cambios, proyectos e iniciativas del SGSI al representante por la Dirección del Sistema de Gestión de Seguridad de la Información.
- Monitorear y velar por el cumplimiento del Plan Operativo de Seguridad de la Información del Fondo.
- Presentar las necesidades de recursos financieros para el desarrollo de proyectos que fortalezcan la gestión de la seguridad de la información con el fin de lograr los objetivos misionales y estratégicos del Fondo.

El **Líder Técnico de Seguridad de la Información** o también designado como **Oficial de Seguridad de la Información** es aquel profesional o contratista quien implementa y mantiene operativamente el Sistema de Gestión de Seguridad de la Información. En sus responsabilidades están:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a la ejecución del Plan Operativo de Seguridad de la Información las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear e implementar las tareas, fechas y plan de trabajo para el cumplimiento de los objetivos específicos de seguridad de la información del Fondo.
- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades de los colaboradores con responsabilidades críticas en el SGSI y proporcionar apoyo administrativo.
- Planear y ejecutar de los planes de trabajo propuestos del SGSI, bajo un enfoque orientado a riesgos para darle solución oportuna y escalar al responsable de seguridad de la información en caso de ser necesario.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Velar por el mantenimiento documental del SGSI, su custodia y protección.
- Contribuir al enriquecimiento en la gestión del conocimiento en materia de seguridad y privacidad de la información apoyando la documentación de las lecciones aprendidas.
- Participar en las reuniones de seguimiento y velar por la actualización de los indicadores de gestión del SGSI.

Responsables críticos de la seguridad digital: Son funcionarios o colaboradores que por sus funciones gestionan, administran o supervisan activos de información críticos del Fondo. A este rol pertenecen los funcionarios directivos y/o líderes de procesos, los colaboradores de Mesa de Servicios y el responsable de infraestructura y servicios tecnológicos. En sus responsabilidades está:

- Cumplir y velar por el estricto cumplimiento de las políticas de seguridad de la información a título personal y en los colaboradores o equipos de trabajo bajo su cargo.
- Atender los requerimientos de seguridad que les soliciten y en caso de ser requerido escalarlo al líder técnico de seguridad de la información o al responsable de seguridad de la información.
- Participar en las reuniones de seguridad de la información cuando sean convocados.
- Brindar y poner a disposición sus conocimientos, habilidades y capacidades en la resolución de problemas e incidentes de seguridad de la información y de seguridad digital.

Responsables de la seguridad de la información en el Fondo Adaptación: Son responsables por la seguridad de la información todos los funcionarios y colaboradores vinculados o que son partes interesadas del Fondo Adaptación. Deben cumplir con las políticas de seguridad de la información y cuando identifiquen algún posible riesgo de seguridad de la información deben notificarlo a la mesa de servicios o al responsable de seguridad de la información o al oficial de seguridad de la información.

2 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Fondo Adaptación protege, custodia y preserva la información gestionada en sus procesos, mediante una adecuada gestión de riesgos de seguridad y privacidad de la información (incluyen los de seguridad digital) que permitan el adecuado acceso, procesamiento, transporte, intercambio, almacenamiento, presentación, comunicación y divulgación de la información, logrando los niveles de confidencialidad, disponibilidad e integridad requeridos para dar cumplimiento a los requisitos legales y reglamentarios y, a las necesidades del cliente interno y externo. La protección, custodia y preservación de la información respalda los objetivos misionales y estratégicos del Fondo, por lo tanto, es responsabilidad de los funcionarios, colaboradores, contratistas, proveedores y partes interesadas dar cumplimiento y hacer cumplir la presente política.

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, contratistas, practicantes y clientes del Fondo Adaptación.

2.1 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.

2.2 Alcance/Aplicabilidad de la política para la gestión de seguridad de la información

- Esta política aplica a todos los activos de información, a todos los procesos del FONDO ADAPTACIÓN y también a sus partes interesadas internas y externas en el cumplimiento de los objetivos misionales y estratégicos.

