GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE V: NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS NP40

CCN
CENTRO CRIPTOLÓGICO NACIONAL

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.02.23 09:31:40 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO

1. 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 <<ENTIDAD>>.

   La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II 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 (ENS).

2. Este documento se considera de uso interno de la <<ENTIDAD>> y por tanto no podrá ser divulgado salvo autorización del <<U/OC>>.

2. ÁMBITO DE APLICACIÓN

3. Esta Norma es de aplicación a todo el ámbito de actuación de la <<ENTIDAD>>, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la <<ENTIDAD>>.
4. 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 <<ENTIDAD>>, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la <<ENTIDAD>> y utilicen contraseñas como medio de autenticación personal.

3. VIGENCIA

5. La presente Norma ha sido aprobada por la <<U/OC>> de la <<ENTIDAD>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la <<ENTIDAD>> 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.
6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.
7. 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

8. La gestión de esta Normativa corresponde a la <<U/OC>>, 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.

9. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la <<U/OC>> revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> de la <<ENTIDAD>>.
10. 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.
11. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

12. *<<En este epígrafe se deben incluir aquellas referencias documentales que vengan a apoyar o completar esta Norma o que hubieren sido consideradas en su redacción.*

***Internas**:*

- ----
- ----
-

***Externas**:*

(Por ejemplo:

- *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.*
- *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.*
- *Documentos y Guías CCN-STIC.*
- *Etc.>>*

6. NORMAS PREVIAS

13. Las presentes "Normas de creación y uso de contraseñas en la <<ENTIDAD>>" complementa, en sus aspectos específicos, a la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>"[1], por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

[1] Se recomienda que el organismo disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

7. NORMATIVA

7.1. USO DE CONTRASEÑAS

14. Las contraseñas (junto con el código de usuario o user-id) son el medio de acceso a…<<*explicitar los sistemas o servicios que precisan de contraseñas como mecanismo de autenticación, tales como el ordenador del puesto de trabajo, el acceso a la red corporativa, acceso a la cuenta de correo electrónico, etc.*>>.

7.2. CÓMO CREAR CONTRASEÑAS ROBUSTAS

15. Es necesario que las contraseñas que se utilicen como mecanismo de autenticación sean robustas, es decir: difícilmente vulnerables.
16. 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).
17. 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[2]. 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[3].

1. <u>Requisitos para el usuario</u>:

   Deben considerarse las siguientes cuestiones, que afectan al usuario que genera las contraseñas[4]:

   – Las contraseñas deben tener una longitud mínima de 8 caracteres.

[2] Véase al respecto, la primera Guía del NIST (NIST Special Publication 800-63. Appendix A -2003), en el que se hacían las recomendaciones señaladas.
[3] Shannon, Claude E. "A Mathematical Theory of Communication", Bell System Technical Journal. Octubre, 1948.
[4] Siguiendo -entre otras publicaciones- lo señalado al respecto por el NIST (National Institute of Standards and Technology) en su "NIST Special Publication 800-63B Digital Identity Guidelines – Authentication and Lifecycle Managament, (June, 2017)",

- 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 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[5].
- No debe permitirse apuntar las contraseñas en papel o bajo otro procedimiento o contenedor no seguro[6].
- 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.

2. Requisitos para el administrador del sistema (sistema de verificación de contraseñas):
   - El sistema de verificación no debe impedir el reconocimiento de contraseñas mayores de 8 caracteres[7].

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

[6] 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.

[7] El sistema de verificación debería permitir la introducción de contraseñas de, al menos, 64 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

- 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[8].
- El sistema de verificación de contraseñas deberá limitar el número de intentos de acceso sin éxito[9].
- El sistema de verificación debería permitir al usuario la función de "pegar" (*paste*), lo que facilitaría el uso de gestores de contraseñas, siempre que el uso de tales herramientas esté permitido y debidamente recogido en la Normativa Interna de la entidad.
- 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[10].
- 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[11].
- El administrador de seguridad ejecutará un programa de descifrado de contraseñas (*password-cracker* [12]) antes de las 24 horas desde el establecimiento de la contraseña, anulando las contraseñas que no superen dicha prueba.
- Todas las contraseñas del sistema serán analizadas por un programa de descifrado de contraseñas al menos cada 30 días, anulándose las contraseñas que no superen dicha prueba.

---

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.

[8] Resulta muy útil disponer de un sistema automático de ayuda al usuario para la confección de contraseñas robustas que le indique, por ejemplo, la fortaleza de la contraseña y le guíe sobre las características que debe tener una contraseña adecuada y robusta.

[9] Medida de seguridad que puede complementarse con una limitación del número de intentos en un periodo de tiempo considerado, etc.

[10] La opción de visualización puede permitir al usuario ver completamente la contraseña o, durante un breve lapso, el último carácter introducido.

[11] Véase la Guía CCN-STIC 807 en lo que respecta a funciones criptográficas para manejar contraseñas.

[12] Tales como: *Brutus, RainbowCrack, Wfuzz, Cain and Abel, John the Ripper, Medusa, OphCrack*, etc.

- Para las contraseñas que no superen el programa de descifrado de contraseñas puede aplicarse un mecanismo en dos fases: en las primeras 24h, si el usuario accede al sistema, se le obligará a modificar su contraseña. Pasadas las 24h, la contraseña se anula y el usuario habrá de pasar por un proceso completo de autenticación.
- Se anularán las contraseñas con más de un año de antigüedad.

7.3. CAMBIO DE CONTRASEÑA

18. Como hemos señalado, si un usuario entiende que su contraseña ha quedado comprometida o la ha cedido a terceros autorizados por motivos de trabajo o mantenimiento, debe proceder a sustituirla por otra que no hubiere sido comprometida, de manera inmediata.
19. Por otro lado, el usuario deberá realizar una petición de cambio de contraseña a la <<U/OC>>, (<<por ejemplo, a través de la herramienta de Atención de Usuarios>>) cuando se produzca alguna de las situaciones siguientes:
    - Olvido de la contraseña.
    - Bloqueo del acceso a través de contraseña tras 3 [o <<*señalar número de intentos*>>] intentos fallidos.
20. En estos casos, como norma general, el cambio de contraseña por una contraseña provisional (generalmente, de un solo uso) será realizado por personal técnico de <<U/OC>>, que comunicará esta contraseña al usuario, sin intermediarios.
21. Las contraseñas proporcionadas por la <<U/OC>>, tras la petición de cambio de contraseña de un equipo y/o aplicaciones, 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.
22. Ningún usuario está autorizado acceder a los servicios internos de la <<ENTIDAD>> utilizando usuario+contraseña 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.

7.4. GESTIÓN DE CONTRASEÑAS

23. El <<ORGANISMO>>, a través de la <<U/OC>>, decidirá sobre la oportunidad de que ciertos usuarios puedan utilizar programas gestores de contraseñas[13].

8. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

24. Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la <<ENTIDAD>> deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla.

[13] Llegado este caso, se recomienda encarecidamente usar un estricto procedimiento de uso de tales gestores.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la <<ENTIDAD>>/empleado de la <<EMPRESA>>*], como usuario de recursos informáticos y sistemas de información de la <<ENTIDAD>>, declara haber leído y comprendido las Normas de Creación y Uso de Contraseñas de la <<ENTIDAD>> (*versión x*) y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a ____ de _____ de 20__>>

Entidad:	
Trabajador (Nombre y Apellidos)	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por la <<ENTIDAD>>: <<*Nombre y Apellidos*>>

DNI número: _____

Número de Registro de Personal: _____