DGIP-RI-DIR-001

DIRECTRICES PARA MANEJO DE CONTRASEÑAS

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Liliana Córdova
Revisado por:	Dirección de Gestión de la Información y Procesos	Ing. Juan Carlos Proaño

Aprobado por:	Director DGIP	Ing. Roberto Andrade	

DGIP-RI-DIR-001

HOJA DEL ESTADO DEL DOCUMENTO

TITULO DEL DOCUMENTO: **Directrices para manejo de contraseñas** ESTADO DEL DOCUMENTO: Para aprobación con cambios			
1. QUIEN EDITA	**2. QUIEN REVISA**	**3. FECHA**	**4. RAZONES DE CAMBIO/QUIÈN CAMBIA**
L.CORDOVA L.CORDOVA	J.PROAÑO J.PROAÑO	13/12/2013 08/07/2014	En revisión Cambio DGIP por UGI, cambio Sistema NP a Sistema Operativo
L.CORDOVA	J.PROAÑO	04/02/2015	Directriz general para estándar de desarrollo de software. Directriz general para Sistemas de Autenticación Única
L.CORDOVA	J.PROAÑO	14/09/2015	Cambio en el formato general del documento

1. OBJETO

El objeto del presente documento es normar la construcción de contraseñas seguras, la protección de las mismas y la frecuencia de cambio, pues son un aspecto importante de seguridad. Ellos son la primera línea de protección para las cuentas del usuario. Una contraseña pobremente seleccionada puede comprometer los servicios de la EPN.

Como tal, todos los funcionarios con acceso a sistemas computacionales de la EPN son responsables de tomar las medidas necesarias para la protección de sus contraseñas.

2. ALCANCE

El alcance de esta directriz incluye a todo el personal que tiene o es responsable de una cuenta (o cualquier forma de acceso que soporta o requiere una contraseña) en cualquier equipo o sistema computacional que reside en la EPN, que tiene acceso a los servicios institucionales, o guarda cualquier información no pública de la EPN.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es :

Responsable de Seguridad

El responsable de revisar esta directriz es el:

Líder del Área de Infraestructura y Redes

El responsable de aprobar esta directriz es:

Director de la DGIP

La autoridad para hacer cumplir esta directriz es:

Director de la DGIP

Los responsables de cumplir esta directriz son :

Comunidad Politécnica

4. DIRECTRIZ

4.1 General

- Todas las contraseñas a nivel de sistema (por ejemplo, Root, administrador de Sistemas Operativos, cuentas de administración, etc.) deben cambiarse en un período de por lo menos un semestre.

- Toda la producción de contraseñas a nivel de sistema deben ser administradas por la DGIP gestionado a través de la base de datos de contraseñas con un gestor responsable de la base de datos.

- Todas las contraseñas a nivel de usuario (por ejemplo, el correo electrónico, Web, computador de escritorio, etc.) deben cambiarse cada semestre por lo menos.

- No deben insertarse las contraseñas en mensajes de correo electrónico u otros formularios de comunicación electrónica, e inalámbrica.

- Todas las contraseñas de nivel de usuario y nivel de sistema deben satisfacer a las normas descritas a continuación.

4.22 Normas

A. Normas de Construcción de Contraseña Generales Fuertes

Las contraseñas son usadas para varios propósitos en la EPN. Algunos de los usos más comunes incluyen: cuentas a nivel de usuario, cuentas Web, cuentas de correo electrónico, protección del protector de pantalla, contraseña del voicemail, el login del router local, entre otras. Subsecuentemente muy pocos sistemas tienen contraseñas temporales, por lo tanto se debe estar consciente de cómo seleccionar las contraseñas seguras.

Las contraseñas **fuertes** tienen las características siguientes:

- Contienen los caracteres mayúscula y minúscula (por ejemplo, un-z, UN-Z)

- Tiene dígitos y caracteres de puntuación así como las cartas por ejemplo: 0-9! @ #$% ^ & * () _+ | ~ - = \ ` {} []: "; '<>?. /)

- Son por lo menos de diez caracteres largos alfanuméricos
- No es una palabra de cualquier idioma, dialecto, lengua, etc.
- No se basan en información personal, los nombres de familia, etc.
- Las contraseñas nunca deben apuntarse o guardarse en línea.
- Intente crear contraseñas que pueden recordarse fácilmente. Una manera de hacer esto es crear una contraseña basada en un título de la canción, afirmación, u otra frase. Por ejemplo, la frase podría ser: "Este mayo Es Una Manera de Recordar" y la contraseña podría ser: "EmEUMdR! " o "EmEUM>r~ " o alguna otra variación.