3 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 de la entidad, 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 funcionarios, contratistas o terceros.
- El Fondo Adaptación protegerá la información accedida, procesada, transportada, almacenada, presentada, comunicada y divulgada por los procesos, con el fin de minimizar los impactos negativos de detrimento y de tipo financiero, legal, operativo o reputacional como consecuencia de incidentes de seguridad de la información para lo cual se implementarán controles como mecanismos de tratamiento del correspondiente riesgo.
- El Fondo Adaptación protegerá su información de las amenazas originadas por parte del personal.
- El Fondo Adaptación implementa controles para la protección de las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos.
- El Fondo Adaptación implementa los controles para cumplir con los niveles requeridos por esta, para la seguridad de los recursos tecnológicos y la red de datos.
- El Fondo Adaptación implementa controles de acceso a la información, sistemas y recursos de red.
- El Fondo Adaptación integra la seguridad de la información al ciclo de vida de los sistemas de información.
- El Fondo Adaptación implementa la mejora continua de la seguridad y privacidad de la información a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas.
- 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.

La presente política debe ser revisada y actualizada anualmente o cuando el Líder de Seguridad de la Información lo determine, teniendo como criterios los cambios relevantes en el contexto interno y externo, cuando la identificación de nuevos riesgos de seguridad de la información lo requiera o cuando el marco legal que regula las políticas nacionales en materia de Seguridad de la Información, Seguridad Digital o Gobierno Digital lo demanden.

4 LINEAMIENTOS OPERACIONALES O ESPECÍFICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Estos lineamientos 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

El Artículo 2.2.22.3.8 Comités institucionales de gestión y desempeño del Decreto 1499 de 2017 establece "En cada una de las entidades se integrará un Comité Institucional de Gestión y Desempeño encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG, … Los Comités Institucionales de Gestión y Desempeño cumplirán las siguientes funciones: … 6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.", por lo tanto, el Comité Institucional de Gestión y Desempeño del Fondo Adaptación o a quien este delegue tiene bajo su responsabilidad asegurar la implementación y desarrollo de la política de seguridad digital y de la información. El proceso de Gestión de Operación y Soporte implementa y mantiene con el apoyo de las partes interesadas el Sistema de Gestión de Seguridad de la Información y apoya en la organización de la información con respecto a dicho sistema de gestión.

4.2 Lineamiento para uso de dispositivos móviles y teletrabajo[2]

Por medio de este lineamiento 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.

Así mismo se establecen lineamientos bajo las situaciones de las modalidades de trabajo en casa y teletrabajo.

- Los dispositivos móviles provistos por el Fondo Adaptación (teléfonos móviles, teléfonos inteligentes y, tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones y las actividades de los colaboradores de la entidad en el ejercicio de sus funciones o de sus obligaciones contractuales.
- Los dispositivos móviles asignados por el Fondo Adaptación deben tener la configuración realizada por el E. T. 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).

[2] El título de este numeral lleva la palabra teletrabajo para dar conformidad al nombre del objetivo de **control A.6.2 Dispositivos móviles y teletrabajo**, del Anexo A de la norma NTC-ISO 27001:2013 y lo establecido en el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de las TIC.

