FUNDACIÓN COMUNITARIA CENTRO DE INFORMACIÓN Y RECURSOS PARA EL DESARROLLO CIRD

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN

Junio de 2001

Reglamento de Seguridad de la Información

A. Definición de Seguridad de la Información (SI):

1. El propósito de la SI es precautelar la continuidad de las operaciones del CIRD y minimizar el eventual daño al funcionamiento de la institución o la posible transgresión a disposiciones legales, mediante la prevención y la disminución al mínimo del impacto de incidentes de seguridad. La reglamentación de la SI permite que la Información Clave sea compartida precautelando la protección de los activos de información y respetando las normas legales vigentes.

B. Componentes de la SI:

La SI se compone de tres elementos:

a) **confidencialidad: la protección contra uso no autorizado y contra interferencia externa.**
b) **integridad: la protección del carácter completo y preciso de la información y del software.**
c) **disponibilidad: asegurar que la información y los servicios vitales estén a disposición del usuario autorizado cuando los necesita..**

C. Respuesta a incidentes

1. Denuncia de incidentes de seguridad

a) Toda persona que tome conocimiento de un incidente de seguridad, deberá informar inmediatamente y en forma directa a la Sección Sistemas Informáticos.
b) La Sección Sistemas Informáticos establecerá un procedimiento formal para efectuar las denuncias asi como un procedimiento a seguir como respuesta a las denuncias que se reciban
c) Todos los funcionarios del CIRD y los terceros que presten servicios en el CIRD deberán estar informados por la Sección de Sistemas Informáticos acerca de los procedimientos establecidos para la denuncia de incidentes de seguridad

2. Denuncia de debilidades en la SI

a) Los usuarios de sistemas de información y archivos deberán tomar nota de cualquier debilidad de seguridad o posible amenaza que puedan observar en los sistemas o archivos e informar de inmediato.
b) Los usuarios deberán informar sobre estas cuestiones a su supervisor inmediato y a la Sección Sistemas Informáticos

c) Los usuarios no deberán, bajo ninguna circumstancia, intentar corregir las debilidades detectadas en sistemas informátIcos efectuando ensayos o arreglos por su cuenta.

3. Denuncia de defectos en software

a) Los usuarios deberán tomar nota de cualquier defecto de funcionamiento de software instalado e informar sobre el particular cuanto antes a la Sección de Sistemas Informáticos
b) Si el usuario sospecha que el mal funcionamiento del software se debe a la presencia en el software de elementos extraños, como ser un virus, deberá seguir inmediatamente el siguiente procedimiento:

i. Anotar los síntomas del problema y cualquier mensaje inusual que apareciere en pantalla.
ii. Cumplido el paso anterior, apagar la computadora y desconectarla del sistema o red si esto es posible. No transferir ningún disquet u otro medio de archivo a otra computadora.
iii. Dar aviso ala Sección de Sistemas Informáticos cuanto antes
iv. El equipo deberá necesariamente ser desconectado de cualquier red u otro equipo, antes de ser examinado o vuelto a encender
v. El usuario no deberá, en ningún caso, intentar remover el software del equipo. La recuperación del mismo estará a cargo de técnIcos.

6. Desplazamiento y retiro de activos de información.

a) Los funcionarios no podrán llevar datos, software o equipos fuera de su lugar de trabajo salvo autorización expresa.

D. Seguridad de los equipos

1. UbIcación y protección de equipos
a) Los equipos deberán ubIcarse en sitios que eviten al máximo el acceso a los mismos de personas no autorizadas a utilizarlos.

2. Fuentes de energía
a) Los equipos serán protegidos contra los daños causados por una interrrupción en la corriente electrIca.

4. Mantenimiento de equipos

a) Los equipos serán mantenidos de acuerdo con las recomendaciones del fabrIcante o del proveedor autorizado.
b) La reparación y el mantenimiento de equipos sólo podrán ser realizados por personas expresamente autorizadas para ello
b) Se llevará un registro completo de todas las fallas detectadas en los equipos.

