REPUBLICA DEL PERU

COPIA FIEL DEL ORIGINAL
Ministerio de Transportes y Comunicaciones
Oficina General de Administración
BETY LUZ GALVAN NARVAEZ
DEPOSITARIO TITULAR
R.M. N° 748 - 2009 MTC / 01
Reg. 1204 Fecha: 30 DIC. 2010

Resolución Directoral

Lima,30 de diciembre del 2010 N° 1266-2010-MTC/10

CONSIDERANDO:

Que, por Resolución Ministerial N° 246-2007-PCM del 22 de agosto de 2007, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", en todas las Entidades integrantes del Sistema Nacional de Informática;

Que, de conformidad con el inciso b) del artículo 45° del Reglamento de Organización y Funciones del Ministerio de Transporte y Comunicaciones, aprobado por Decreto Supremo N° 021-2007-MTC, la Oficina de Tecnología de Información es competente para establecer políticas y normas relacionadas a los sistemas informáticos del Ministerio de Transporte y Comunicaciones;

Que, la Oficina de Tecnología de Información de la Oficina General de Administración ha alcanzado un documento denominado "Política de Contraseñas y Uso de Acceso a los Equipos Informáticos y a las Aplicaciones de los servicios del Ministerio de Transportes y Comunicaciones";

Que, la Oficina de Tecnología de Información y la Asesoría Legal de la Oficina General de Administración, a través del Memorándum N° 2662-2010-MTC/10.06, sustentado en el Informe N° 002-2010-MTC/RPG, y del Informe N° 1248-2010-MTC/10.10, del 10 y 20 de diciembre de 2010, respectivamente, han emitido opinión favorable respecto al contenido del proyecto de documento indicado en el considerando anterior;

Que, en tal sentido, resulta conveniente establecer una política de contraseñas para el acceso a los equipos informáticos y a las aplicaciones de los servicios, por medio de un proceso de gestión, con sujeción a la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI", para lo cual debe emitirse el acto administrativo correspondiente;

Que, por Resolución Secretarial N° 222-2007-MTC/04 del 16 de noviembre de 2007, la Secretaría General asignó a la Oficina General de Administración la función de expedir directivas internas sobre los Sistemas Administrativos a su cargo, así como de control patrimonial, de alcance general a todos los órganos y unidades orgánicas del Ministerio de Transportes y Comunicaciones;

De conformidad con lo dispuesto en la Ley N° 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones y el Reglamento de Organización y Funciones del Ministerio de Transportes y Comunicaciones, aprobado por Decreto Supremo N° 021-2007-MTC;

SE RESUELVE:

Artículo 1°.- Aprobar el documento "Política de Contraseñas y Uso de Acceso a los Equipos Informáticos y a las Aplicaciones de los servicios del Ministerio de Transportes y Comunicaciones", el mismo que forma parte integrante de la presente Resolución.

Artículo 2°.- Disponer la publicación del documento aprobado por el artículo 1° de la presente Resolución en la página Web del Ministerio de Transportes y Comunicaciones.

Regístrese y comuníquese.

KJELLING RUIZ DILLON
DIRECTOR GENERAL
Oficina General de Administración

"POLITICA DE CONTRASEÑAS Y USO DE ACCESO A LOS EQUIPOS INFORMATICOS Y APLICACIONES DE LOS SERVICIOS DEL MINISTERIO DE TRANSPORTE Y COMUNICACIONES"

I. OBJETIVO

Establecer los procesos de gestión para una adecuada política de contraseñas y uso de acceso a los equipos informáticos y aplicaciones de los servicios del Ministerio de Transportes y comunicaciones.

II. FINALIDAD

Resguardar la Integridad, confidencialidad, disponibilidad de la información en la creación y uso de las contraseñas que acceden a los equipos informáticos y aplicaciones (equipos de seguridad de red, equipo de comunicaciones, servidores, sistema contra incendio, sistema de acceso personal) del Ministerio de Transportes y Comunicaciones, resguardando la integridad de los datos y estableciendo un control adecuando en la controles de acceso.