- 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 a la mesa de servicios quienes evaluarán si se escala o no la solicitud al Oficial de Seguridad o al líder del E. T. de Tecnologías de la Información.
- Todo acceso remoto a los recursos de la red corporativa del Fondo Adaptación, deben ser por medio de VPN debidamente solicitadas por el jefe inmediato o supervisor del contrato y autorizadas por el E. T. de Tecnología de Información.
- Todo acceso autorizado por VPN debe tener un periodo determinado con una fecha de inicio posterior a la vinculación a la entidad (laboral o contractual) y una fecha de expiración de los permisos de acceso.
- Todo correo enviado desde una cuenta institucional debe llevar la firma del remitente para su identificación. En caso de gestionar el correo desde equipos que no son propiedad del Fondo, se debe configurar la firma institucional para su uso.
- Toda información gestionada por el Fondo Adaptación y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con el Fondo.
- No se debe acceder remotamente a los recursos de la red corporativa del Fondo Adaptación desde equipos que no cuenten con antivirus actualizado y funcionando, o que no cuenten con las actualizaciones de seguridad del sistema operativo o que sea de uso público (café Internet, por ejemplo) o que se sospeche que no es seguro.
- Cuando se acceda remotamente a la información del Fondo Adaptación se debe cumplir con las políticas de pantalla limpia (aplica para el trabajo desde casa).

4.3 Lineamiento 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 para atender y cumplir 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 pérdida de integridad, confidencialidad y/o disponibilidad de la información o de los activos de información.
- Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación al Fondo Adaptación para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012, 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 Lineamiento de Gestión de Activos de Información

Estos lineamientos 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.

Todo activo de información debe ser identificado, clasificado y tenido en cuenta para la gestión de riesgos de seguridad de la información y de seguridad digital.

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 con 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).
- Custodios de activos de información: son responsables de la cadena de custodia la cual se apoya en la aplicación de controles para la protección de la información según su nivel de clasificación y el recurso en donde esta se almacene.

4.5 Lineamiento de Uso de Activos de Información

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

- Los activos de información pertenecen al Fondo Adaptación y el uso de estos debe emplearse exclusivamente con propósitos laborales.
- Los usuarios deberán utilizar únicamente los recursos tecnológicos autorizados por el E. T. 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 copia de 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 con las normas sobre clasificación de la información de acuerdo con 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 E. T. 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 E. T. de Tecnología de Información.
- Estarán bajo custodia del E. T. 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 E. T. 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 Equipo de Trabajo 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, enrutador, wifi público, etc.), esto compromete la seguridad de los recursos informáticos del Fondo Adaptación.
- El E. T. 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 E. T. 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 lograr su custodia y confidencialidad y pueda ser recuperada en caso de desastre o de incidentes catastróficos y con los equipos de procesamiento que tenga predefinido el E. T. de Tecnología de la Información.
- 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 Lineamiento de uso de estaciones cliente

El objetivo de este lineamiento 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 proceso de Gestión de arquitectura de TI, el 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 de forma permanente información pública reservada y pública clasificada en dichos equipos y por lo tanto esta información se debe almacenar en los espacios de almacenamiento definidos por el E. T. de Tecnología de Información y así mismo realizar el borrado seguro de dicha información cuando se haga la devolución del correspondiente equipo.
- 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 producto de su gestión en el marco del cumplimiento de sus funciones o de sus obligaciones contractuales.
- En el Disco C:\ de los equipos -equipos de escritorio y/o portátiles- asignados a los colaboradores (usuarios) se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.
- Los usuarios podrán trabajar sus archivos de gestión en los equipos -equipos de escritorio y/o portátiles- que les fueron asignados 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.
- El préstamo de recursos tecnológicos como equipos de cómputo, computadores portátiles, etc., se debe hacer a través de la mesa de ayuda de TI con anticipación y se proveerá de acuerdo con 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; el Fondo Adaptación no se hace responsable por pérdida o daño de los recursos tecnológicos como equipos portátiles, dispositivos móviles, etc., de uso personal o de terceros.

- El E. T. de Tecnología de la Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no sean propiedad del Fondo Adaptación.

4.7 Lineamiento de seguridad de equipos de propiedad de contratistas

Por medio de este lineamiento se dictan los lineamientos para el uso de equipos de propiedad de contratistas que hacen uso de los recursos y servicios tecnológicos del Fondo Adaptación.

