FODESEP
FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR

RESOLUCIÓN No. 006 D E 2010
(26 DE AGOSTO DE 2010)

"Por medio de la cual se adoptan las Políticas de uso Responsable de las Tecnologías de la Información y las Comunicaciones -TICs- del Fondo de Desarrollo de la Educación Superior "FODESEP"

LA GERENTE GENERAL DEL FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR - FODESEP,

En uso de sus facultades legales y estatutarias, especialmente la prevista en los literales "a" e "i" del artículo 49 de los Estatutos del Fondo y particularmente en las disposiciones del Decreto 1158 de 2008, y

CONSIDERANDO:

Que dentro de las funciones que debe desarrollar el representante legal y jefe de la administración de FODESEP, el Gerente General tiene, entre otras, la obligación de cumplir y hacer cumplir la ley, los estatutos y los reglamentos; así como administrar los bienes de FODESEP.

Que teniendo como norte estratégico las fases de Gobierno en línea surge la necesidad de desarrollar los lineamientos que establezca las políticas de uso responsable de las tecnologías, y con ello proteger la propiedad intelectual de los sistemas de información y la plataforma tecnológica de FODESEP.

Que es compromiso de todo el personal que labora en FODESEP, direccionar a la entidad a la consolidación de una plataforma tecnológica con información confiable, integral, oportuna y de calidad que permita la toma de decisiones en todas las áreas, para así lograr tener control y propender por una viabilidad sostenible en un corto tiempo en todas las dependencias con procesos de una alta calidad y eficiencia.

Que en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Adoptar las Políticas de uso Responsable de las Tecnologías de la Información y las Comunicaciones -TICs- del Fondo de Desarrollo de la Educación Superior –FODESEP-, las cuales forman parte integral de la presente resolución, como instrumento de organización de la gestión del Fondo.

ARTÍCULO SEGUNDO: La aplicación de las Políticas de uso Responsable de las Tecnologías de la Información y las Comunicaciones -TICs-, estará a cargo de cada una de los empleados, contratistas o cualquier persona que haga uso de las mismas dentro del Fondo de Desarrollo de la Educación Superior, FODESEP.

ARTÍCULO TERCERO: La divulgación de las Políticas de uso Responsable de las Tecnologías de la Información y las Comunicaciones -TICs- estará a cargo de la Secretaría General, con el apoyo del Profesional 3 Tecnología.

ARTÍCULO CUARTO: El seguimiento a las Políticas de uso Responsable de las Tecnologías de la Información y las Comunicaciones -TICs- estará bajo la responsabilidad de cada una de las áreas de FODESEP, con la asesoría y el acompañamiento de Control Interno.

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

ARTÍCULO QUINTO: La presente Resolución rige a partir de su expedición.

Dada en Bogotá, D.C., a los veinticinco (25) días del mes de agosto de dos mil diez (2010).

COMUNÍQUESE Y CÚMPLASE,

EULALIA NOHEMI JIMÉNEZ RODRÍGUEZ
Gerente General

Proyectó: Bárbara Alexy Carbonell P., Secretaria General
Revisó y aprobó: José Alejandro Duque Ramírez, Asesor Jurídico

POLÍTICAS DE USO RESPONSABLE DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICs DEL FONDO DE DESARROLLO DE LA EDUCACION SUPERIOR – FODESEP.

INTRODUCCIÓN

La Unidad de Informática teniendo como objetivo principal prestar un servicio eficiente a los clientes internos, y de esta manera lograr un impacto favorable en la atención a los usuarios externos con calidad, define las políticas de uso de las TICs: canales de datos e Internet, hardware y software del Fondo de Desarrollo de la Educación Superior - FODESEP, con normas aplicables y extensivas a los servicios proporcionados por nuestra Entidad.

El compromiso del Fondo de Desarrollo de la Educación Superior - FODESEP es direccionar a nuestra entidad para contar con una plataforma tecnológica con información confiable, integral, oportuna y de calidad que permita la toma de decisiones en todas las áreas, para así lograr tener control y propender por una viabilidad sostenible en un corto tiempo en todas las dependencias con procesos de una alta calidad y eficiencia.

1. PROPOSITO.

Es el propósito de este documento definir la política Institucional respecto del uso responsable de los sistemas de información en el Fondo de Desarrollo de la Educación Superior – FODESEP; es decir, el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad de la información, sistemas de información y recursos tecnológicos Institucionales.

2. ALCANCES.

Esta política se aplicará a todos los empleados, cualquiera sea su jerarquía, a los consultores, contratistas, y a cualquier otra persona que tenga acceso a los sistemas de información de la Institución. También se aplica esta política a todos los equipos y sistemas informáticos (servidores, computadores personales, estaciones de trabajo, elementos de infraestructura tecnológica, bases de datos, sistemas de información que apoyan los procesos administrativos, software, productos de ofimática y correos electrónicos) que se encuentren bajo responsabilidad operacional de la entidad.

Las políticas y estándares de seguridad de información del Fondo aplica también a los recursos informáticos que pertenecen a terceras partes tales como organismos del Estado, personas jurídicas de derecho privado, etc., en aquellos casos en donde exista un deber contractual para proteger los recursos mientras se encuentren en custodia de la entidad.

