UNIVERSIDAD DE MURCIA

Normativa sobre contraseñas de usuario

Servicio especial de apoyo TI a investigadores

Área de las Tecnologías de la Información y las Comunicaciones Aplicadas

Universidad de Murcia

Versión: Febrero-2018

Preámbulo

Tanto el Esquema Nacional de Seguridad (ENS) como la Ley Orgánica de Protección de Datos (LOPD) establecen la necesidad de adopción de medidas de seguridad y fortalecimiento con respecto al ciclo de vida de las contraseñas. El Reglamento (R.D. 1720/2007) que desarrolla la LOPD determina medidas concretas es su articulado como la duración de las claves y límite en los intentos fallidos de conexión para aquellos sistemas que gestionan datos personales.

El articulo 93.4 indica: "El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible" lo cual supone en la práctica que las contraseñas deben tener una duración máxima de 1 año.

El artículo 98 contempla que el responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Esto supone que se debe poner límite a los intentos de conexión fallidos en los sistemas.

En base a ello, la presente Normativa de Uso tiene por objeto establecer las normas particulares sobre el uso de contraseñas para los usuarios de los servicios de las Tecnologías de la Información y las Comunicaciones (en adelante TIC) de la Universidad de Murcia.

Esta Normativa se mantendrá en todo momento actualizado y accesible mediante los procedimientos que en él se determinan.

Capítulo I - Objeto

Artículo 1. Descripción

La combinación usuario/contraseña identifica en todo momento las acciones que un usuario realiza en un sistema informático quedando éste como responsable último de dichas acciones.

Por este motivo los usuarios son responsables de la custodia de sus contraseñas y de adoptar las medidas de seguridad necesarias para evitar que sean comprometidas.

Artículo 2. Medidas de seguridad

ÁTICA adoptará las medidas de seguridad necesarias para dotar de mayor fortaleza y seguridad a las contraseñas de los usuarios de los servicios y recursos TIC, en particular las descritas en el Capítulo II de esta Normativa.

Capítulo II - Características y uso de las contraseñas

Artículo 3. Formato

Este servicio está abierto a Personal Docente e Investigador (PDI).

La elección de las contraseñas por parte de los usuarios se ajustarán a las siguientes especificaciones en cuanto el formato de las mismas:

a) La longitud mínima de una contraseña debe ser de 8 caracteres.

b) Debe contener caracteres de 3 de los siguientes 4 conjuntos:

   1. Alfabeto en minúsculas (sin la ñ y sin acentos)
   2. Alfabeto en mayúsculas (sin la Ñ y sin acentos)
   3. Símbolos: . : { } ! @ # $ % ^ & * ? _ ~ -
   4. Números del 0 al 9

Artículo 4. Ciclo de vida

La gestión de las contraseñas se podrá realizar en los siguientes procedimientos habilitados por ÁTICA:

a) En Sede Electrónica sede.um.es

b) En los procedimientos automáticos habilitados en Recursos Humanos y matriculaciones de estudiantes

c) En el portal de correo web https://webmail.um.es/cambiaclave/cambia.php

d) En otros procedimientos habilitados por ATICA.

Cuando un usuario acceda por primera vez a un servicio mediante la combinación usuario/contraseñas está debe ser cambiada inmediatamente. Es responsabilidad del usuario custodiar dicha clave desde ese momento.

Los usuarios están obligados a cambiar la contraseña con una periodicidad mínima de un año. Trascurrido un año de vigencia de una contraseña, sí el usuario no la cambia, el sistema pedirá el cambio obligatorio de ésta.

Las contraseñas no podrán reutilizarse en ningún caso una vez que hayan caducado o renovado por cualquier causa.

Artículo 5. Limitación en el número de intentos de conexión fallida

Los distintos sistemas limitarán el número de intentos de conexión fallidos bloqueando la cuenta de usuario.

Si técnicamente esto no fuese posible, se penalizarán progresivamente los reiterados intentos fallidos de conexión para evitar ataques de fuerza bruta.

Artículo 6. Renovación

Ante el olvido de claves, vulneraciones de las mismas o cualquier otra causa que exija la renovación de la contraseña (o clave) de una cuenta se utilizará uno de los siguientes métodos:

a) En Sede Electrónica utilizando certificado digital.

b) Utilización de la TUI en los TPS y en las aplicaciones que se disponga.

c) Mediante confirmación de envíos SMS.

d) De modo presencial en el Centro de Atención a Usuarios de ÁTICA

Capítulo III - Recomendaciones y buenas prácticas

Artículo 7. Recomendaciones y buenas prácticas

Los colectivos citados en el Artículo 4 de este Reglamento deben solicitar el acceso a los servicios incluidos en el Artículo 2 mediante la apertura de una petición DUMBO a través de los canales que ÁTICA ha dispuesto. En ella se incluirá una descripción del servicio o recurso que se solicita.

Se establecen una serie de recomendaciones y buenas prácticas con carácter general para el uso de contraseñas por parte de los usuarios. Estas medidas van destinadas a fortalecer el uso de contraseñas y que éstas no sean comprometidas por terceras personas que puedan usar el sistema es su beneficio o deteriorarlo.

En relación con la elección de la contraseña por parte del usuario:

La contraseña elegida no debe parecerse a, o contener, la dirección de correo o descripción de la cuenta, ni al servicio al que da acceso.

La contraseña elegida no debe ser una palabra que esté en algún diccionario de algún idioma (inglés, francés, español, etc.).

No se debe utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, número de DNI o número de teléfono, a la hora de elegir la contraseña. Tampoco se debe utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (por ejemplo, un apodo, alias, etc.).

Se debe evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”). No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

Se debe evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña, es deseable una combinación de todos ellos.

A la hora de elegir la contraseña, se recomienda utilizar una frase fácil de memorizar, acortarla y sustituir vocales por caracteres especiales. También se pueden utilizar reglas nemotécnicas del tipo “persona, acción y objeto” donde las palabras no tienen relación entre sí, pero son fáciles de recordar y se puede completar con números y caracteres especiales.

En relación al uso de la contraseña:

No se debe escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo móvil (por ejemplo, no guardar las contraseñas en documentos de texto dentro del ordenador).

No enviar nunca la contraseña por correo electrónico o en un mensaje. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

Se debe procurar limitar el número de intentos de acceso para evitar bloqueo de la cuenta.

No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).

Capítulo IV - Reforma de la normativa

Artículo 8. Reforma de la normativa

Esta Normativa se mantendrá en todo momento actualizado y accesible de forma electrónica desde la sede web de la Universidad de Murcia en la URL https://www.um.es/atica/normativa/ y de forma impresa en la sede institucional de ÁTICA.

La Normativa de Uso se modificará en el caso de que los avances tecnológicos, otras normas de rango superior u otras circunstancias lo aconsejen o exijan, por mandato del CIO de la Universidad o de cualesquiera órganos superiores.

La aprobación de esta Normativa es potestad del Consejo de Gobierno de la Universidad de Murcia.

Capítulo V - Disposiciones finales

Artículo 9. Disposiciones finales

Esta Normativa entrará en vigor al día siguiente de su aprobación en Consejo de Gobierno de la Universidad de Murcia.