III. ALCANCE

Las disposiciones contenidas en el presente documento son de aplicación para todos los servidores de la Sede Central y Oficinas Periféricas, que tengan acceso a los sistemas y equipos informáticos del Ministerio de Transporte y Comunicaciones.

IV. BASE LEGAL

- Ley Nº 29370, "Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones".
- Ley 27444, Ley del Procedimiento Administrativo General
- Decreto Supremo Nº 021-2007-MTC, Reglamento de Organización y Funciones del Ministerio de Transportes y Comunicaciones.
- Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición".
- Resolución Ministerial Nº 246-2007-PCM del 22 de agosto de 2007, que regula el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas practicas para la gestión de la seguridad de la información. 2ª Edición", en todas las Entidades integrantes del Sistema Nacional de Informática.
- Resolución de Contraloría Nº 320-2006-CG – "Normas de Control Interno para el Sector Público".

V. VIGENCIA

A partir de la fecha de aprobación de la presente Directiva.

VI. DISPOSICIONES ESPECÍFICAS

La creación de las contraseñas y uso de los accesos a los equipos informáticos y aplicaciones que la O.T.I., a de utilizar en los procesos y operaciones requieren de su autenticación, para cada usuario final (convencional) o especializado (técnico).Para efectos de nuestra seguridad se aplicara de la siguiente manera:

6.1 CONTRASEÑAS DE ACCESO A LOS EQUIPOS Y SISTEMAS DE COMUNICACIONES DE RED (SWITCHES, ROUTERS, ETC.), SEGURIDAD DE LA RED (FIREWALL, IPS, ETC.) Y SERVIDORES:

Dirigidos a usuarios administradores de servidores, de la red y la seguridad de la red.

- Utilizar como mínimo 12 caracteres para crear la clave.
- Utilizar en una misma contraseña dígitos, letras y caracteres especiales (por ejemplo: 0-8, !@#$%^8*() +|~=\`{}[]:";'<>?,./).
- Utilizar letras mayúsculas y minúsculas (por ejemplo: a-z, A-Z).
- Las contraseñas deben cambiarse con una periodicidad máxima de un trimestre (90 días) procurar no generar reglas secuenciales de cambio.
- En caso de una medida cautelar o emergencia, el administrador, ya sea de los equipos de comunicaciones de red, seguridad de la red o servidores, pueden cambiar la contraseña.
- Las contraseñas no deben de ser nunca almacenadas en un equipo de cómputo. Se debe de tratar de crear contraseñas que puedan ser recordadas fácilmente. Una forma de hacer esto es crear una contraseña basado en el nombre de una canción, una afirmación o una frase.
- Fácilmente: Una forma de hacer esto es crear una contraseña basado en el nombre de una canción, una afirmación o una frase.

6.2 CONTRASEÑAS DE ACCESO A LAS CUENTAS DE USUARIO:

Dirigido a todos los usuarios que acceden a su equipo por medio de sus cuentas.

- Longitud mínima de - 8 caracteres, recomendado
- Longitud máxima – 15 caracteres
- Complejidad mínima - no incluir palabras de diccionario. Las contraseñas deben utilizar tres de los siguientes cuatro tipos de caracteres:

1. Minúsculas
2. Mayúsculas
3. Números
4. Caracteres especiales como !@#$%^8*(){}[]

- Las contraseñas deben ser sensibles a mayúsculas y minúsculas. Los nombres de usuario o ID de inicio de sesión no deben ser sensibles a mayúsculas y minúsculas.
- Historial de Contraseña - Exigir un número de contraseñas únicas antes de que una contraseña pueda ser reutilizada. Este número no debe ser inferior a tres (03).
- Edad máxima de la contraseña - 45 días.
- Cuenta bloqueada temporalmente – En tres (03) intentos de acceso fallido.