3. TERMINOS Y DEFINICIONES

Para los propósitos de esta política se aplicarán las siguientes definiciones:

Comunicaciones electrónicas: incluyen todo uso de los sistemas de información para comunicar, publicar material y contenido por medio de servicios como correo electrónico, foros de discusión, páginas html, o alguna herramienta similar.

Exploits: es un método concreto de uso de un error de algún programa (bug) para entrar en un sistema informático. Generalmente, un exploit suele ser un programa que

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

se aprovecha de algún error del sistema operativo, por ejemplo: obtener los privilegios del administrador y así tener un control total sobre el sistema.

Material no permitido: incluye la transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales o internacionales.

Packet Spoofing: es el procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo adoptando otra identidad de remitente para engañar al programa o sistema que protege la red contra intrusos (firewall).

Red Institucional: es el conjunto de recursos de conectividad computacionales que permite la comunicación de datos e información a través de las oficinas incluyendo la Internet.

Redes: incluye cualquier sistema de cableado o equipos físicos como enrutadores, switches, además de varios sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.

Sistemas de información: incluye cualquier sistema o aplicación de software que sea administrado por la Institución y de los cuales ella es responsable, como APOTEOSYS, SICOOP, SCHIP, MUISCA, AURORA, SIMCO PLUS, entre otros, aplicaciones de servidores y escritorio, sistemas operativos y aplicaciones de Internet.

Uso responsable: Es el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad de la información, sistemas de información y recursos tecnológicos Institucionales.

Usuario(s): incluye toda aquella persona no necesariamente vinculada con la Institución, a quien FODESEP proporcione los medios y niveles de autorización y acceso necesarios para hacer uso de los servicios o sistemas de información de ésta (personal de planta, contratistas, etc.).

4. GENERALIDADES.

El Fondo de Desarrollo de la Educación Superior FODESEP, se esmera por facilitar el acceso al personal administrativo, directivo, consultores, contratistas, a fuentes de información nacional e internacional y por proveer un ambiente que fomente la difusión del conocimiento, el proceso de creación y los esfuerzos de colaboración, en el marco de la misión institucional.

El acceso a los sistemas de información del Fondo de Desarrollo de la Educación Superior FODESEP es información privilegiada y privada, por lo cual su trato debe ser de esta manera por todos los usuarios de dichos sistemas. Los usuarios deben actuar honesta y responsablemente. Cada usuario es responsable por la integridad y seguridad de estos recursos y tiene el deber de respetar los derechos de otros usuarios, el apropiado uso de las instalaciones físicas y sus métodos de control, además de respetar toda licencia pertinente y acuerdo contractual que esté relacionado con la plataforma tecnológica de la entidad.

Todos los usuarios deberán actuar de acuerdo con estos lineamientos y las leyes nacionales e internacionales pertinentes. El incumplimiento de esta política puede

resultar en la negación de acceso a los sistemas de información de la Institución o a otras acciones disciplinarias o legales.

FODESEP puede restringir o prohibir el uso de su plataforma tecnológica en cualquier caso en el que se demuestre alguna violación de estas políticas o de alguna disposición normativa.

Los Recursos de Información son activos costosos y el uso no autorizado, alteración, destrucción o revelación de estos activos es un crimen relacionado con la Tecnología de la Información y las Comunicaciones (TICs).

Tratar de burlar los controles de accesos administrativos o de seguridad para los Recursos de Información es una violación de esta política. Asistir a alguien o solicitar a alguien que burle los controles de accesos administrativos o de seguridad es una violación a esta política.

Todos los empleados recibirán una copia de la declaración de las políticas de seguridad en TICs. Cada nuevo empleado recibirá una copia del área de Gestión de Talento Humano.

5. USO PERMITIDO DE LA RED INSTITUCIONAL

- El uso es permitido para asuntos de la Institución y el uso para asuntos personales es restringido. Los sistemas de información de la Institución son primordialmente para uso de asuntos relacionados con la misma. Las TICs no pueden ser usadas para asuntos personales. El uso personal de la plataforma tecnológica para accesar, descargar, transmitir, distribuir o almacenar material obsceno está enteramente prohibido. Bajo ninguna circunstancia el uso personal de estos sistemas por parte de los empleados de la Institución debe influir de manera negativa en el desempeño de las tareas y responsabilidades para con la misma. El uso personal puede ser negado en casos en los que se haga uso excesivo de los recursos de las TICs.

- Se requiere autorización previa y escrita por parte de la Secretaria General del FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR FODESEP para el uso personal o uso contrario a esta política de la Institución. El uso de los recursos de las TICs que tenga como objetivo cualquier tipo de ganancia económica personal para cualquier usuario está totalmente prohibido, con excepción de algún uso especial que sea autorizado formalmente por la Gerencia General.

6. ACCESO A LA RED INSTITUCIONAL Y A SUS SERVICIOS

- Las identificaciones y claves de acceso a la Red Institucional, la Intranet o a cualquier otro Sistema de Información son propiedad de la Entidad. Estas identificaciones y claves son para uso estrictamente personal e intransferible y la responsabilidad de su uso debido recae exclusivamente en el usuario al que se le asignen.