- Antes de conectar por primera vez equipos o dispositivos a la red LAN corporativa se debe solicitar su autorización de conexión al E. T. de Tecnología de Información para el debido análisis, aprobación o no y registro en la base de datos de control de equipos de terceros que usan la infraestructura tecnológica de la entidad.
- Todo activo de información como los equipos de escritorio, equipos portátiles, dispositivos móviles, equipos servidores, equipos de comunicaciones (switches, enrutadores, firewalls.) y demás equipos de cómputo o almacenamiento electrónico, debe ser identificado y etiquetado de acuerdo con los criterios establecidos en la guía 5 "Guía para la gestión y clasificación de activos de información". Para los equipos que no son propiedad del Fondo Adaptación y es requerida su conexión a la red corporativa se debe informar al propietario los requisitos requeridos en el equipo para su incorporación a la red corporativa y el acceso a sus recursos.
- Todo equipo o dispositivo conectado a la red corporativa del Fondo Adaptación debe tener actualizado y con licencia legal:

    - Antivirus
    - Sistema operativo y mecanismo de actualizaciones automáticas de seguridad
    - Suite ofimática
    - Cliente VPN provista por Fondo Adaptación (en caso de requerirse)

- Todo propietario de equipos conectados a la red corporativa del Fondo Adaptación y que no son propiedad de la entidad, debe cumplir con las políticas de seguridad y privacidad de la información y utilizar los mecanismos de control de acceso lógico y físico dispuestos para tal fin. Estás políticas de operación incluyen entre otras el uso de los puntos de la red de datos, el uso de impresoras y su servicio de impresión, el uso de internet y la gestión de usuarios del Fondo Adaptación.
- El Fondo Adaptación no presta el servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no son de su propiedad o que no están bajo su responsabilidad legal.
- 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, daño3 o hurto de equipos, dispositivos móviles o elementos/componentes tecnológicos que no son

[3] Daño hace referencia al mal funcionamiento o disfuncionalidad total de algún componente del equipo portátil o dispositivo móvil o elemento/componente tecnológico. Estos daños pueden ser causados por sobre carga eléctrica, por virus o secuestro informático, caída de elementos pesados sobre el equipo, dispositivo o elemento, o por otras causas.

de su propiedad o que no están bajo su responsabilidad legal y que se encuentren en las instalaciones de la entidad.

- El Fondo Adaptación no hace respaldo a equipos que no son de su propiedad o que no están bajo su responsabilidad legal. En caso de requerirse extracción de información en equipos que no son propiedad del Fondo Adaptación se debe realizar la solicitud de dicho servicio a E. T. de Tecnología de Información, quienes evaluarán la viabilidad, la pertinencia y 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 deben utilizar la cuenta de usuario del directorio activo del Fondo Adaptación que se le asigne, 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, es personal e intransferible.
- Está prohibido la instalación de software propiedad del Fondo Adaptación en equipos que no son propiedad o que no están bajo su responsabilidad legal de la entidad. Sólo se podrá instalar software del Fondo siempre y cuando el contrato con la entidad así lo estipule.
- El E. T. 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 Lineamiento 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 debe visitar y/o navegar en sitios o portales web 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 de los responsables técnicos en seguridad de la información del E. T. de Tecnología de la Información.
- El E. T. de Tecnología de Información otorgará o no la autorización de navegación a los usuarios del Fondo Adaptación, previa solicitud del jefe de la dependencia.
- El E. T. 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 Lineamiento de disposición de información, medios y equipos

El objetivo de este lineamiento 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 E. T. de Tecnología de Información.

4.10 Lineamiento de control de acceso

El objetivo de este lineamiento 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 Fondo Adaptación proporciona a los funcionarios todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo salvo autorización dada por el E. T. de Tecnología de Información, no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes y/o access point.
- 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 E. T. 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 malicioso.

- Todo trabajo para 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 líder del E. T. de Tecnología de Información del Fondo Adaptación.
- El E. T. 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 Lineamiento de establecimiento, uso y protección de claves de acceso

El objetivo de este lineamiento es definir los criterios y usos aceptables de claves de acceso.