E. Protección contra software defectuoso o maligno

1. Control de virus:

a) Se deberá respetar en todo momento los acuerdos de licencia de uso de software con los proveedores.
b) Queda prohibido el uso de software que no esté debidamente autorizado por el proveedor y aprobado por la Sección de Sistemas Informáticos
c) El software anti-virus será utilizado en la institución de la manera siguiente:

i. los usuarios deberán proceder diariamente, como rutina, a hacer correr el software anti-virus al inicio de sus tareas.
ii. la reparación o saneamiento de software conteniendo virus será efectuada sólo por personal técnIco.

d) Los usuarios de sistemas , procederán a revisar periódicamente el software y los datos contenidos en los sistemas. La presencia de archivos espurios o modificaciones no autorizadas deberán ser denunciados inmediatamente.
e) Cualquier disquet de origen incierto o no autorizado deberá ser revisado usando software anti-virus antes de ser utilizado.

F. Rutinas diarias

1. Back-up de datos (archivos de respaldo): Cada usuario deberá proceder rutinariamente a crear copias de respaldo de la información sensible o crítIca a fin de evitar una posible interrupción de operaciones por falta de información. Se deberán seguir las siguientes indIcaciones:

a) Un nivel mínimo de copias de respaldo (back-up) de información sensible, junto con un registro (índice) preciso y completo de las copias de respaldo, deberá ser mantenida en un sitio diferente al del sistema a una distancia prudente
b) Para las aplicaciones más importantes, se mantendrán por lo menos tres generaciones de datos de respaldo.

c) Los archivos con datos de respaldo deberán contar con la suficiente protección física.
d) Los datos de respaldo deberán ser revisados regularmente a fin de tener la seguridad de que podrán ser utilizados en cualquier momento en caso de necesidad.
e) Cada responsable de información determinará el tiempo mínimo de retención de copias de respaldo.

G. Administración de redes:

1. Control de seguridad de redes: Los administradores de redes deberán asegurarse que los controles apropiados estén instalados a fin de proteger a la información dentro de la red y evitar acceso no autorizado a la misma. En partIcular se deberá:

a) Separar, donde esto sea posible, las operaciones de procesamiento de la operación de redes
b) Reglamentar adecuadamente el uso remoto de equipos.
c) Instalar controles adecuados para proteger la información que circula por infraestructura de uso públIco.

H. Manipulación de medios magnétIcos y otros:

1. Manejo de medios removibles: Para el manejo de de medios removibles tales como cintas, discos, cartuchos e informes impresos, quedan establecidas las siguientes medidas de control :

a) cualquier medio removible que sea transladado de una dependencia a otra deberá contener sólo la información que necesite el receptor. Toda otra información deberá ser borrada antes del translado.
b) los medios removibles estarán almacenados en forma segura y de acuerdo a las especifIcaciones de los proveedores

2. Seguridad del correo electrónIco: Al usar el correo electrónIco, se deberá tener en cuenta las siguientes característIcas de dIcho servIcio:

a) su vulnerabilidad al acceso no autorizado
b) la probabilidad de errores en las direcciones
c) la falta de regulación legal, en el sentido de no contarse con pruebas de origen, envío, entrega o aceptación.
d) el efecto sobre la seguridad de la publicación de direcciones

e) la posibilidad de vulnerar la seguridad al permitir acceso remoto.

I. Administración de acceso de usuarios

1. Registro de usuarios: La sección de Sistemas Informáticos deberá contar con un procedimiento de registro y bajas para el acceso a todo sistema. El acceso será controlado por medio de un procedimiento de registración de las siguientes caracterísTlcas:

a) el usuario deberá contar con autorización del responsable del sistema para poder acceder al mismo
b) el nivel de acceso autorizado deberá adecuarse a una necesidad real operativa de la institución.
c) los usuarios deberán contar con una autorización escrita de su nivel de acceso
d) los responsables de los sistemas no podrán dar acceso a terceros sin la previa autorización
e) se mantendrá un registro oflcial de todos los usuarios autorizados
f) se revocará inmediatamente la autorización de acceso en el caso de que la persona cambie de puesto o se retire de la institución
g) se asegurará que los códigos de identiflcación de usuarios que dejen de ser utilizados no puedan ser otorgados a nuevos usuarios.

2. Administración de palabras clave (passwords) de usuarios: La asignación de palabras clave (passwords) seguirá el siguiente procedimiento administrativo:

a) los usuarios firmarán un documento por el cual se comprometen a mantener la confidencialidad del password
b) inicialmente la sección de Sistemas Informáticos proveerá al usuario un password de uso transitorio, que el mismo usuario deberá cambiar inmediatamente.
c) los password de uso transitorio se podrán otorgar también a usuarios que hayan perdido su propio password, siempre y cuando se cuente con la certeza de la identidad del usuario.
d) los passwords de uso transitorio se entregarán a los usuarios de una manera segura y directa. La transmisión de passwords de uso transitorio por terceras personas o por medios indirectos está prohibida
e) se considerará la posibilidad de usar otras tecnologías (verifIcación electrónica de firma, identiflcación de huella dactilar, etc.), para niveles superiores de seguridad.

