Política Manejo de Contraseñas

Pontificia Universidad Católica Madre y Maestra

Junio 2010

Política Manejo de Contraseñas

Área: UAR	Fecha: 01/06/2010
Información de Contacto: Francisco Sued	Referencia: **POL_TI_002_20100628**
Modificado por: Steven Sánchez	Versión:1.2

CONTENIDO

1. Introducción

1.1 Objetivo

El objetivo de esta política es establecer un estándar para la utilización de contraseñas seguras, la protección de dichas contraseñas y la frecuencia en que las mismas deberán ser cambiadas.

Las contraseñas son un importante aspecto de seguridad en los ambientes computacionales. Esta es la primera línea de protección para las cuentas de usuarios. Una contraseña mal elegida, puede resultar en el comprometimiento de toda la red interna de la institución. Así que todos los empleados, estudiantes, consultores y contratistas de PUCMM son responsables de tomar todas las medidas necesarias para escoger y asegurar sus contraseñas.

1.2 Alcance

El alcance incluye a todo el personal que posee o sea responsable de una cuenta (o cualquier otra forma de acceso que soporte o requiera contraseña) en un sistema o equipo que resida dentro de los recintos o campus de la PUCMM, con acceso a la red interna, o que almacene cualquier tipo de información no pública.

1.3 Glosario de Términos

* **Routers:** Enrutador, ruteador o encaminador. Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa 3.

* **Switchs:** Un conmutador o switch. Es un dispositivo analógico de lógica de interconexión de redes de computadores que opera en la capa 2.

2. Política de Manejo de Contraseña

Ya que las contraseñas son utilizadas para diversos propósitos como: acceder correos electrónicos, recursos de la red, servidores, estaciones de trabajo, etc., deben tomar en cuenta las siguientes recomendaciones para escoger contraseñas seguras.

2.1 Características de contraseñas pobres o débiles

a. La contraseña contiene menos de 8 caracteres.
b. La contraseña contiene palabras de uso común, como:
   - Nombre de familiares, mascotas, amigos, compañeros de trabajo, personajes, etc.
   - Términos computacionales y nombres de comandos, sitios, hardware, software.
   - Palabra relacionada al nombre de la institución “PUCMM” y/o Pontificia Universidad Católica Madre y Maestra.
   - Fecha de nacimiento o cualquier otra información personal como la dirección y número de teléfono.
   - Palabras o cualquier otro patrón como: aabb, qwerty, abcdef, zyxwvuts, 123321,123456, etc.
   - Cualquiera de las anteriores deletreadas al revés.

2.2 Características de contraseñas robustas

a. Contienen caracteres en mayúsculas y minúsculas. (Ej.: a-z, A-Z).
b. Contienen dígitos, signos de puntuación y caracteres. (EJ.: 0-9!@#$%^&*()_+~?).
c. Tienen una longitud de por los menos ocho (8) caracteres alfanuméricos.
d. No son palabras en ningún lenguaje, dialecto, argot, jergas propias colectivas, etc.
e. No son basados en información personal, nombre de familiares, etc.
f. Las contraseñas nunca deben ser anotadas o almacenados en el computador (incluyendo PDA o cualquier otro dispositivo similar) sin ser cifrada o guardada físicamente en la oficina. Se debe utilizar contraseñas que puedan ser recordadas fácilmente. Una forma es utilizar contraseñas basadas en frase, canciones o afirmación. Ej.: De la frase “Perro que labra no muerde” podríamos obtener la contraseña “PqLnm@45” adicionalmente podríamos agregarle otros caracteres especiales o numéricos para robustecer la contraseña.

2.3 Política para la protección de contraseñas

a. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
b. La contraseña asignada al personal administrativo de nuevo ingreso deberá ser proporcionada de manera confidencial y personal con previa autorización del jefe inmediato y solicitada por Recursos Humanos (HHRR). Esta contraseña será entregada al momento de firmarse el convenio de confidencialidad de forma impresa o verbal.
c. La contraseña asignada al personal docente de nuevo ingreso deberá ser proporcionada de manera confidencial y personal con previa autorización del departamento al que pertenece y solicitada por la Vicerrectoría Académica. Esta contraseña será entregada al momento de firmarse el convenio de confidencialidad de forma impresa o verbal.
d. La contraseña asignada a los estudiantes de nuevo ingreso deberán ser proporcionada de manera confidencial y personal. Esta contraseña será entregada por el departamento de registro a requerimiento de los estudiantes de forma impresa o verbal.