- El acceso no autorizado a los sistemas de información de la Institución está prohibido.

- Nadie debe usar la identificación, identidad o contraseña de otro usuario, y de la misma manera ningún usuario debe dar a conocer su contraseña o identificación a otro, excepto en casos que se requieran para la reparación o el mantenimiento de algún

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

servicio o equipo y en este caso debe dar a conocer estos datos única y exclusivamente a funcionarios de informática de FODESEP.

- Siempre que un usuario termine su relación laboral o contractual con FODESEP, sus identificaciones y contraseñas para todos los sistemas de información serán inactivados inmediatamente.

- Ningún usuario podrá sin permiso escrito de la Entidad, hacer modificaciones a la Red Institucional, la Intranet o a sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la red. Ante cualquier acción de este tipo la Entidad adelantará acciones de carácter administrativo, laboral, penal, civil, o cualquiera que corresponda, según sea el caso.

- En la Red Institucional no está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser previamente consultada con la Unidad de Informática de FODESEP.

- El acceso a Internet en las oficinas de FODESEP, debe hacerse desde una estación debidamente registrada y/o autorizada por la unidad de Informática de FODESEP, es decir, el computador debe estar registrado dentro del DNS (Domain Name Server) primario de FODESEP y estar localizado con una dirección IP legítima.

- Las claves de seguridad deben ser cambiadas periódicamente por el dueño del identificador de usuario (login) por lo menos cada 42 días, tiempo definido por el Directorio Activo del Servidor de Windows.

- El usuario que inicia sesión es responsable de administrar su clave de seguridad y de todas las acciones y funciones realizadas bajo su sesión.

7. USO INDEBIDO DE LAS REDES, LAS COMUNICACIONES ELECTRONICAS Y SISTEMAS DE INFORMACION

El uso indebido de las REDES, las COMUNICACIONES y SISTEMAS DE INFORMACION ESTA PROHIBIDO E INCLUYE:

- Intentar instalar u operar puntos de acceso inalámbricos (access point) conectados a la red cableada de FODESEP sin autorización de la Gerente General.

- Intentar modificar, reubicar o sustraer del lugar donde han sido instalados o configurados equipos de cómputo, software, información o periféricos sin la debida autorización.

- Acceder sin la debida autorización de FODESEP, mediante computadores, software, información o redes de la Institución, a recursos externos o internos que pertenezcan a FODESEP (bases de datos, sistemas de información, etc.).

- Interferir sin autorización el acceso de otros usuarios a los recursos de los sistemas de información de la Entidad.

- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.

- Utilizar los sistemas de información para propósitos ilegales o no autorizados.

- Enviar cualquier comunicación electrónica fraudulenta.

- Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente sin la autorización escrita del propietario del software.

- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.

- Usar las comunicaciones para acosar o amenazar a los usuarios de la Institución o externos, de alguna manera que sin razón interfiera con el desempeño de los empleados.

- Usar las comunicaciones para revelar información privada sin el permiso explícito del dueño.

- Leer la información o archivos de otros usuarios sin su expreso permiso.

- Alterar o falsificar de manera fraudulenta los registros de la Entidad (incluyendo registros computarizados, permisos, documentos de identificación, u otros documentos o propiedades.)

- Usar las comunicaciones para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.

- Usar las comunicaciones para apropiarse de los documentos de otros usuarios.

- Lanzar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva.

- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Entidad.

- Transportar o almacenar material con derechos de propiedad o material nocivo usando las redes de la Entidad.

- Utilizar cualquier sistema de información de la Institución para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno.

- Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.

- Instalar o usar software de espionaje, monitoreo de tráfico o programas maliciosos en la Red Institucional.

- Introducir cualquier tipo de programas o instalar cualquier software sin la autorización por escrito de la Gerente General de FODESEP.

- Efectuar violaciones a la seguridad o interrupciones de la comunicación de la red.

- Las violaciones de la seguridad incluyen "sniffer", "floodeos", "packet spoofing", negación del servicio (DOS), manipulación de ruteo, etc.

- Monitorear o escanear puertos de servidores o switches, a menos que se cuente con la autorización necesaria de la representante legal de FODESEP.

- Evitar o interceptar la autenticación de cualquier usuario por cualquier método.

- Usar cualquier método (exploits, scripts, comandos) para acceder a recursos a los que no se tiene acceso a áreas protegidas.

- La información confidencial debe ser accesada solo por el personal que ha sido autorizado sobre la base estricta de "necesidad de conocer" en la realización de sus actividades. Los datos que contengan información confidencial deben ser identificados y tratados como confidenciales en su totalidad.

- Todas las estaciones de trabajo y computadoras de usuario final deben tener instalado software de protección contra virus.

- Todas las áreas de procesamiento de información usadas para mantener Recursos de Información deben ser protegidas con controles físicos apropiados de acuerdo con el tamaño y complejidad de las operaciones y de la criticidad y sensibilidad de los sistemas que operan en ellas. El acceso físico a estas áreas debe ser restringido y solo permitir el acceso a personal autorizado.