- Restablecer la cuenta después del bloqueo temporal - El tiempo es tomado entre el acceso fallido y antes de que se cuente el acceso fallido sea limpiado. El valor recomendado es de 20 minutos. Esto significa que si hay tres malos intentos en 20 minutos, la cuenta será bloqueada.
- Duración del bloqueo de cuenta - El administrador debe restablecer el cierre temporal de la cuenta estando conscientes de la posible interrupción de los intentos fallidos en la red. Dependiendo de la situación, la cuenta de cierre debe estar entre 30 minutos y 2 horas.
- Ante el bloqueo de una cuenta, el usuario autorizado deberá comunicarse vía telefónica al anexo 1170 ó por correo electrónico a mesadeayuda@mtc.gob.pe, al área de Soporte técnico y operaciones para que se desbloquee dicha cuenta.
- Los protectores de pantalla deben estar protegidos con contraseña y deben estar activados y se activaran dentro de 5 minutos de inactividad del usuario. Los computadores no deberían ser descuidados con el usuario conectado, ni con el protector de pantalla protegido con contraseña activa. Los usuarios deben tener la costumbre de no salir de sus equipos al estar desbloqueados. Se puede pulsar la tecla CTRL-ALT-DEL teclas y seleccione "Bloquear equipo".

6.3 CONTRASEÑAS DE ACCESO A LAS APLICACIONES:

Dirigido a todos los usuarios que acceden a las aplicaciones de servicios desde su equipo y por medio de sus cuentas.

- Longitud mínima de - 8 caracteres recomendado
- Longitud máxima - 15 caracteres
- Complejidad mínima - no incluir palabras de diccionario. Las contraseñas deben utilizar tres de los siguientes cuatro tipos de caracteres:

  1. Minúsculas
  2. Mayúsculas
  3. Números
  4. Caracteres especiales como !@#$%^&*()-{}[]

- Las contraseñas deben ser sensibles a mayúsculas y minúsculas y los nombres de usuario o ID de inicio de sesión no deben ser sensibles a mayúsculas y minúsculas.
- Historial de Contraseña - Exigir un número de contraseñas únicas antes de que una contraseña pueda ser reutilizada. Este número no debe ser inferior a 6.
- La contraseña de origen, debe de ser cambiada con carácter de obligatoriedad, en la primera sesión de uso para que así el usuario sea el único que tenga conocimiento de su contraseña.
- Tiempo máxime de la contraseña - 30 días
- Almacenar contraseñas usando cifrado reversible - Esto no debería hacerse sin una autorización especial de la OTI ya que reduciría la seguridad de la contraseña del usuario.
- Cuenta bloqueada temporalmente - 3 intentos de acceso fallido.
- Restablecer la cuenta después del bloqueo temporal - El tiempo es tomado entre el acceso fallido y antes de que se cuente el acceso fallido sea limpiado. El valor recomendado es de 20 minutos. Esto significa que si hay tres malos intentos en 20 minutos, la cuenta será bloqueada.
- Duración del bloqueo de cuenta- El administrador debe restablecer el cierre temporal de la cuenta estando conscientes de la posible interrupción de los intentos fallidos en la red. Dependiendo de la situación, la cuenta de cierre debe estar entre 30 minutos y 2 horas.

- Ante el bloqueo de una aplicación, el usuario autorizado deberá comunicarse vía telefónica al anexo 1170 ó por correo electrónico a mesadeayuda@mtc.gob.pe, al área de Soporte técnico y operaciones para que se desbloquee dicha aplicación.

VII. DISPOSICIONES GENERALES

El objetivo de que todo el proceso de comunicación sea gestionado de forma segura, a la hora de acceder a los equipos informáticos, recae en la toma de una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad. La creación de las contraseñas que la Oficina de Tecnología de Información, en adelante O.T.I., e de utilizar en la mayoría de los procesos y operaciones, requieren de su autenticación, para cada usuario final (convencional) o especializado (técnico).

