Normas de creación y uso de contraseñas

1.- Resumen de versiones

Número	Fecha	Modificación
1	03/10/2019	Creación del documento

2.- Validación/aprobación

Clasificación:	USO INTERNO	Estado:	FINAL
Autor/origen	Jesús Manuel Martínez Castillo		
Revisión:	Consejo de Dirección de ATICA		08/10/2019
Aprobado:	Comisión de Seguridad		22/10/2019
Publicación:			29/10/2019

Área de Tecnologías de la Información y las Comunicaciones Aplicadas
Campus Universitario de Espinardo. 30100 Murcia
T. 868 88 4222 – F. 868 88 8337 – www.um.es/atica

Índice de contenidos

3.- Objeto

El objetivo de la presente norma es regular la creación y uso de contraseñas robustas, cuando este sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios de la Universidad de Murcia. Este documento se considera de uso interno de la Universidad de Murcia y, por tanto, no podrá ser divulgado salvo autorización del Responsable de Seguridad.

4.- Alcance

Esta Norma es de aplicación a todo el ámbito de actuación de la Universidad de Murcia, y sus contenidos traen causa de las directrices de carácter más general definidas en el documento *SGENS_01_Politica de Seguridad de la Información UM*.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Universidad de Murcia, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la Universidad de Murcia.

5.- Legislación y normativa aplicable

Las referencias tenidas en cuenta para la redacción de esta norma han sido:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Documentos y Guías CCN-STIC.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Público.
- La Jurisprudencia existente en materia de protección de datos de carácter personal. Se tendrán en cuenta también los informes y resoluciones de la AEPD.

6.- Roles y Responsabilidades

Comisión de Seguridad
• Aprobación de la norma de creación y uso de contraseñas. • Interpretar las dudas que puedan surgir de su aplicación. • Proceder a su revisión, cuando sea necesario actualizar su contenido o se cumplan los plazos máximos establecidos para ello. • Verificar su efectividad.

Responsable de Seguridad
• Custodia y divulgación de la versión aprobada de este documento

7.- Cuerpo del documento

7.1. Cómo crear contraseñas robustas

Es necesario que las contraseñas que se utilicen como mecanismos de autenticación sean robustas, es decir: difícilmente vulnerables.

En este sentido, se han definido las siguientes reglas, que se recomiendan sean seguidas por todos los usuarios a la hora del establecimiento de contraseñas:

- La longitud mínima de una contraseña debe ser de 8 caracteres.
- Debe consistir en una combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, dígitos numéricos y signos especiales):
  - Alfabeto en minúsculas (sin la ñ y sin acentos)
  - Alfabeto en mayúsculas (sin la Ñ y sin acentos)
  - Símbolos: . : { } ! @ # $ % ^ & * ? _ ~ -
  - Números del 0 al 9
- No conviene que posea caracteres idénticos consecutivos.
- Como recomendación, la contraseña no debería ser igual a ninguna de las últimas 5 contraseñas usadas.
- A la hora de elegir contraseña, se recomienda seguir la guía de recomendaciones y buenas prácticas definida en el apartado 8.4.

7.2. Gestión y renovación de contraseñas

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/

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.

7.3. 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.

7.4. Recomendaciones y buenas prácticas

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.).

8.- Vigencia

La aprobación de la presente Norma es potestad de la Comisión de Seguridad de la Información de la Universidad de Murcia y entrará en vigor al día siguiente de su aprobación y publicación en la web de ATICA.

Tras su aprobación establecerá las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Universidad de Murcia pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los epígrafes anteriores.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la Universidad de Murcia.

La presente normativa deberá ser revisada anualmente, o con menor periodicidad, si existieran circunstancias que así lo aconsejen.

La revisión aplicará a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, la adaptación a cambios habidos en el marco legal, la infraestructura tecnológica, organización general, etc.