8. PRIVACIDAD

La privacidad de los usuarios no está garantizada. Cuando los sistemas de información de la Entidad funcionan correctamente, un usuario puede considerar que sus datos generados son información privada, a menos que él mismo realice alguna acción para revelarlos a otros. Los usuarios deben estar conscientes que ningún sistema de información es completamente seguro, por lo cual personas dentro y fuera de la institución pueden encontrar formas de tener acceso a la información. DE ACUERDO CON ESTO, LA ENTIDAD NO PUEDE, Y NO GARANTIZA LA PRIVACIDAD DE LOS USUARIOS.

Reparación y mantenimiento de equipos. El personal de soporte técnico tiene la autoridad para acceder a archivos individuales o datos cada vez que deban realizar mantenimiento, reparación o chequeo de equipos de computación. Sin embargo el personal de soporte técnico de sistemas no puede exceder su autoridad en ninguna de estas eventualidades para usar esta información con propósitos diferentes al de mantenimiento y reparación.

Respuesta al uso indebido de computadores y sistemas de información. Cuando por alguna causa razonable determinada por la Unidad de Informática de FODESEP, se sospeche de algún tipo de uso indebido como se describe en la sección siete (7) de este documento, la Representante Legal de FODESEP, o quien ella designe, puede acceder a cualquier cuenta, datos, archivos, o servicio de información perteneciente a los involucrados en el incidente, para investigar y de acuerdo con los hallazgos o evidencias dar traslado a la Secretaria General de FODESEP, para que de acuerdo con el marco de su actuación, reglamentos, normas y políticas institucionales, inicien los procesos y apliquen las sanciones respectivas, de ser el caso. Los empleados de la Unidad de Informática están en la obligación de monitorear constantemente los sistemas de información de la Institución a través de los medios correspondientes para responder oportunamente a cualquier acción que atente contra la integridad, disponibilidad, seguridad y desempeño correcto de los mismos mediante la negación,

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

restricción de acceso a usuarios o sistemas, aislamiento y desconexión de equipos o servicios.

9. INSTALACION Y USO DE SOFTWARE.

De acuerdo con las normas locales e internacionales relativas a los derechos de propiedad intelectual, el único software que será instalado en el computador del usuario será aquel que previamente haya sido estandarizado y/o autorizado por la Entidad y para lo cual ésta dispone de las licencias respectivas a su nombre.

Todo usuario está obligado a conocer el alcance de uso de cada una de las licencias de software a su disposición por esta razón la información estará disponible en la oficina de sistemas de FODESEP. De esta manera el usuario conoce lo que le es permitido y prohibido en cuanto al uso del software y será responsable ante la Institución y/o ante terceros del uso que haga del mismo.

El usuario no deberá participar en la copia, distribución, transmisión o cualquier otra práctica no autorizada en las licencias de uso de software.

No es permitida la instalación de software de "dominio público" o de "distribución libre" (Shareware y Freeware) sin la debida autorización de la unidad de informática de FODESEP.

Toda instalación, desinstalación o traslado de software (incluyendo aquellos de "dominio público" o de "distribución libre) desde y hacia un equipo Institucional requiere autorización y coordinación previa con la unidad de informática de FODESEP.

Cualquier software que se haya instalado en un equipo Institucional que no cumpla con lo estipulado anteriormente, será desinstalado sin que ello derive ninguna responsabilidad para la Institución.

Al usar una licencia de software que ha sido instalado en un equipo Institucional o en un equipo personal, el usuario reconoce los derechos de la Institución anteriormente descritos y es consciente de ellos.

10. CORREO ELECTRÓNICO

El correo electrónico se provee a los empleados dentro de la organización como parte de los recursos de tecnología que ofrece el Fondo. El propósito del correo electrónico es que sirva de la manera más conveniente para la comunicación entre los propios empleados y con los clientes externos. No es práctica del Fondo el estar monitoreando el contenido de los mensajes de correo electrónico. Sin embargo, la información del correo electrónico institucional puede estar sujeta a divulgación bajo diferentes circunstancias, como por ejemplo: revisiones de auditoría, investigaciones legales, etc.

Todas las políticas incluidas en este documento son aplicables al correo electrónico Institucional. El correo electrónico debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los destinatarios colectivos y los foros de discusión. Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.

Los mensajes de correo electrónico institucional (dominio fodesep@fodesep.gov.co) deben ser borrados una vez que la información contenida en ellos ya no sea de utilidad.

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

Participar en una cadena de correos es una violación seria de las Políticas de Uso Aceptable; en el entendido que debido a la facilidad de propagación del correo electrónico, estas cadenas se ha n convertido en mensajes masivos. Los mensajes de cadena buscan coaccionar o convencer de varias maneras a sus lectores de que dicha cadena sea reenviada a otro grupo de usuarios de correo electrónico. El nombre de "cadena" proviene del encadenamiento de pasajes que hacen estos mensajes de usuario a usuario.

En ningún caso es permitido suplantar cuentas de usuarios ajenos.

