POLÍTICAS Y PROCEDIMIENTOS INTERNOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

	Nombre	Cargo	Firma
Revisó	Luis Germán Botero Ortiz	Director Administrativo y Financiero	
Aprobó	Natalia Arango	de Comité de Calidad	

FONDO PARA LA ACCIÓN AMBIENTAL Y LA NIÑEZ-FONDO ACCIÓN

POLÍTICAS Y PROCEDIMIENTOS INTERNOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO **Pág.**

Presentación

El **Fondo Acción** es una Fundación sin ánimo de lucro constituida bajo las leyes colombianas. En cumplimiento a lo dispuesto en la Ley 1581 de 2012 *"Por la cual se dictan disposiciones legales para la protección de Datos Personales"* y sus normas reglamentarias, se ha incorporado la presente Política y procedimientos internos en materia de Seguridad de la Información.

Con la promulgación de la presente Política y Procedimientos internos en materia de Seguridad de la Información, el **Fondo Acción** formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar su integridad, confidencialidad y disponibilidad, conforme a las disposiciones sobre protección de datos vigentes.

1. Seguridad de la Información

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las características de la información tales como: confidencialidad, integridad, disponibilidad, cumpliendo en todo caso, con los parámetros legales, normativos y estatutarios del **Fondo Acción**.

2. Alcance

La presente Política y procedimientos internos de seguridad de la información, aplica a todos los funcionarios en todos los niveles de **Fondo Acción**. Aplica a todas las bases de datos y archivos de información personal que estén en poder de **Fondo Acción** y que este dentro del marco contextual de la Ley 1581 de 2012 y sus normas reglamentarias.

3. Objetivos

Proteger, preservar y administrar la información del **Fondo Acción**, así como de las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad de la información.

4. Responsabilidad

La Política y procedimientos Internos de Seguridad de la Información es de aplicación obligatoria para todo el personal del **Fondo Acción**, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

La Coordinación de Sistemas, con apoyo de la Dirección Jurídica del **Fondo Acción**, serán los responsables de revisar, actualizar y aprobar el texto de la presente Política.

La Coordinación de Sistemas será el área responsable de impulsar la implementación y cumplimiento de la presente Política, así como de desempeñar funciones relativas a la seguridad de los sistemas de información de la entidad.

La Coordinación de Sistemas deberá seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología del **Fondo Acción**.

La dirección Jurídica cumplirá la función de notificar a todo el personal que se vincula contractualmente con el **Fondo Acción** de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, así como de los cambios que en ella se produzcan. Así mismo tendrá como funciones la de verificar el cumplimiento de la presente Política en la gestión de todos los contratos del **Fondo Acción** con empleados y con terceros y de asesorar en materia legal a la organización en lo que se refiere a la seguridad de la información.

El personal del **Fondo Acción** que hace uso de la información y de la plataforma tecnológica para su procesamiento, son responsables de conocer y cumplir la presente Política de Seguridad de la Información.

5. Seguridad de la información con respecto al Recurso Humano del Fondo Acción

El **Fondo Acción** protege la información que recopila, en una base de datos segura. En el almacenamiento de la información hemos tomado una serie de medidas para proteger la información, de uso indebido, pérdida, acceso no autorizado, modificación o divulgación no autorizada. El **Fondo Acción** emplea firewalls, sistemas de detección de intrusos y herramientas de detección de virus para proteger los datos.

Así mismo, los empleados del **Fondo Acción** requieren como condición de su empleo el manejo confidencial de toda la información en poder del **Fondo Acción**, y para mantener la confidencialidad de esa información. También se les asigna nombres de usuario y contraseñas para acceder a los aplicativos y unidades de almacenamiento de datos del **Fondo Acción**.

La administración de los usuarios es de responsabilidad de la Coordinación de Sistemas, novedades de inclusión, aplicación de privilegios y eliminación de usuarios está contenida en esta responsabilidad.