- 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 por el 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 y contraseñas son personales e intransferibles.
- El cambio de contraseña debe ser solicitado solamente por el titular de la cuenta o su jefe inmediato.
- A partir del quinto intento consecutivo sin éxito de inicio de sesión, se bloquea la cuenta de usuario.
- 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 mecanismos de almacenamiento de terceros ni de los exploradores web.
    - Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
    - La clave de acceso será desbloqueada luego de la solicitud formal al E. T. 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 90 días, o cuando lo establezca el E. T. 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 E. T. 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 Lineamientos de uso de discos de red o carpetas virtuales

El objetivo de este lineamiento 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 o supervisor deberá enviar un correo autorizando el acceso y permisos correspondientes al usuario para el cumplimiento de sus funciones u obligaciones contractuales según corresponda, a la mesa de ayuda del E. T. 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, tablets, celulares inteligentes, etc. o en los discos de red que sean propiedad del Fondo Adaptación o suministrado por este para el desarrollo de las funciones u obligaciones contractuales.
- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo suministradas por el Fondo Adaptación, sin expresa autorización de su jefe inmediato o supervisor.

- 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 E. T. 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 E. T. de Tecnología de la Información.

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

El objetivo de este lineamiento 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 E. T. de Tecnología de Información de la entidad.
- La instalación, activación y gestión de los puntos de red es responsabilidad del E. T. de Tecnología de Información.

4.14 Lineamiento de uso de impresoras y del servicio de impresión

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

- A cada usuario del servicio de impresión se le asigna un PIN o clave para que pueda hacer uso del servicio. Este PIN es personal e intransferible.
- A cada usuario se le será asigna un número de impresiones, digitalizaciones y copias al mes. Es responsabilidad del usuario administrar debidamente el servicio asignado. El Equipo de Trabajo de Gestión Servicios será el encargado de administrar el servicio de impresoras de los usuarios.
- Los documentos que se impriman en las impresoras del Fondo Adaptación deben ser para el cumplimiento de las funciones laborales o de las obligaciones contractuales.
- 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 E. T. 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 Lineamiento de seguridad física

El objetivo de este lineamiento 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 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, debe mantener en operación los 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 E. T. de Tecnología de Información, deberá implementar protecciones que eviten o 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 o centros de control.

4.16 Lineamiento de seguridad del centro de datos y centros de cableado

El objetivo de este lineamiento 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 de quienes ingresen, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- El E. T. de Tecnología e Información implementa y mantiene los mecanismos de contingencia y recuperación de los centros de datos y demás instalaciones de almacenamiento o procesamiento de datos, para atender situaciones que interrumpan la provisión de los recursos y servicios de TIC que respaldan los procesos y actividades críticas en el cumplimiento de los objetivos misionales del Fondo.
- La limpieza y aseo del centro de datos está a cargo del Área Administrativa y debe efectuarse en presencia de un funcionario y/o contratista del E. T. 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, dichas actividades son prohibidas; 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 inflamables.
    - 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 los responsables 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 y la puerta cerrada.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

4.17 Lineamientos de Seguridad de los Equipos

El objetivo de este lineamiento es asegurar la protección de la información en los equipos. 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 E. T. de Tecnología de Información.
- Los equipos dispuestos a ser alojados en áreas seguras deben cumplir con los requisitos de alistamiento definidos por el E. T. de Tecnología de Información, como lo es un sistema operativo con las actualizaciones de seguridad vigentes, el antivirus o mecanismo de protección contra virus, la instalación de software con licenciamiento legal.
- Protecciones en el suministro de energía

- A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores y los monitores o 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 interrupción del suministro del proveedor de energía

Seguridad del cableado

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

Mantenimiento de los Equipos

- El Fondo Adaptación debe mantener contratos de soporte y mantenimiento de los equipos críticos y las garantías de los equipos de escritorio, portátiles y dispositivos móviles que son propiedad del Fondo.
- 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 atendiendo la debida programación y autorización por parte del E. T. de Tecnología de Información.
- 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 encuentre información clasificada de acuerdo con los niveles de clasificación de la información pública reservada o información pública clasificada (privada o semiprivada).
- Para que los equipos se puedan sacar fuera de las instalaciones del Fondo, 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 E. T. 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.