11. PAGINAS WEB Y SISTEMA DE MANEJO DE CONTENIDO

La unidad de informática de FODESEP, acogiendo la directriz organizacional, determinará los estándares para aquellos contenidos considerados como oficiales de la Institución. Ninguna otra página o contenido electrónico puede hacer uso de los logos de FODESEP sin la debida autorización de la Representante Legal. Los editores de las páginas Web que usen información asociada con FODESEP deben acogerse a las políticas de la Institución, a la ley que las regula incluyendo derechos de autor, leyes sobre obscenidad, calumnia, difamación y piratería de software. El contenido debe ser revisado periódicamente para asegurar continuamente su veracidad.

12. MANEJO DE LOS DATOS Y LA INFORMACIÓN

Dueños de la Información: Las unidades administrativas son los directamente responsables de la creación y mantenimiento de los datos.

Responsabilidades de los Dueños de Información: El dueño de la información es responsable de:

- Propender por la calidad de los datos gestionados por sus áreas.
- Determinar cómo debe ser usada la información.
- Realizar los Backups de su propia información.

Responsabilidades de los Custodios de Información: El custodio de datos es la unidad asignada para proveer servicios asociados a los datos. El custodio es:

- El centro de Servicios de Información y Computación que soporta las aplicaciones administrativas y de producción.
- El gerente u operador de un centro de procesamiento de datos, servidor o red de computadoras y/o estaciones de trabajo.
- El usuario final de una estación de trabajo (terminal o microcomputadora).

Responsabilidades de los Usuarios de los Datos: El usuario de los datos es la persona a la que se le ha concedido autorización explícita para acceder a los datos por parte del dueño de la información. El usuario debe:

- Utilizar los datos solo para los propósitos especificados por el dueño de la misma.
- Acatar las medidas de seguridad especificadas por el dueño de la información o custodio.
- No revelar la información sobre los datos o controles de acceso sobre los mismos a menos que sea autorizada de manera específica y por escrito por parte del dueño de la información.

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

APÉNDICE "A" - ADMINISTRACIÓN DE CLAVES DE SEGURIDAD:

La información manejada por los sistemas computacionales debe ser protegida adecuadamente contra modificación, divulgación o destrucción no autorizada. Controles efectivos para el acceso lógico a los Recursos de Información minimiza los errores accidentales cometidos por los empleados y la negligencia, y reduce las oportunidades de los crímenes por computadora. Cada usuario de un proceso automatizado de misión crítica le es asignado un único identificador personal para identificación de usuario. La identificación de usuarios es autenticada antes que el sistema conceda acceso a la información automatizada.

Selección de Claves de Seguridad: Las claves de seguridad son usadas para autenticar la identidad de un usuario y establecer responsabilidad. Una clave de seguridad que es fácil de adivinar es una clave de seguridad inadecuada que compromete la seguridad y responsabilidad de las acciones ejecutadas por el identificador de usuario que lo representa.

Cualquier clave de seguridad que alguien pueda adivinar no es una buena selección. Las claves de seguridad más populares son: Su nombre, el nombre del esposo o esposa(o), novio o novia. Claves de seguridad no apropiadas son aquellos nombres que se deletrean de atrás hacia delante o que están seguidos de un dígito. Entre más corta la clave de seguridad más fácil de adivinar. Otras claves no apropiadas son los números telefónicos, nombres de celebridades y escritores famosos, nombres de películas de cine, nombres de tiendas y almacenes, bebidas favoritas o gente famosa.

Algunas reglas para seleccionar una buena clave de seguridad son:

- Uso de mayúsculas y minúsculas si el sistema computacional encuentra una diferencia entre las mayúsculas y las minúsculas.
- Incluir dígitos y caracteres de puntuación así como letras.
- Seleccione algo que le sea fácil de recordar para que no tenga que escribirlo.
- Use por lo menos 8 caracteres. La seguridad en la clave de seguridad se incrementa a medida que esta es más extensa.
- Debe ser fácil de digitar rápidamente.
- Use dos palabras cortas y combínelas con un carácter especial.
- Utilice un acrónimo que tenga un especial significado para usted, como **TLQTDEM** (**T**odo **L**o **Q**ue **T**u **D**igas **E**s **M**entira).
- Cambiar la clave cada 42 días.

Manejo de Claves de Seguridad: Una advertencia generalizada es "nunca escriba una clave de seguridad". Nunca escriba la clave en el calendario del escritorio, o en una etiqueta autoadhesiva, o dentro de la gaveta de su escritorio.

Si usted necesita escribir una clave de seguridad, tenga en cuenta lo siguiente:

- No identifique la clave de seguridad como una clave de seguridad.
- No incluya el nombre de la cuenta o el número telefónico de la computadora en la misma hoja de papel.
- No fije la clave de seguridad a la terminal, teclado o cualquier parte de la computadora o escritorio de trabajo.
- Mezcle o cifre caracteres adicionales a la versión escrita de la clave de seguridad de una manera que usted la recuerde, pero haga la versión escrita diferente a la clave de seguridad real.

- Nunca guarde su clave de seguridad en línea y nunca envíe una clave de seguridad a otra persona a través del correo electrónico.

