Junta de Castilla y León

USO OFICIAL

Instrucción técnica de seguridad

Política de Gestión de contraseñas de las cuentas educa.jcyl.es

Nivel de difusión: **TLP:GREEN**

Servicio de Seguridad de la Información

Servicio de Seguridad de la Información

abril 2023

Contenido

1 Objetivo

El objetivo de la presente Instrucción Técnica 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 que la Consejería de Educación de la Junta de Castilla y León pone a disposición de su comunidad educativa.

El presente procedimiento operativo de creación y uso de contraseñas complementa en sus aspectos específicos a la normativa general de utilización de los recursos y sistemas e información de la Junta de Castilla y León.

Este documento se considera de uso interno del personal perteneciente a la Consejería de Educación de la Junta de Castilla y León, y por tanto no podrá ser divulgado salvo autorización expresa de la Consejería de Educación.

2 Ámbito de aplicación

Esta Instrucción Técnica es de aplicación a todo el ámbito de actuación de la Consejería de Educación donde se utilicen cuentas del dominio @educa.jcyl.es, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la Junta de Castilla y León (ORDEN FYM/337/2022, de 8 de abril, por la que se aprueba la norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León publicada en el BOCyL nº 75 de 20 de abril de 2022).

La presente Instrucción Técnica será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en los Centros Educativos de titularidad de la Consejería de Educación (en adelante CEDUs), incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de dicho Organismo y utilicen contraseñas como medio de autenticación personal, así como el personal de la Consejería de Educación o personal externo que utilice los servicios que presta dicha Consejería mediante cuentas del dominio @educa.jcyl.es.

Todos los usuarios de los recursos informáticos y/o sistemas e información afectados deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Instrucción Técnica, debiendo suscribirla.

3 Desarrollo de la instrucción técnica

3.1 Política de gestión de contraseñas

Las contraseñas, junto con un identificador de usuario, son el mecanismo de protección de acceso más común, uso habitual en el acceso al puesto de usuario y a las diferentes aplicaciones y servicios incluidos en el ámbito mencionado en el punto anterior. Son la protección básica habitual utilizada cuando sólo existe un único factor: ‘algo’ que se conoce.

La contraseña asociada a una credencial solo se activará bajo el control del usuario, siendo personales e intransferibles. El empleado público reconocerá que las ha recibido y aceptará las obligaciones implícitas de su tenencia: cambio de contraseña provisional/temporal, custodia diligente, protección de su confidencialidad y comunicación a su CAU de incidente en caso de olvido, bloqueo de acceso o pérdida.

Se informará sobre la necesidad de modificar una contraseña asignada de forma inicial, sobre las normativas de seguridad existente y sobre la posibilidad de reportar incidentes sobre dicho mecanismo de autenticación.

Se retirarán las contraseñas débiles y/o por defecto de aquellos equipos y recursos, antes de su entrada en funcionamiento u operación.

3.2 Creación robusta de las contraseñas

Las contraseñas deberán adecuarse a unas reglas de calidad suficientes para que sean robustas, es decir, difícilmente vulnerables.

Deberán ser fáciles de recordar y difíciles de averiguar mediante técnicas automatizadas de cálculo computacional o mediante técnicas de ingeniería social.

Las contraseñas tendrán una longitud mínima y deberán incluir requisitos de complejidad de contraseña. Se recomienda la concatenación de varias palabras que juntas carezcan de significado para construir contraseñas largas cuya deducción no sea simple.

Las contraseñas no deberán contener:

- Contraseñas en blanco.
- Identificador de usuario.
- Secuencias fácilmente identificables, incluyendo número o letras consecutivos o repetidos (1234, 1111, abcd, aaaa, etc.), letras cercanas en la distribución de teclado (asdf).
- Contraseñas por defecto de sistemas sin configurar.
- Información fácilmente asociable al usuario como nombres de familiares o mascotas, números de teléfonos, matriculas, fechas o en general información pública del usuario.

3.3 Protección de contraseñas

Las contraseñas deben mantenerse en secreto y no deben compartirse con nadie.

Deben existir mecanismos de expiración y caducidad de contraseñas para obligar a los usuarios al cambio de esta.

No hay distinción para las contraseñas con privilegios especiales (administrador, root, etc.)

No hay obligación de modificar el identificador de las cuentas de usuario (acceso a sistema operativo, correo, servicios web, etc.)

Las contraseñas se almacenarán con un sistema de encriptación fuerte. En el caso de que fuera necesario y a petición del propio usuario, el administrador le podrá generar una nueva contraseña. Para ello, el usuario deberá estar perfectamente identificado, siguiendo el procedimiento o protocolo de verificación de identidades. También se podrá generar una nueva contraseña para un usuario a petición del Responsable de Seguridad.

El usuario deberá modificar su contraseña de forma periódica, si se ha olvidado de ella, si se ha bloqueado el acceso tras varios intentos fallidos o si existen sospechas de que la contraseña ha sido comprometida.

En estos casos, el proceso seguirá el circuito de cambio de contraseña asignando al usuario una contraseña provisional (de un solo uso). Preferiblemente, esta contraseña debe ser entregada en mano o a través de algún medio que no permita su acceso por personas no autorizadas. En el caso de enviarlas por medios telemáticos o en un soporte, se enviarán separadas del identificador.