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 de las instalaciones de la entidad.
- 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.
- Normas de protección
- Los funcionarios o colaboradores 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 este.
- 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 Lineamiento de escritorio y pantalla limpia

El objetivo de este lineamiento 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 reservada o clasificada gestionada por la entidad y 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 sesión de usuario 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, tablets, 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 Lineamiento de adquisición, desarrollo y mantenimiento de sistemas de información

El objetivo de este lineamiento es garantizar que la seguridad es parte integral de los sistemas de información de la entidad.

- Incluir en los sistemas de información o aplicativos informáticos, controles de seguridad y permitan el cumplimiento con las políticas de seguridad de la información.
- En caso de desarrollos propios, el E. T. de Tecnología de Información debe separar los ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
- El E. T. de Tecnología de Información debe 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 y despliegue en el ambiente de producción.
- El E. T. de Tecnología de Información desarrolla y/o adquiere el software requerido por el Fondo Adaptación; de manera coordinada con el proceso que manifieste la necesidad del software, el E. T. de Tecnología de Información establecen y definen los requerimientos funcionales y no funcionales para la adquisición o desarrollo de la correspondiente solución tecnológica. En los requerimientos no funcionales se deben incluir los 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 E. T. 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.
- Salvo autorización expresa y escrita por el Fondo, 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 E. T. 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 E. T. de Tecnología de Información.
- El E. T. 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 E. T. 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 E. T. 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 cláusulas 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 presenta para dar de baja el software de acuerdo con los lineamientos dados por la Entidad.
- El E. T. de Tecnología de Información debe implementar actividades para la protección contra códigos maliciosos y de reparación.
- El E. T. 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 E. T. 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 Lineamiento de respaldo y restauración de información

El objetivo de este lineamiento 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, o sistemas remotos de almacenamiento en centros de datos de terceros contratados para tal fin.
- 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 guardan 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 o por requerimiento legal.
- 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 compartidas remotas o en los espacios de almacenamiento en la nube destinados 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 copias de respaldo.
- El E. T. 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 Lineamiento para la realización de copias en los computadores de usuario final

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

- De acuerdo con 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 E. T. de Talento Humano, el E. T. 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 se requiere información gestionada por un funcionario o colaborador retirado se debe solicitar a Mesa de Servicios quien escalará al Líder del E. T. de Tecnología de Información y al líder del proceso al que pertenecía el funcionario o colaborador retirado quienes autorizarán o no la entrega de dicha información.
- Se debe seguir el procedimiento de Borrado Seguro para equipos devueltos a almacén o para dar de baja, 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 E. T. 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 Lineamiento de seguridad de las comunicaciones

El objetivo de este lineamiento 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 E. T. de Tecnología de Información debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red del Fondo Adaptación.
- La configuración de la red corporativa del Fondo Adaptación y la configuración de los dispositivos/equipos de seguridad deben atender los estándares técnicos establecidos por el E. T. de Tecnología de Información.
- El E. T. 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 E. T. 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 E. T. de Tecnología de Información debe segmentar la red, de modo que permita separar los grupos de servicios de información.

4.23 Lineamiento para la transferencia de Información

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

- Toda transferencia de información al interior y exterior del Fondo Adaptación debe protegerse contra interceptación, copiado, modificación, enrutado y destrucción.
- Todo reenvío automático de correos electrónicos institucionales a buzones externos con la finalidad de copia de respaldo, debe ser autorizado por el jefe inmediato o supervisor y por el E. T. de Tecnología de Información.
- Los funcionarios del Fondo Adaptación que traten temas cuya información es pública reservada o pública clasificada (privada o semiprivada), deben cuidar de mantener tanto la confidencialidad como el manejo de la custodia de dicha información.