APÉNDICE "B" - SEGURIDAD PERSONAL Y SENSIBILIZACIÓN DE SEGURIDAD

La gente es el activo más importante dentro de una organización, y de ellos depende el mantener un nivel de seguridad efectivo. Al mismo tiempo las personas representan la mayor amenaza a la seguridad de la información. Un programa de seguridad no puede ser efectivo si no se mantiene una conciencia y motivación en los empleados.

Requerimientos de los Empleados: Cada empleado es responsable por la seguridad de los sistemas al grado en que lo requiera la labor que desempeñe en el uso de información y tecnología relacionada. El cumplimiento de las responsabilidades en la seguridad es obligatorio y las violaciones a los requerimientos de seguridad pueden ser causal de acciones disciplinarias incluyendo la destitución, sanciones civiles y sanciones criminales.

Posiciones en Sitios Sensibles o de Responsabilidad o Confianza Especial: Las posiciones o cargos individuales deben ser analizados para determinar las vulnerabilidades potenciales asociadas al trabajo en cada cargo. En algunos casos, será apropiado que algunas áreas de la organización, con la aprobación del departamento de Recursos Humanos, designen el perfil de usuarios para cierto tipo de cargos en donde se requiere confianza y responsabilidad especiales. También es apropiado designar ciertas áreas o localidades como sensibles y requerir procedimientos y seguridad especiales para todos los empleados cuyos deberes incluyen acceso a estas áreas.

Conciencia de Seguridad y Entrenamiento: Un efectivo nivel de sensibilización y entrenamiento es esencial para que un programa de seguridad en información sea viable. Los empleados que no son informados de los riesgos o de las políticas administrativas entorno a la seguridad, probablemente no tendrán en cuenta los pasos a seguir en prevenir una violación de seguridad.

Cada departamento dentro de la organización deberá proveer un programa de sensibilización y entrenamiento en seguridad de la información y en la protección de los Recursos de Información para todo el personal que de una u otra manera entre en contacto con Recursos de Información críticos o sensibles de la organización.

Aceptación de Derechos y Responsabilidades: El personal con acceso a los sistemas de información de la organización aceptan los requerimientos de seguridad del sistema y su responsabilidad para mantener la seguridad de los mismos antes de ganar acceso al sistema. Esta aceptación se hará cuando sea firmada la declaración de responsabilidad de seguridad durante las sesiones de entrenamiento o cuando el departamento de Recursos Humanos lo requiera.

APÉNDICE "C" - RECUPERACIÓN DE DESASTRES

Se requiere que la Unidad de Informática se prepare y anticipe por la pérdida de las capacidades de procesamiento de información. Los planes y acciones para recuperarse de siniestros van desde rutinas de copias de respaldo de datos y software en el evento de siniestros mínimos o interrupciones temporales, hasta planes de recuperación de desastres integrales en caso de pérdidas catastróficas de Recursos de Información.

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

Copias de Respaldo ("*Backup de Datos*") Las copias de respaldo en sitio (*On-site*) son empleadas para tener los datos actuales disponibles en forma legible en máquinas dentro del área de producción en el evento en que los datos operativos se pierdan, destruyan o estén corruptos; y evitar el tener que reingresar los datos desde la fuente original. Las copias de respaldo o de almacenamiento fuera de sitio (Off-site) envuelven el mismo principio pero está diseñada para períodos de protección más largos en un ambiente más controlado, requiere actualizaciones menos frecuentes y provee una protección adicional en contra de amenazas potenciales de destrucción sobre el sitio primario y sus datos.

Debe haber copias de respaldo del software y los datos esenciales para la continuidad de las operaciones de misión crítica. Los controles de seguridad sobre los recursos para las copias de respaldo deben ser tan rigurosos como los exigidos para los recursos del sitio primario.

Copias de Respaldo Alternas: Los procedimientos para copias de respaldo en los diferentes sistemas o plataformas de la organización y los diferentes servidores dentro de la organización están diseñados para protegerse contra pérdidas de datos causadas por fallas en el hardware o cualquier otro desastre. El período y frecuencia de estas copias de respaldo puede que no provea la suficiente protección que cumpla con los requerimientos de los usuarios para las copias de respaldo. Por lo tanto, es recomendable la realización de copias de seguridad adicionales por parte de los usuarios que así lo consideren necesario.

Planes de Contingencia: Los planes de contingencia o planes de control de desastres, especifican acciones que la administración ha aprobado de antemano para cumplir con cada uno de los siguientes objetivos: identificar y responder a desastres; proteger las personas y los sistemas; y minimizar el daño. Los planes de recuperación y respaldo especifican como llevar a cabo los procesos de misión crítica en la ausencia de los recursos que los soportan.

APÉNDICE "D" - CONTROLES EN EL DESARROLLO DE APLICACIONES

El grupo de desarrollo de aplicaciones debe cumplir con la siguiente guía de seguridad.

