Universidad Politécnica de Cartagena
Unidad de Informática

Política de contraseñas - UPCT

Aprobada por: Consejo de Gobierno de la UPCT.

Fecha: 4 de julio de 2013**.**

Resumen:

En el presente documento se describirán una serie de requisitos necesarios y de recomendaciones encaminadas a mejorar la seguridad y robustez de las contraseñas personales para acceso a los servicios telemáticos ofrecidos por la UPCT.

Quiénes deben conocer este documento:

La presente Política será de aplicación para todas las personas que, de manera permanente o eventual, sean usuarios y posean una cuenta de acceso a los servicios y Sistemas de Información de la UPCT y utilicen contraseñas como medio de autenticación personal.

Por lo tanto, este documento debe ser conocido por:

- Toda la comunidad universitaria, como usuarios de los distintos servicios telemáticos.
- Los administradores de servicios.

Este documento es público y estará disponible en la Sede electrónica de la UPCT.

Por qué debe conocerse este documento:

El acceso a los servicios se basa en que cada usuario dispone de una cuenta en la UPCT, a la que se le asocia una contraseña que sólo dicho usuario conoce. Si esta contraseña es débil o poco segura se comprometen la confidencialidad y la autenticidad de los servicios, tanto para el propio usuario como para el resto de la comunidad universitaria. Es, por lo tanto, necesario establecer unos requisitos mínimos y unas recomendaciones básicas para que nuestras contraseñas garanticen un mínimo nivel de seguridad.

Todos los usuarios son responsables de sus contraseñas de acceso a los servicios y de los accesos que se produzcan haciendo uso de dichas contraseñas.

Como referencia y base de esta política se pueden consultar la Guía CCN-STIC 821 (Apéndice V) y el documento *"Política de contraseñas y seguridad de la información"* elaborado por el INTECO (http://www.inteco.es/Seguridad/Observatorio/Articulos/recomendaciones_creacion_uso_contrasenas)

Requisitos de las contraseñas de usuarios:

Estos requisitos van dirigidos a evitar que la contraseña deje de ser secreta, ya sea por revelación por parte del propio usuario, como porque algún atacante consiga descifrarla.

Todas las contraseñas de los usuarios de la UPCT deben cumplir las siguientes reglas:

1. Estar formada por al menos 8 caracteres.

2. Contener caracteres de al menos dos de las siguientes tres clases de caracteres:
   - Alfabéticos (o sea, a-z, A-Z); no se recomienda utilizar la "ñ" o vocales con tilde.
   - Numéricos (o sea, 0-9).
   - Caracteres especiales y de puntuación (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

3. No utilizar contraseñas que se puedan adivinar fácilmente, como pueden ser:
   - Una cadena de caracteres derivada del nombre de la cuenta del usuario.
   - Una cadena de caracteres formada por la repetición de caracteres.
   - Una palabra contenida en un diccionario (de lengua española o extranjera).
   - Una palabra de diccionario seguida o precedida de un carácter (p.ej. "palabra1" o "Xpalabra" o "palabra!".
   - Un nombre de pila: Nombres de familiares, amigos, mascotas, ciudades, etc.
   - Fechas de cumpleaños u otra información personal tales como dirección o número de teléfono.
   - Conjuntos de letras o números que sigan un patrón sencillo, tales como aaabbb, qwerty, abcdef, 123321, etc.

4. La contraseña deberá cambiarse al menos una vez cada año. En la web de ayuda del Servicio de Informática (Wiki) se informará sobre el procedimiento y las herramientas para el cambio de contraseñas.

5. **Nunca se solicitarán ni se revelarán contraseñas por correo electrónico.**

Las contraseñas se almacenarán con sistemas de encriptación fuerte. En el caso de que fuera necesario y a petición del propio usuario, el administrador le podrá generar una contraseña nueva; para ello el usuario debería estar perfectamente identificado, personándose ante el administrador con su DNI. También se podrá

generar una nueva contraseña para un usuario a petición del Responsable de la Información.

Al usuario se le habilitará una opción para el cambio de su contraseña de forma segura. **En cualquier caso, nunca se utilizarán canales inseguros (correo electrónico, Web no segura, etc.) para solicitar al usuario su contraseña**.

Recomendaciones sobre las contraseñas de usuarios:

- Se recomienda cambiar la contraseña en el primer momento de acceder a la cuenta, para que la nueva contraseña sea distinta a la que va en la solicitud.
- Es muy recomendable utilizar el **servicio "He olvidado mi contraseña"** para poder obtenerla de forma automática en caso de olvido; para ello hay que hacer una configuración previa de esta utilidad, disponible en el Portal de Servicios.
- No escribir nunca las contraseñas o almacenarlas en algún fichero.
- Las contraseñas deben ser suficientemente largas y fáciles de recordar. Para ello recomendamos crear la contraseña a partir de una frase que nos resulte fácil de reproducir. Por ejemplo: de la frase "*En un lugar de la Mancha: Albacete*" podríamos obtener la siguiente contraseña: *E1ldlM:AB* .
- Aunque se ha especificado en el apartado anterior que la contraseña se cambiará al menos una vez al año, recomendamos que dicho cambio se haga al menos cada 6 meses y, en cualquier caso, siempre que se tenga alguna sospecha de que haya podido ser conocida o adivinada por algún tercero; en este caso también debe ponerse en contacto con el personal de la Sección de Redes de la Unidad de Informática.
- El usuario no deberá emplear la misma contraseña para su cuenta de la universidad en otros servicios ajenos a la misma.
- La contraseña no se debe revelar a nadie, ni directamente, ni por teléfono, ni en respuesta a mensajes de correo electrónico en las que se le solicite.

Recomendaciones sobre contraseñas de servicios y servidores

Estas últimas recomendaciones van dirigidas a aquéllos que administran o son responsables de algún servidor o servicio que sea accesible a distintos usuarios (externos o internos):

- Tener unos criterios para la creación y asignación de contraseñas lo más similares posibles a los Requisitos obligatorios expuestos en esta Política.
- Los servidores y dispositivos se deben configurar con cuentas separadas para los que tienen privilegios de administración y los que no.
- Los usuarios se deberían autenticar con cuentas que no tuvieran más privilegios que los necesarios para hacer uso del servicio.
- El acceso a los privilegios correspondientes (para administrar la máquina) debe hacerse mediante mecanismos de "escalado de privilegios"; en este caso además quedará traza de qué usuario ha accedido a estos privilegios especiales.

- Sólo se tendrán los privilegios especiales el tiempo que sea estrictamente necesario.
- Se deberá dar de baja a aquellos usuarios que dejen de pertenecer al colectivo al que va destinado el servicio.