Para lo cual nos basamos en la "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información "Cláusula 11.2.3 Gestión de Contraseñas de usuario" "Cláusula 11.3.1 Responsabilidades de los Usuarios".Código de buenas prácticas para la gestión de la seguridad de la Información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

7.1 Cuidados de elección de contraseñas por parte de los usuarios:

Los usuarios finales (convencional) o especializado (técnico) emplean claves de acceso a sus dispositivos personales (laptop's, celulares con tecnología 3G) o estaciones de trabajo. La O.T.I provee herramientas informáticas para sus labores sin embargo respalda al usuario final (convencional) o usuario especializado (técnico) a establecer la clave de acceso a los mismos.

Sin embargo la O.T.I provee las buenas prácticas de seguridad para la selección y uso de contraseñas, de las cuales son los usuarios los únicos responsables de dicha elección.

7.2 Consecuencias de la sustracción o revelación de contraseñas

El objetivo de la sustracción de contraseñas es apropiarse de la Información del usuario con la finalidad de realizar acciones dañinas o delictivas como borrado de toda información y/o otras acciones. Las consecuencias son diversas y varían según el valor que cada usuario haya establecido como información.

Si un tercero suplanta nuestra identidad utilizando nuestro usuario y contraseña podrá acceder a los sistemas con nuestro usuario y, bien sustraer todo tipo de información del trabajador, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias económicas, de responsabilidad jurídica y de imagen.

7.3 Métodos de sustracción de contraseñas:

Los métodos para la sustracción de las contraseñas de un usuario son diversos podemos clasificarlos de esta manera:

a) Ingeniería social, por ejemplo utilizando el teléfono o un correo electrónico este grupo destaca el fraude conocido como "phishing", consiste en obtener las contraseñas o número de la tarjeta de un usuario,

mediante un e-mail, sms, fax, u/o otro medio de acceso que suplanta la personalidad de una entidad de confianza y donde se le insta al usuario que introduzca sus datos.

b) También es posible que el usuario se la comunique o ceda a un tercero y, por accidente o descuido, quede expuesta al delincuente, por ejemplo, al teclearla delante de otras personas. Puede ser que el atacante conozca los hábitos del usuario y deduzca el sistema que éste tiene para crear contraseñas (por ejemplo, que eligs personajes de su libro favorito) o que asigne la misma contraseña a varios servicios (correo electrónico, código PIN de las tarjetas de crédito o teléfono móvil, contraseña de usuario en su ordenador, etc.).

c) Ataque de fuerza bruta o de diccionario: consiste en que el atacante pruebe contraseñas sucesivas hasta encontrar la que abre el sistema. Se trata de métodos avanzados que en consiguen averiguar la contraseña cifrada atacándola con un programa informático ("crackeador") que la descodifica.

7.4 Características que debe reunir una contraseña:

a) Personal: Cada persona que acceda a un servicio, aplicación o sistema debe tener su propia contraseña.

b) Secreta: sólo el usuario de la contraseña debe conocerla.

c) Intransferible: la contraseña no debe ser revelada a ningún tercero para su uso.

d) Modificable solo para el titular: el cambio de contraseña, sea cual fuera el motivo, debe ser realizado por el usuario titular de la misma. Sólo en situaciones excepcionales, podría ser cambiada por el administrador, por ejemplo, cuando el usuario la hubiera olvidado o si estuviera en riesgo la seguridad de la organización, como sería en el caso de que fuera divulgada o detectada como débil luego de una auditoria.

e) Difícil de averiguar: Al momento de elegir su nueva contraseña, el usuario debe seguir ciertos lineamientos que impidan que pueda ser obtenida fácilmente.

