NP.40 NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS

Documento de uso interno

ÌNDICE

CONTROL DE VERSIONES

Revisión	Fecha	Motivo del Cambio
1.0	1/11/2023	Versión inicial
Realizado y revisado: SICUE / Responsable de seguridad	Aprobado: Comité de Seguridad Fecha: 17/11/2023	

1 Objetivo

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 por parte de los usuarios de los Sistemas de Información de la Universidad de Extremadura.

Este documento se considera de uso interno de la Universidad de Extremadura (a partir de ahora, UEx) y, por tanto, no podrá ser divulgado salvo autorización del Responsable de Seguridad/Comité de Seguridad.

2 Ámbito de aplicación

Esta Norma se aplica a todo el ámbito de actuación de la UEx, y sus contenidos traen causa de las directrices de carácter más general definidas en el documento **PO.01 Política de Seguridad de la Información de la Universidad de Extremadura** (D.O.E. 109/2023, de 8 de junio).

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 Uex**, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la Uex y utilicen contraseñas como medio de autenticación personal.

3 Vigencia

La presente Norma ha sido aprobada por el Comité de Seguridad de la UEx, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la UEx 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 siguientes epígrafes.

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

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4 Revisión y evaluación

La gestión de esta Normativa corresponde al Comité de Seguridad que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los

plazos máximos establecidos para ello.

- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente normativa, que se someterá, de haber modificaciones, a aprobación.

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

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5 Normas previas

Las presentes Norma de creación y uso de contraseñas, complementa en sus aspectos específicos, a la **Normativa General De Utilización De Los Recursos Y Sistemas De Información De La UEx** y a las **Normas de Uso del Correo Electrónico (e-mail) en la UEx**, por lo que complementa a dichas normativas en los aspectos no señalados en las mismas.

6 Normativa

6.1 Uso de contraseñas

Las contraseñas (junto con el código de usuario o userid) son el medio de acceso a diferentes tipos de sistemas y servicios de información que necesitan de autenticación, tales como el ordenador del puesto de trabajo, el acceso a la red corporativa, acceso a la cuenta de correo electrónico, etc.

6.2 Cómo crear contraseñas robustas

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

Los siguientes párrafos señalan los aspectos que deben tenerse en cuenta para la creación de contraseñas robustas, atendiendo a los dos elementos involucrados: usuario y administrador del sistema (sistema de verificación de contraseñas).

Cuestiones previas:

- Como norma general, las contraseñas deben ser fáciles de recordar y de introducir, aunque difíciles de adivinar y de descubrir por fuerza bruta (prueba exhaustiva de todas las posibilidades).

- Tradicionalmente, se ha venido sosteniendo que las contraseñas, cuando son elegidas por el usuario, deberían poseer unas ciertas características, entre las que se encontraban: una longitud mínima y la conveniencia de que el conjunto de caracteres escogidos, además de no constituir una palabra de un diccionario, o una fecha, o un nombre propio, debería ser una combinación de letras mayúsculas y minúsculas, números y signos de puntuación.
- Sin embargo, la dificultad de recordar contraseñas construidas de la forma anterior (lo que suele provocar que los usuarios opten por escribir tales contraseñas en papel o en lugares no protegidos), junto con el incremento de la potencia de los ordenadores, han hecho que este procedimiento de generación de contraseñas no sea tan eficaz como originariamente pudo parecer. Por el contrario, la complejidad en la elección de una contraseña se determina usando el concepto de entropía, derivado de la Teoría de la Información de Shannon.

6.2.1 Requisitos para el usuario:

Deben considerarse las siguientes cuestiones, que afectan al usuario que genera las contraseñas:

- Las contraseñas deben tener una **longitud mínima** de 12 caracteres, y deberán combinar caracteres de distinto tipo: mayúsculas, minúsculas, números, y símbolos especiales.[1]
- Utilizar la **concatenación de varias palabras** para construir contraseñas largas (*passphrases*) cuya deducción, automática o no, no sea simple. Por ejemplo: "*elefanteneumáticocarpeta*", incluso contemplando la presencia de espacios en blanco. Por ejemplo: "*cocina televisor ventana*". También pueden utilizarse frases cortas sin sentido, tales como *"blue pigs do not piss", "los tontos huelen amarillo", "los de aquí son cortos de nariz", "azulín, azulado, esta contraseña me la he inventado"*.
- Las contraseñas **no deberán** estar compuestas de datos propios que otra persona pueda adivinar u obtener fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, etc.), ni ser frases famosas o refranes, ni ser estrofas de canciones o frases impactantes de películas o de obras de literatura.
- La contraseña, así formada, no deberá ser igual a ninguna de las últimas 3 contraseñas usadas, ni estar formada por una concatenación de ellas.
- Las contraseñas deberán sustituirse por otras si existe evidencia de que hubieren sido comprometidas.
- Como se ha dicho, las contraseñas deberán ser fáciles de recordar. Se hace necesario, por tanto, encontrar una solución de compromiso entre la robustez de la contraseña y la facilidad con la que puede recordarse. En este sentido, un mecanismo útil suelen ser los llamados **acrósticos**, que consisten en seleccionar un carácter de cada palabra de una frase fácilmente memorizable.