4.24 Política de uso del correo electrónico

El objetivo de este lineamiento 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 y colaboradores del Fondo Adaptación deben hacer uso del correo electrónico institucional suministrado por el E. T. de Tecnología de Información, para el desarrollo de las actividades oficiales inherentes al cargo asignado o de las actividades que permitan el cumplimiento de sus obligaciones contractuales, según corresponda.
- El correo electrónico institucional es el provisto por el E. T. de Tecnología de Información y solo desde este se debe gestionar toda comunicación del Fondo Adaptación, así mismo el E. T. de Tecnología de Información es el responsable de los aliados estratégicos para la determinación de la plataforma del servicio de correo electrónico, plataforma colaborativa y sitio web institucional.
- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información que gestiona el Fondo.
- Los servicios de correo electrónico corporativo se emplean para atender el cumplimiento de los objetivos misionales, estratégicos y las actividades de apoyo de la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC del Fondo Adaptación se consideran propiedad 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 dichas cuentas al E. T. 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 o contractual 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 con 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 E. T. de Tecnología de Información.
- En el momento de retiro de un funcionario, se debe desactivar la cuenta se desactivará, se realiza copia de respaldo de la cuenta de correo; dichas copias de respaldo se custodian en donde se defina y disponga por el E. T. de Tecnología de Información. Esta acción se ejecuta en el momento que el E. T. de Recursos Humanos de la entidad envía la notificación de retiro del funcionario o cuando los supervisores de contratos notifiquen de la terminación anticipada de un contratista.
- Toda terminación anticipada de contratos en el Fondo Adaptación debe ser informada al E. T. de Tecnología de Información para realizar las correspondientes actividades de retiro y desactivación de cuentas de usuario.

4.25 Lineamientos específicos para funcionarios y contratistas del E. T. de Tecnología y Sistemas de la Información

El objetivo de este lineamiento 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 E. T. 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 E. T. de Tecnología y de la Información.
- Los usuarios y claves de los administradores de sistemas y del personal del E. T. de Tecnología de la Información son de uso personal e intransferible.
- El personal del E. T. 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 E. T. 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 con el software disponible en la entidad. Por 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 E. T. de Tecnología de Información no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del jefe del E. T. de Tecnología de Información y el registro en el sistema de la mesa de ayuda.
- Los funcionarios del E. T. 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 E. T. 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 E. T. 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 Lineamiento de tercerización u outsourcing

El objetivo de este lineamiento 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 E. T. 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, evaluar, tratar y monitorear los riesgos relacionados con los contratistas o proveedores en relación con los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.
- Se deben identificar, evaluar, tratar 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 deben 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 Lineamiento de Gestión de Incidentes de Seguridad de la Información

El objetivo de este lineamiento 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 establece 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 de este.
- 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 E. T. de Tecnología de Información para responder a los eventos o incidentes de seguridad de la información; debe generarse el procedimiento de respuesta.
- El CSIRTde 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 Lineamiento de gestión de continuidad de seguridad de la información

El objetivo de este lineamiento 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.
- El E. T. 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 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 E. T. 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 Lineamientos específicos 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 instala 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 tienen 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 E. T. 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 los responsables de la 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 Lineamiento de uso de mensajería instantánea y redes sociales.

El objetivo de este lineamiento 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 están 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 debe ser autorizadas por el E. T. 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 E. T. 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 E. T. de Tecnología de Información del Fondo Adaptación.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización E. T. 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 E. T. 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 está 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 E. T. de Tecnología de Información.

8 Marco Legal y Requisitos

8.1 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 Ciberseguridad y Ciberdefensa
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.

8.2 Requisitos técnicos

- Modelo de Seguridad y Privacidad de la Información – MinTIC.
- 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.
-