J. Responsabilidades del usuario

1. Uso de palabras clave (passwords): Los usuarios seguirán las siguientes directrices para escoger su password:

a) los passwords son de uso personal
b) los passwords deben mantenerse en secreto
c) se deberá evitar registrar el password en un documento a papel escrito
d) cambiarán de password cada vez que sospechen una posible brecha en la confidencialidad
e) seleccionarán passwords con un mínimo de seis caracteres
f) no basarán sus passwords en ninguno de los siguientes elementos:

i. meses del año, dias de la semana, o cualquier otra forma de fecha
ii. nombres, apellidos, inIciales o números de matrícula de automóvil
iii. nombre de empresas, marcas conocidas , o "slogan"
iv. números de teléfono o series que contengan sólo números; deben ser siempre alfanumérIcos
v. cédula de identidad, RUC, u otro número usado como identifIcador
vi. más de dos caracteres idéntIcos en forma consecutiva
vii. passwords que sólo contengan números o que contengan sólo letras.

2. Equipos desatendidos: Los usuarios deberán asegurarse de que los equipos desatendidos estén protegidos, adoptando al menos las siguientes medidas:

a) salir del programa o aplicación cuando se haya terminado la tarea
b) salir de la computadora central (mainframe) cuando haya terminado la tarea y no proceder simplemente a apagar la PC o terminal.
c) resguardar el acceso a las PC o terminales mediante una llave o un pasword cuando no lo está usando.

3. IdentifIcadores de usuarios: Todos los usuarios deberán tener un identificador personal (IP) para su uso exclusivo, para asegurar que las actividades puedan ser posteriormente vinculadas a una persona responsable
4. Sistemas de administración de palabras clave (passwords) : Las computadoras deberán tener incorporado un sistema de passwords para autenticar a los usuarios. Dicho sistema de passwords tendrá las siguientes característIcas:

a) Basarse en el uso de passwords personales para deslindar responsabilidades
b) Permitirá a los usuarios crear sus propios passwords y tendrá un procedimiento de confirmación que tenga en cuenta la posibilidad de errores de tipeo.

c) Incluirá la necesidad de un cambio frecuente en los passwords para las cuentas con privilegios especiales
d) Los usuarios cambiarán su password de uso transitorio al primer logon (secuencia de acceso)
e) Se mantendrá un registro en la computadora de todos los passwords usados y cambiados en los últimos doce meses y se prohibirá su uso por otros usuarios.
f) Los passwords no serán visibles en pantalla en ningún momento
g) Los passwords se almacenarán en archivos separados de los datos de las aplIcaciones principales de los sistemas
h) Se almacenarán los passwords en forma encriptada, usando un algoritmo de encriptación de sentido únIco (one-way encription algorithm)
i) Se modifIcarán los passwords por defecto (default passwords) del proveedor de software una vez instalado
j) Se empedirá el uso de passwords que tengan las siguuientes carcaterístIcas:

i. meses del año, dias de la semana, o cualquier otra forma de fecha
ii. nombres, apellidos, inIciales o números de matrícula de automóvil
iii. nombre de empresas, marcas conocidas , o "slogan"
iv. números de teléfono o series que contengan sólo números
v. cédula de identidad, RUC, u otro número usado como identifIcador
vi. más de dos caracteres idéntIcos en forma consecutiva
vii. passwords que sólo contengan números o que contengan sólo letras.

K. Aspectos básIcos de la planifIcación de continuidad operativa

1. Procedimiento de planifIcación de la continuidad operativa: La Sección de Sistemas Informáticos desarrollará y mantendrá actualizados los planes de continuidad de operaciones para todos los sectores del CIRD. El proceso de planificación debe incluir la identifIcación y reducción de los riesgos presentados por amenazas accidentales o deliberadas a los sistemas vitales de información y a los AFIC. Los planes se desarrollarán para permitir la continuidad de las operaciones a pesar de la falla o destrucción de un sistema, archivo o servicio vital.