Las contraseñas no se enviarán nunca en claro a través de las redes de comunicaciones evitando su interceptación.

Se recomienda el uso de gestores de contraseñas para que los usuarios eviten escribir las mismas en claro en cualquier soporte.

Todas las contraseñas por defecto de los sistemas o aplicaciones deben ser desactivadas cuando no sean necesarias. La autenticación de las aplicaciones debe ser individual, no estando permitida la autenticación por grupo. Cuando sea necesario por razones operacionales, deberá estar justificado y aprobado formalmente, aplicando los controles de seguridad compensatorios necesarios.

Los sistemas de información no deben mostrar las contraseñas en claro por pantalla.

El número de intentos de acceso sin éxito consecutivos a un sistema de información debe estar limitado, tras el cual, se bloquearán los sistemas.

Se debe evitar la característica "recordar Contraseña" existente en algunas aplicaciones y formularios.

3.4 Requisitos de las contraseñas

Los sistemas de información, siempre que sea posible, deberán garantizar el cumplimiento de los requisitos de la siguiente tabla.

Parámetro	Valor
Periodo máximo de rotación	365 días para las cuentas de usuario.
Caducidad de contraseñas	Automática, al finalizar el periodo máximo de rotación.
Reutilización de contraseñas	Ninguna de las 24 últimas. 5 intentos de entrada antes de bloqueo.
Intervalo mínimo entre cambios	2 días.
Longitud mínima	12 caracteres.
Requisitos de complejidad	• No contener en parte o en su totalidad el nombre de usuario. • Estar compuesta por al menos 3 de los siguientes 4 conjuntos de caracteres: – Caracteres alfanuméricos en mayúsculas. – Caracteres alfanuméricos en minúsculas. – Caracteres numéricos. – Símbolos/caracteres especiales.

3.5 Usos prohibidos

No se almacenarán las contraseñas en inventarios, ni en servicios, soportes o herramientas que no aporten los suficientes mecanismos de seguridad en su acceso.

No se registrarán las contraseñas en soportes no protegidos, siendo necesario un servicio o herramienta con encriptación fuerte y no alojada en la nube.

No se repetirá la contraseña de acceso al puesto de usuario en otras aplicaciones y servicios ACCyL que permitan la elección de esta. No se reutilizarán las últimas contraseñas, según el procedimiento corporativo aplicable.

Queda prohibido el uso de las mismas contraseñas en servicios personales y no relacionados con la actividad laboral del puesto de trabajo.

Queda prohibido el uso y acceso a servicios de la ACCyL utilizando usuario y contraseña de otro empleado público o usuario, lo que comprometería la confidencialidad y la autenticidad.

El incumplimiento de estas obligaciones podrá dar lugar a la desactivación temporal o permanente de las credenciales asociadas, así como a la responsabilidad disciplinaria que proceda, sin perjuicio de las consecuencias legales que conlleve dicho incumplimiento.

3.6 Ciclo de vida de la identidad del usuario

Se considera identidad del usuario al conjunto de identificador de usuario y su correspondiente contraseña.

3.6.1 Creación

Las cuentas y sus contraseñas se crean automáticamente cuando el usuario entra en el sistema educativo de Castilla y León (no se cuenta como tal los estudios universitarios), a través del Sistema de Gestión de Identidades de la Consejería de Educación. Una vez creada la identidad del usuario (Identificador y contraseña), ésta se comunica al Centro Educativo junto con la información contenida en este procedimiento. La cuenta se crea con una expiración inicial de 30 días, tiempo para que las credenciales lleguen al usuario a través del CEDU (para usuarios pertenecientes a dicho CEDU), o a través de los canales habituales para la gestión de cuentas (para el resto de los usuarios de la Consejería de Educación o para los usuarios externos que prestan servicios a dicha Consejería), para que el usuario cambie la contraseña y sea únicamente conocida por él.

En el caso de usuarios correspondientes a padres/tutores de alumnos, pueden darse de alta accediendo al Área privada en el Portal de Educación, y con la misma política de gestión de contraseñas que el resto de los usuarios.

3.6.2 Modificación

En el portal de Educación existe un enlace para la recuperación/modificación de contraseña. Dicho enlace es accesible desde el Area privada del usuario o en la pantalla de login para el caso de recuperación de contraseña (que implicará el cambio de dicha contraseña).

3.6.3 Borrado

El sistema de gestión de identidades de la Consejería de Educación elimina automáticamente la cuenta cuando el usuario sale del sistema educativo de Castilla y León.

No hay opción de borrar la cuenta mientras el usuario pertenezca al sistema educativo de Castilla y León ya que todos los pertenecientes a dicha comunidad deben utilizar canales oficiales para ciertas tareas que requieren de una cuenta en dicho sistema.

4 Anexos

4.1 Legislación

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León.
- Reglamento 910/2014 del parlamento europeo y del consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- ORDEN FYM/337/2022, de 8 de abril, por la que se aprueba la norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León publicada en el BOCyL nº 75 de 20 de abril de 2022.

4.2 Referencias

- CCN-STIC-821 Normas de Seguridad en el ENS.
- CCN-STIC-821 Apéndice V Normas de creación y uso de contraseñas.
- CCN-STIC-436 Herramientas de Análisis de Contraseñas.