7.5 Consideraciones y Acciones Generales para el Uso y Gestión de Contraseñas Seguras:

a) Cuide que no lo vean cuando escribe su clave y no observe a otros mientras lo hacen.
b) No utilizar la misma contraseña para distintas cuentas de los sistemas y equipos del Fondo, así como para otros accesos a red o aplicaciones proporcionados.
c) No comparta su clave con otros, ni pida la clave de otros.
d) No escriba la clave en un papel ni la guarde en un archivo sin cifrar.
e) Si por algún motivo tuvo que escribir la clave, no la deje al alcance de terceros (debajo del teclado, en un cajón del escritorio, etc.) y nunca pegada al monitor.
f) No habilite la opción de "recordar contraseñas" en los programas que utiliza.
g) Nunca envié su clave por correo electrónico o chat ni la mencione en una conversión presencial o telefónica, ni se la entregue a nadie, aunque sea o diga ser el administrador del sistema.
h) No mantenga una contraseña indefinidamente. Cámbiela regularmente, aunque las políticas de Administración de claves no lo obliguen expresamente.

i) No dude en cambiar sus contraseñas si sospecha que alguien puede conocerlas. Adicionalmente, en el ámbito laboral, hágale saber al personal competente de O.T.I. cualquier incidente que tenga en su cuenta.
j) No utilice ni permita que le asignen una cuenta sin contraseña.
k) Si se le ha otorgado una contraseña para el primer acceso a un sistema o si le ha olvidado, proceda a cambiarla en forma inmediata, aún cuando el mismo sistema no se lo requiera.
l) Si se le ha otorgado una contraseña para el primer acceso a un sistema o si le ha olvidado, proceda a cambiarla en forma inmediata, aún cuando el mismo sistema no se lo requiera.
m) Si debe acceder a algún servicio o a su correo electrónico en un lugar público, por ejemplo un cibercafé, considere que su clave puede haber sido espiada o comprometida, por lo que se recomienda que proceda a cambiarla ni bien le sea posible.

VIII. GLOSARIO:

a) **Aplicación:** Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo. Esto lo diferencia principalmente de otros tipos de programas como los sistemas operativos (que hacen funcionar al ordenador), las utilidades (que realizan tareas de mantenimiento o de uso general), y los lenguajes de programación (con el cual se crean los programas informáticos).

b) **Servidor:** Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

c) **Contraseña:** Conjunto finito de caracteres limitados que forman una palabra secreta, clave que sirve a uno o más usuarios para acceder a un determinado recurso.

d) **Centro de Cómputo:** Es un área de trabajo cuya función es la de concentrar, almacenar y procesar los datos y funciones operativas de una organización de manera sistematizada. Se encuentran los equipos de comunicación de red: switches, routers, etc.; equipos de seguridad de red: Firewall, IPS, etc.; los servidores,- sistema de protección contra incendios, sistema biométrico, sistema de ventilación, sistema de alimentación eléctrica ininterrumpida (UPS).

e) **Estación de Trabajo:** En informática una estación de trabajo (en inglés Workstation) es un microordenador de altas prestaciones destinado para trabajo técnico o científico. En una red de computadoras, es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red.

f) **Directorio Activo:** El Directorio Activo es la implementación de Microsoft del servicio de directorios LDAP para ser utilizado en entornos Windows. El Directorio Activo permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Directorio Activo almacena información de una organización en una base de datos central, organizada y ,accesible. Pueden encontrarse desde Directorios Activos con cientos de objetos para una red pequeña hasta Directorios Activos con millones de objetos.

g) **Switch:** Es un dispositivo digital de lógica de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

h) **Router:** Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

i) **Equipos de Comunicaciones:** Referente switch, router, hub

j) **Seguridad de red:** Referente firewall, IPS, IDS

k) **Firewall:** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

l) **IDS:** Un sistema de detección de intrusos, es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

m) **Sistema Biométrico:** Sistema automatizado de control de acceso de identificación dactilar para usuarios autorizados.

n) **Sistema de Protección Contra Incendios:** Dispositivos que detectan automáticamente ondas de calor o flama y que lleva a cabo la descarga del agente extintor.

o) **UPS:** (Uninterruptible Power Supply: 'suministro de energía interrumpido), es un dispositivo que mediante a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

p) **Caracteres Especiales:** Dígitos y caracteres de puntuación así como símbolos especiales.

q) **Caracteres Alfanuméricos:** Son caracteres combinados entre números y letras que pueden o no definir frases o palabras.