NOTA: No use ambos ejemplos como contraseñas.

Para sistemas de autenticación única con o sin token la longitud de la cadena de seguridad personal debería tener como mínimo 5 números, que no pueden ser una combinación de fecha de años de nacimientos, cédulas, ni números de pasaporte, ni una cadena secuencial de números, ni cadena secuencial inversa.

B. Estándares de Protección de Contraseñas

Hasta que no exista un sistema de autenticación única, no use la misma contraseña para las cuentas de la EPN para varios accesos por ejemplo cuenta SAE, cuenta correo electrónico, etc.

No comparta las contraseñas de la EPN con cualquiera, incluyendo a ayudantes administrativos o secretarias. Todas las contraseñas serán tratadas como información confidencial sensible de la EPN.

A continuación se presenta una lista de cosas que no se deben hacer:

- No revele una contraseña por el teléfono a ninguna persona
- No revele una contraseña en un mensaje del correo electrónico
- No revele una contraseña al jefe
- No hable sobre una contraseña delante de otros

- No indique al formato de una contraseña (por ejemplo, "nombre de mi nombre")
- No revele una contraseña en encuestas o formularios de seguridad
- No comparta una contraseña con los miembros familiares
- No revele una contraseña a los colaboradores mientras está en vacación

Si alguien requiere una contraseña, refiérase a este documento o llame a alguien involucrado en actividades de Seguridad de Información.

No usar la opción "Recordar contraseña" de aplicaciones (por ejemplo., Eudora, Outlook, Messenger de Netscape, Mozilla Firefox, entre otros).

De nuevo, no apunte y no guarde las contraseñas en cualquier parte en su dependencia.

No guarde las contraseñas en un archivo en CUALQUIER computadora (incluso Palm Pilots o dispositivos similares) sin cifrado.

Cambie por lo menos una vez la contraseña cada seis meses. El intervalo de cambio recomendado es cada cuatro meses.

Si una cuenta o la contraseña es motivo de desconfianza o se sospecha que ha sido revelada, se debe denunciar el incidente inmediatamente a la DGIP.

Se debe ejecutar intentos de descifrado o adivinanza de contraseñas. Estas pueden ser ejecutadas periódicamente o en períodos aleatorios por la DGIP o sus delegados. Si una contraseña es adivinada o descifrada durante una de estas revisiones, el usuario exigirá que sea cambiada.

C. Estándares de Desarrollo de Aplicaciones

Los diseñadores de la aplicación deben asegurar que sus programas contienen como mínimo las siguientes precauciones de seguridad.

Las aplicaciones:

- Deben apoyar la autenticación de usuarios individuales, no grupales.

- Los desarrolladores deben insertar código para apoyar que el registro de claves del usuario respete las normas de construcción de contraseñas fuertes.
- No deben guardar las contraseñas en texto legible o en cualquier manera fácilmente reversible.
- Debe proveer facilidades de administración de contraseñas para que el usuario autorizado otorgue la restauración de contraseñas sin tener que conocerlas.

D. Uso de Contraseñas para los Usuarios de Acceso Remoto

El acceso a los servicios de la EPN vía acceso remoto debe usar una autenticación de claves publicas/privadas, usando una contraseña de acceso fuerte.

E. Contraseñas para Acceso Remoto

Las contraseñas son usadas para la autenticación de claves publica/privada. Un sistema de claves publicas/privadas define una relación de seguridad fuerte a través de una clave pública que es conocida por todos, y una clave privada que sólo es conocida por el usuario. Sin la contraseña para "desbloquear" la clave privada, el usuario no puede obtener acceso.

Las contraseñas para acceso remoto son una versión más larga de las contraseñas comentadas en el literal A, y es por consiguiente más segura. Una contraseña de acceso remoto está típicamente compuesta de múltiples palabras. Debido a esto, una contraseña de acceso remoto está más segura contra los "ataques de diccionario."

Todas las reglas que se aplican a las contraseñas anteriormente descritas, se aplican también a las contraseñas de acceso remoto.