Centro Informático Científico de Andalucía
CONSEJERÍA DE TRANSFORMACIÓN ECONÓMICA, INDUSTRIA, CONOCIMIENTO Y UNIVERSIDADES

JUNTA DE ANDALUCIA

NORMAS DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

NS03 – GESTIÓN DE CONTRASEÑAS

Fecha: 22 agosto 2019

Índice de contenido

1. OBJETIVO

1. El presente documento constituye la norma de seguridad del CICA en cuanto a la creación y uso de contraseñas, y forma parte del conjunto de normas de seguridad del CICA, "NS00 CICA – GENERAL".

2. CREACIÓN Y USO DE CONTRASEÑAS

2.1. USO DE CONTRASEÑAS

2. Las contraseñas (junto con el identificador de usuario o user-id) son el medio de acceso principal a los sistemas y servicios existentes en el CICA y que precisan de contraseñas como mecanismo de autenticación, tales como el ordenador del puesto de trabajo, el acceso a la red corporativa y a los distintos sistemas y aplicaciones corporativos, acceso a la cuenta de correo electrónico, etc. Es por esto que se redactan las presentes normas.

2.2. CÓMO CREAR CONTRASEÑAS ROBUSTAS

3. Las contraseñas que se utilicen como mecanismo de autenticación deben ser robustas, es decir: difícilmente vulnerables.
4. 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).
5. 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.
   - 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 9 caracteres.
       - Deben contener como mínimo cuatro letras, de las cuales al menos una debe ser

Mayúscula.

- Deben contener como mínimo un número.
- Deben contener como mínimo un carácter especial de los siguientes (- * ? ! @ # $ / () {} = . , ; :).
- NO deben contener vocales tildadas, ni eñes, ni espacios.
- NO se enviarán por correo electrónico.
- NO se utilizará la característica "recordar contraseña" de ninguna aplicación (ej: Outlook, Internet Explorer, Thunderbird).
- NUNCA se deben almacenar en un servidor o maquina en red sin utilizar algún tipo de encriptación.
- NO serán utilizadas su clave en computadores considerados como no confiables.
- Es recomendable utilizar la concatenación de varias palabras para construir contraseñas largas (passphrases) cuya deducción, automática o no, no sea simple. Por ejemplo: "elefanteneumáticocarpeta". También pueden utilizarse frases cortas sin sentido, tales como "blue-pigs-do-not-piss", "los-tontos-huelen-amarillo", "los-de-aqui-son-cortos-de-nariz", "azulin,azulado,esta_contraseña_me_la_he_inventado".
- 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.
- NO deberán ser igual a ninguna de las últimas contraseñas usadas, ni estar formada por una concatenación de ellas.
- Deberán sustituirse por otras si existe evidencia de que hubieren sido comprometidas.
- 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. 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 (compañeros de trabajo, superiores, familiares, personal técnico, etc). En caso de haber tenido necesidad imperiosa de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata. Se pondrá especial cuidado en no permitir que nadie vea cuando teclea la clave en un computador.
- NO utilizar la misma contraseña para distintos servicios web o en el acceso a distintos

dispositivos.

- Los sistemas recordarán las últimas 6 claves utilizadas, por lo que no se podrán reutilizar.
- Deben ser cambiadas de forma obligatoria cada 4 meses. Este cambio será forzado desde la administración de las aplicaciones, o cuando los administradores de los sistemas lo consideren necesario debido a alguna vulnerabilidad en los criterios de seguridad.

- 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. 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).
  - 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.
  - 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.
  - 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 un programa de descifrado de contraseñas (password-cracker[1]) 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.

1 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 24 horas, si el usuario accede al sistema, se le obligará a modificar su contraseña. Pasadas las 24 horas, 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.

2.3. CAMBIO DE CONTRASEÑA

6. 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.
7. Por otro lado, el usuario deberá realizar una petición de cambio de contraseña al CSU mediante correo a soporte@cica.es cuando se produzca alguna de las situaciones siguientes:
   - Olvido de la contraseña.
   - Bloqueo del acceso a través de contraseña tras el límite de intentos fallidos establecidos.

     En estos casos, como norma general, el cambio de contraseña por una contraseña provisional (generalmente, de un solo uso) será realizado por personal técnico del CSU, que comunicará esta contraseña al usuario, sin intermediarios.
   - Las contraseñas proporcionadas por el CSU, 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.
   - Ningún usuario está autorizado acceder a los servicios internos del CICA 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.

2.4. GESTIÓN DE CONTRASEÑAS

8. El CICA, a través del Área de Seguridad, decidirá sobre la oportunidad de que ciertos usuarios puedan utilizar programas gestores de contraseñas.

2.5. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

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

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [personal del CICA/ empleado de la Empresa _____], como usuario de recursos informáticos y sistemas de información del CICA, declara haber leído y comprendido las Normas de Creación y Uso de Contraseñas del CICA y se compromete, bajo su responsabilidad, a su cumplimiento.

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

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

Revisor por parte del CICA: _____

DNI número: _____

Número de Registro de Personal: _____