- Los programas y sistemas deben ejecutar solo las funciones que fueron definidas en los requerimientos del sistema y no pueden interferir con otros sistemas a menos que esto haya sido especificado en los requerimientos.
- Los recursos para desarrollo tales como terminales, estaciones de trabajo, servidores y software de desarrollo solo podrán ser usados en proyectos aprobados.
- Se llevará a cabo una administración de cambios la que incluirá información para cada cambio que identifique como mínimo: quién lo solicita, acción tomada, por quién, fecha, autoridad que aprueba.
- Las modificaciones deben ser aprobadas por el gerente de desarrollo y el gerente de la organización dueño del sistema de aplicación.
- Los cambios no autorizados a los sistemas de producción no son permitidos y son considerados una violación a las políticas de seguridad
- Procedimientos formalmente definidos son requeridos para los planes de pruebas antes de la implementación de cualquier sistema; pruebas de seguridad respecto de la modificación de datos de producción, acceso controlado a los datos, producción y librerías de los programas.
- Los gerentes de proyecto convocarán revisiones al sistema, inspecciones y reuniones de acercamiento de forma periódica para asegurar el cumplimiento a los controles y a las políticas de seguridad.

- Los gerentes de proyecto solicitarán o proveerán entrenamiento efectivo en seguridad a todo el grupo de desarrollo de software.
- Los procedimientos de seguridad, prácticas de trabajo, métodos de programación, estándares, librerías de producción y todos los datos globales de seguridad estarán sujetos a revisión por el CSO (Computer Security Officer) y la Auditoría Interna u Oficina de validación y verificación del Fondo.
- La ejecución de programas que actualizan las bases de datos de producción debe ser realizada por el personal de control de producción y no por los programadores.
- El personal de control de producción debe tener acceso de solo lectura a las librerías de programas de producción y no deben tener acceso a las librerías de código fuente de programas.
- El movimiento de programas a producción debe ser aprobado por los administradores de aplicaciones asignados.
- Todas las solicitudes de requerimiento de cambios y reporte de problemas deben estar diligenciados y con la aprobación de un cliente representativo y autorizado.
- Las nuevas estructuras de Bases de Datos y cambios a bases de datos existentes debe estar aprobada por el DBA (Administrador del Sistema de Bases de Datos) antes que la estructura modificada sea colocada en producción.
- Los gerentes, coordinadores o líderes de proyecto se asegurarán que se han efectuado revisiones sobre todos los nuevos programas o cambios a los programas antes de que estos sean puestos en producción. Todos los reportes sin excepción deben ser revisados y documentados de manera periódica.

APÉNDICE "E" – MANEJO DEL HADWARE

La administración, mantenimiento, modernización y adquisición de equipos de cómputo y de telecomunicaciones debe adoptar los siguientes criterios para proteger la integridad técnica de la institución.

Cambios al Hardware: Los equipos de cómputo de la entidad no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del área de Gestión Tecnológica y estadística.

- Todos los empleados deben reportar los daños o pérdida total o parcial del equipo que tengan a su cuidado de propiedad de la institución. La intervención directa para reparar el equipo está expresamente prohibida. La Entidad debe proporcionar personal interno o externo para la solución del problema reportado.

- Todos los equipos de la entidad se encuentran relacionados en un inventario que incluye la información de sus características, configuración, determinando, su ubicación.

- Los equipos de microcomputadores (PC, servidores, LAN, etc.) no deben moverse o reubicarse sin la aprobación previa del Coordinador de la Unidad de Informática, y el responsable de Talento Humano y Recursos Físicos de FODESEP.

Acceso físico y lógico:

- Los equipos deben estar conectados a la red interna.

- Todos los computadores y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co

- Las bibliotecas de cintas magnéticas, discos y documentos se deben ubicar en un área restringida dentro del centro de cómputo y en sitios alternos con acceso únicamente a personas autorizadas.

- Con la excepción de los equipos de cómputo portátiles y los equipos de telecomunicaciones, se prohíbe el uso de módems que establecen conexiones de marcado directo. Todas las conexiones con los sistemas y redes de la entidad deben ser dirigidas a través de dispositivos probados y aprobados por la Entidad y contar con mecanismos de autenticación de usuario.

- Los equipos de cómputo de FODESEP no pueden ser accedidos por terceros a través de diversos canales, como líneas conmutadas, redes de valor agregado, Internet y otros, de ser requerido deberá ser aprobado por la Unidad de Informática, previo visto bueno del Gerente General del Fondo.

- Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la Entidad será restringido por el Profesional 3 Informática del Fondo.

APÉNDICE "F" - INSTALACIONES FISICAS

Todos los funcionarios de la Entidad deberán seguir los siguientes lineamientos de seguridad física con el fin de salvaguardar los recursos técnicos y humanos de la entidad.

Control de acceso físico: La Entidad cuenta con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes y sistema de alarmas, en las dependencias que la entidad considera críticas.

Personas:

- En el evento que un empleado o contratista de FODESEP termine su vínculo con la Entidad, todos sus códigos de acceso deben ser cambiados o desactivados. Además, en caso de pérdida de la escarapela o tarjeta de acceso también deben desactivarse dichos códigos.

- Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.

- Como mecanismo de prevención, ningún empleado, contratista o visitante puede comer, fumar o beber en el centro de cómputo o instalaciones con equipos tecnológicos. Al hacerlo exponen los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.