2.4 Cambio periódico de Contraseñas

a. Las contraseñas predeterminadas que traen los equipos nuevos tales como routers, switchs y otros equipos de comunicación, deben ser cambiadas inmediatamente se pone en servicio dicho equipos. De igual manera, las contraseñas predefinida de cuentas de usuarios administrador que vienen por defecto en los manejadores de base de datos, sistemas operativos y cualquier otro software de alto riesgo, deben ser cambiadas inmediatamente se pone en servicio y/o cuando se realiza una actualización de versión.
b. Toda solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada por escrita y debe ser debidamente aprobada, en caso de que se realice por correo electrónico debe llevar firma digital.
c. Se ha establecido que las contraseñas tendrán una validez de ciento ochenta (180) días, a los quince (15) días previos al vencimiento de la contraseña, se le notificará al usuario para que éste proceda a cambiar su contraseña. Si el usuario no cumple con este requisito, su cuenta será bloqueada automáticamente, y este deberá contactar a la Unidad de Administración de Redes (UAR) si es un usuario de la red, para proceder a desbloquear su cuenta.
d. Se deberá limitar a cinco (5) el número de intentos fallidos para el acceso a los sistemas de la PUCMM bloqueando los accesos asignados a dicha contraseña. La reactivación de los accesos deberá ser realizada solamente por la unidad responsable de la administración del servicio utilizado.
e. No se deberá reutilizar las mismas contraseñas cada vez que le sea solicitado el cambio de la misma, los sistemas principales guardarán un mínimo de tres (3) últimas contraseñas para que no sean reutilizadas.
f. El cambio de contraseña a los docentes, estudiantes y personal administrativo deberá ser realizado de forma presencial por el mismo usuario. De no poderse

realizar de esta forma, se le solicitará que acceda al portal institucional y realice el cambio a través de la aplicación web destinada para estos fines. De no tener el usuario la posibilidad de cambiar su contraseña por los dos métodos anteriormente descrito, la Unidad de Administración de Redes (UAR) podrá realizar el cambio de contraseña de forma telefónica requiriéndole al usuario una identificación necesaria que valide su identidad.

2.5 Aspectos de Seguridad de Contraseñas

Nunca comparta o revele una contraseña con nadie, incluyendo asistentes administrativos o secretarias. Todas las contraseñas deben ser tratadas como información sensitiva y confidencial de la PUCMM.

A continuación mencionamos una lista de acciones que “Nunca” deberá hacer:

a. Nunca revele una contraseña por teléfono a nadie.
b. Nunca revele una contraseña en un correo.
c. Nunca revele una contraseña al jefe.
d. Nunca hable sobre una contraseña en frente de nadie.
e. Nunca haga alusión al formato de una contraseña (EJ.: “Mi apellido”).
f. Nunca revele una contraseña en un cuestionario o formulario de seguridad.
g. Nunca comparta una contraseña con un familiar.
h. Nunca revele una contraseña a un compañero de trabajo mientras este de vacaciones.

Si alguien demanda que usted revele una contraseña, refiéralo a este documento o haga que contacte al Coordinador General de Tecnología de Información.

Nunca utilice la opción de “Recordar Contraseña” de ninguna aplicación (Ej.: Internet Explorer, Outlook, Netscape, Messenger, etc.).

Si se sospecha que una cuenta o contraseña ha sido violada, reporte el incidente a la Unidad de Administración de Redes (UAR) si es un usuario de la red, y de esta forma cambie todas sus contraseñas. La Unidad de Administración de Redes (UAR) deberá notificar al Coordinador General de Información cualquier tipo de incidente relacionado a la violación de cuentas de usuario.

La Unidad de Administración de Redes (UAR) y/o las personas designadas como administrador de seguridad de los sistemas de información, realizan pruebas periódicas o al azar cada cuatro (4) meses para detectar contraseñas débiles. Aquellas contraseñas que sean quebrantadas durante esta revisión se le requerirán que sean cambiadas inmediatamente.

3. Responsabilidades

La Unidad de Administración de Redes (UAR) deberá velar por la correcta asignación de contraseñas a los usuarios de nuevo ingresos y/o para aquellos usuarios que requieren de cambios en su contraseña.

Todo el personal que utilice cuentas de usuarios con privilegios administrativos en la red, servidores y sistemas de información de la PUCMM, serán responsable de toda actividad que represente un riesgo de seguridad para la institución.

El Coordinador General de Tecnología de Información será responsable de notificar a la Vicerrectoría de Administración y Finanzas (VAF) sobre cualquier eventualidad relacionada a la violación de cuentas de usuarios.

La Unidad de Auditoría Interna periódicamente estará monitoreando el cumplimiento de esta política.

4. Sanciones

El no cumplimiento de esta política podría tener como consecuencia la pérdida del acceso a los sistemas de PUCMM. Los abusos reiterados de esta política tienen como consecuencia el despido. La acción específica emprendida estará basada en un estudio de la trasgresión y de las circunstancias que rodeen el incumplimiento.

5. Historial de revisión

Este documento debe ser revisado y/o actualizado a partir de la fecha de su primera publicación e implementación por lo menos una vez al año.

Versión	Fecha de Revisión	Descripción de cambio	Preparado por	Autorizado por
1.1	05/01/12	Publicación original	Steven Sánchez	Alejandro J. Liz
1.2	11/01/2021	Modificación	Steven Sánchez	Francisco Sued