6. Seguridad Física y del entorno

6.1 Acceso

El acceso físico a las oficinas del **Fondo Acción** está controlado, las redes inalámbricas no permiten acceder a la red local, el personal ajeno a la organización no puede conectarse a la LAN; si por alguna razón es necesario el Coordinador de Sistemas supervisa esta operación.

Otro nivel controlado de acceso es el cuarto de Tics al cual solo accede el Coordinador de Sistemas.

Accesos remotos no son permitidos de afuera hacia adentro y en caso de ser necesario este tipo de conexión, el Coordinador de Sistemas también supervisa esta operación.

6.2 Seguridad en los equipos

El **Fondo Acción** provee la infraestructura necesaria para que opere de manera segura en cuanto a nivel de fluido eléctrico, ambiente propio, acceso físico y virtual no permitidos. El cableado estructurado está totalmente supervisado. Los servidores que contienen la información y servicios son mantenidos de manera preventiva y correctiva a nivel de hardware y software. Adicionalmente se cuenta con: a) detección de incendio y sistemas de extinción de conflagraciones, b) bajo riesgo de inundación, c) pólizas de seguros de equipos que cubre siniestros, d) sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Los equipos individuales asignados al personal del **Fondo Acción** deben estar correctamente instalados y operados por personal de la organización quienes son capacitados para operarlos, así mismo, en cuanto al contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados y protegidos de forma correcta de acuerdo a los estándares que para tal efecto la Coordinación de Sistemas de Información contemple.

Existe una política para la creación y el manejo de copias de seguridad que hace parte del Sistema de Gestión de la Calidad, denominada: DA-MA-06 Plan de Contingencia y Políticas de Backus SGC.

7. Administración de las comunicaciones y operaciones

7.1 Reporte e investigación de incidentes de seguridad

El personal del **Fondo Acción** debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a la información a la Coordinación de Sistemas.

7.2. Protección contra software malicioso y hacking.

Como control mínimo, los equipos individuales de trabajo del **Fondo Acción** deben estar protegidos por software Antivirus, Spywares, Malware con capacidad de actualización. Los usuarios de la estación no están autorizados a deshabilitar este control ni a instalar software no autorizado ni legal.

7.3 Intercambio de Información con Organizaciones Externas.

Toda la información institucional debe ser manejada de acuerdo a la legislación vigente sobre la materia (Ley 1581 de 2012 y normas reglamentarias)

7.4 Internet y Correo Electrónico

El uso de Internet y de los servicios de correo electrónico debe garantizar el cumplimiento del Código de Ética del **Fondo Acción** y el manejo responsable de los recursos de tecnologías de la información.

7.5 Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas del **Fondo Acción,** deben ser aprobadas por la Coordinación de Sistemas. No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de Autor.

8. Control de Acceso

8.1 Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales debe estar restringido según los perfiles de usuario definidos por la Coordinación de Sistemas, para tal efecto el **Fondo Acción** cuenta con el documento denominado DA-MA-07 POLITICAS DE USO DE LOS ESPACIOS COMPARTIDOS DEL SERVIDOR Y FORMATO, que hace parte del Sistema de Gestión de la Calidad.

8.2 Control de Claves y Nombres de Usuario

Así mismo, los empleados del **Fondo Acción** requieren como condición de su empleo el manejo confidencial de toda la información para el tratamiento de datos personales en poder del **Fondo Acción,** y para mantener la confidencialidad de esa información personal. También están obligados a utilizar nombres de usuario y contraseñas al acceder a los sistemas del **Fondo Acción**.

Como requisito para la terminación de relación contractual -o laboral- del personal del **Fondo Acción,** la Coordinación de Sistemas debe cancelar las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la organización.

9. Adquisición, Desarrollo y Mantenimiento de Sistemas Software

Para apoyar los procesos operativos y estratégicos, el **Fondo Acción** hace uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

10. Cumplimiento

Todo uso y seguimiento de uso a los recursos de TI en el **Fondo Acción** debe estar de acuerdo a las normas y estatutos internos, así como a la legislación nacional en la materia.