[1] Puede verificar la robustez de su contraseña en https://www.passwordmonster.com/

Por ejemplo, la frase: "Mi nombre es Napoleón Bonaparte. Tengo 36 años.", puede generar la cadena de caracteres "*MneNB.T36a.*"

- No debe permitirse apuntar las contraseñas en papel o bajo otro procedimiento o contenedor no seguro. No obstante, si se apuntan para no depender de la memoria, deben estar protegidas por algún contenedor seguro: un contenedor criptográfico como los gestores de claves con cifra o una caja fuerte, por ejemplo.
- Es especialmente importante mantener el carácter secreto de la contraseña. No debe entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata.
- No utilizar la misma contraseña para distintos servicios web o en el acceso a distintos dispositivos.
- Las contraseñas se cambiarán con una cierta periodicidad. Un año parece un tiempo razonable para su sustitución.

6.2.2 Requisitos para el administrador del sistema (sistema de verificación de contraseñas):

- El sistema de verificación debería permitir la introducción de contraseñas de, al menos, 32 caracteres, entre los que podría aceptarse el espacio en blanco, los caracteres imprimibles ASCII y UNICODE [ISO/ISC 10646] (con la cautela, en este último caso, de que cada código Unicode debe computarse como un único carácter). Cuando se trata de contraseñas largas -formadas por la concatenación de varias palabras- puede resultar útil que el sistema de verificación de contraseñas reemplace la presencia de varios espacios en blanco consecutivos por uno solo. En cualquier caso, el sistema de verificación no debe truncar la contraseña generada por el usuario.
- El sistema de verificación no debe ofrecer al usuario mecanismos para recordar su contraseña, (tales como: "¿Cómo se llamaba tu primera mascota?", etc.).
- El sistema de verificación de contraseñas debería comparar la nueva contraseña del usuario con una "lista negra" de contraseñas inaceptables, por ser ampliamente usadas, deducibles o haber estado comprometidas, entre ellas: contraseñas obtenidas de previas violaciones de seguridad, palabras de diccionarios, uso de caracteres repetitivos ("aaaaaa") o secuenciales ("1234abcd"), palabras relacionadas con el contexto, tales como el nombre del organismo, del servicio, el user-id del usuario y cualquiera de sus derivados. En estos casos, el sistema de verificación debería rechazar la contraseña e instar al usuario al generar una nueva contraseña.
- El sistema de verificación de contraseñas deberá limitar el número de intentos de acceso sin éxito. Esta medida de seguridad puede complementarse con una limitación del número de intentos en un periodo de tiempo considerado, etc.

- El sistema de verificación debería permitir al usuario la función de “pegar” (paste), lo que facilitaría el uso de gestores de contraseñas.
- Aunque por defecto se oculte, el sistema debe permitir al usuario ver el contenido de su contraseña, dándole la oportunidad de visualizar los caracteres si considera que está en un entorno confiable. La opción de visualización puede permitir al usuario ver completamente la contraseña o, durante un breve lapso, el último carácter introducido.
- El sistema de verificación de contraseñas debe usar algoritmos de cifrado autorizados, así como un canal protegido cuando requiera una contraseña del usuario.
- El sistema de verificación debe memorizar las contraseñas de los usuarios utilizando procedimientos seguros, de forma que las haga resistentes a ataques offline.
- El administrador de seguridad ejecutará herramientas de hacking ético para verificar la fortaleza de las contraseñas. Aquellas que no superen dicha prueba serán desactivadas obligando al usuario a cambiar la contraseña.
- Se anularán las contraseñas con más de un año de antigüedad.

6.3 Cambio de contraseña

Como se ha señalado, si un usuario ha olvidado o entiende que su contraseña ha quedado comprometida debe sustituirla por otra nueva, de manera inmediata usando el sistema de gestión de credenciales

https://www.unex.es/organizacion/servicios-universitarios/servicios/siue/funciones/servicio_usuario/gestion-de-credenciales

En cualquier caso, las contraseñas proporcionadas por el SICUE son consideradas contraseñas “provisionales” y son muy inseguras. Por ello, el usuario deberá proceder a sustituir la contraseña “provisional” por una contraseña personal que cumpla con los requisitos indicados en el apartado anterior. El usuario deberá realizar este cambio durante el primer inicio de sesión en su puesto de usuario.

Ningún usuario está autorizado acceder a los servicios internos de la UEx utilizando las credenciales de otros usuarios, incluyendo el simple conocimiento de la contraseña de otro usuario. Esta práctica compromete la confidencialidad de la información, y por supuesto, la autenticidad de quién accede a ella.

6.4 Gestión de contraseñas

El Comité de Seguridad/la Oficina de Seguridad, a través del SICUE, decidirá sobre la oportunidad de que ciertos usuarios puedan utilizar programas gestores de contraseñas. En estos casos, se seguirá el procedimiento especificado a este fin.

6.5 Modelo de Aceptación y compromiso de cumplimiento

Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la UEx deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla explícitamente en el sistema de gestión de credenciales.

7 Referencias

Esta Norma se apoya y se ve complementada por las siguientes referencias:

Internas:

- PO.01 Política de Seguridad de la Información de la Universidad de Extremadura, D.O.E. 109/2023, de 8 de junio.
- NG.01 Normativa General De Utilización De Los Recursos Y Sistemas De Información.
- NP.02 Normas de Uso del Correo Electrónico (e-mail) en la UEx.

Externas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).
- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- Guía de seguridad de las TIC CCN-STIC 821 Anexo V. NP.40 Normas de Creación y uso de contraseñas.