- Las reuniones de trabajo donde se discute y maneja información sensible, se deben realizar en salas cerradas para que personas ajenas a ella no tengan acceso.

Equipos y Otros Recursos:

- Toda sede y equipo informático, ya sean propios o de terceros, que procesen información para la entidad o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física que se emitan, con el fin de evitar el acceso a personas no autorizadas a las áreas restringidas donde se procese o mantenga

información secreta, confidencial y privada, y asegurar la protección de los recursos de la plataforma tecnológica y su información.

- No se debe proveer información sobre la ubicación del centro de cómputo, como mecanismo de seguridad.

Protección física de la información:

- Todas las personas que laboren para la Entidad y/o aquellas designadas por otras entidades para desarrollar actividades particulares en FODESEP (consultores y contratistas), son responsables del adecuado uso de la información suministrada para tal fin, por lo cual se debe velar por su integridad, confidencialidad, disponibilidad y auditabilidad. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

- Al terminal la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la institución. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

12. INCUMPLIMIENTO.

FODESEP hará responsable a sus usuarios de la presente Política y las consecuencias que se derivarían de su incumplimiento. Así mismo, los nuevos usuarios deberán conocer estas políticas desde su ingreso al Fondo.

FODESEP se reserva el derecho de evaluar periódicamente el cumplimiento de estas Políticas. Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo con los procedimientos establecidos por la Institución y en estricto acatamiento de las estipulaciones legales vigentes.

En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con esta política, será directamente responsable de las sanciones legales (que por responsabilidad laboral, penal y civil se incurra) derivadas de sus propios actos. Igualmente, será responsable de los costos y gastos en que pudiera incurrir la Institución derivada de la defensa por el uso no autorizado o indebido de licencias de software.

En razón de lo anterior, no es permitido alegar ignorancia ni a estas políticas, ni a la documentación que en ellas se mencione, incluyendo, por supuesto, las demás licencias en uso.

En el caso en que razonablemente se asuma que se está haciendo uso ilegal o incorrecto de los servicios informáticos o sistemas de información, la Institución estará en absoluta libertad de limitar o remover las cuentas asignadas sin asumir por ello ninguna responsabilidad de ningún tipo.

13. NOTIFICACIÓN.

Con el fin de dar cumplimiento a las Políticas de uso responsable de los Sistemas de Información y Recursos Informáticos, la Secretaria General de FODESEP, establecerá

un acta de compromiso que firmarán todos los usuarios al momento de ingreso a la Entidad.

14. APLICACIÓN Y CUMPLIMIENTO

Esta política aplica a todos los empleados y contratistas de FODESEP, sean directivos, administrativos, técnicos, etc. Cualquier usuario que viole esta política será objeto de sanción disciplinaria, incluyendo la terminación de su relación laboral o contractual con el Fondo de Desarrollo de la Educación Superior FODESEP.

El presente documento será publicado en la página Web de FODESEP y en una cartelera de la Entidad, para conocimiento e inmediato acatamiento de los empleados y contratistas de FODESEP.

Dada en Bogotá, D.C.,

EULALIA NOHEMI JIMÉNEZ RODRIGUEZ
Gerente General

BARBARA ALEXY CARBONELL PINZÓN
Secretaria General

ALVARO WILINGTON ORTIZ SUAZA
Profesional 3 Tecnología

Proyectó: Alvaro Wilington Ortiz Suaza, Profesional 3 Tecnología
Revisó Bárbara Alexy Carbonell Pinzón, Secretaria General
Aprobó: José Alejandro Duque Ramírez, Asesor Jurídico

FODESEP
FONDO DE DESARROLLO DE LA EDUCACION SUPERIOR

ACTA DE COMPROMISO DE CUMPLIMIENTO DE LAS POLÍTICAS DE LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS DEL FONDO DE DESARROLLO DE LA EDUCACIÓN SUPERIOR "FODESEP"

En consideración de lo expresado en el Reglamento de Servicios Informáticos y en las Políticas Institucionales de FODESEP, yo, _____ en mi calidad de_____ (empleado, contratista, proveedor) portador de _____ (cédula de ciudadanía, pasaporte, tarjeta de identidad), número _____, manifiesto que he leído y entendido en su totalidad el reglamento y las políticas, por esta razón me comprometo a cumplir con ellas. Asimismo, reconozco que mi incumplimiento podría acarrear la responsabilidad disciplinaria, civil y penal no sólo para mi persona sino también para la Institución. Por ésta razón, acepto que puedo ser sancionado por la Institución como corresponda lo cual podría incluir la terminación de la relación _____(laboral, contratista, proveedor, etc.), con el FONDO DE DESARROLLO DE LA EDUCACION SUPERIOR "FODESEP"; sin perjuicio de la aplicación de las responsabilidades civiles y penales a que haya lugar.

Firma _____

Nombre del Usuario:_____
Bogotá, D.C., (colocar la fecha)

FODESEP de las afiliadas, por las afiliadas, para las afiliadas.
Calle 57 # 8b-05 int 32 PBX: 3478616 Fax: 3472310 e-mail: fodesep@fodesep.gov.co
http :www.fodesep.gov.co