Universidad de Alcalá

Política de contraseñas

Aprobada por acuerdo de Comité de Seguridad de la Información y Seguridad TIC de la Universidad de Alcalá en su sesión de 15 de marzo de 2024

Las contraseñas constituyen el mecanismo básico que se emplea para la autenticación de los usuarios en el acceso a sistemas, servicios y aplicaciones. La fortaleza del mecanismo de autenticación basado en contraseña se fundamenta en dos principios básicos. En primer lugar, la contraseña debe ser secreta; sólo debe conocerla el propio usuario que además es el responsable de su custodia. En segundo lugar, no debe ser posible averiguar la contraseña; las contraseñas no deben ser predecibles ni deducibles a partir de información disponible de forma pública.

Si alguna de las dos condiciones anteriores no se cumple, se puede comprometer no sólo la seguridad del usuario sino la de toda la Universidad de Alcalá (UAH). Cualquiera que conozca la contraseña de un usuario legítimo, será reconocido ante los servicios y aplicaciones de la Universidad de Alcalá como ese usuario. Todos los usuarios son responsables de sus contraseñas de acceso a servicios y aplicaciones y de los accesos que se produzcan haciendo uso de ellas.

El conjunto usuario y contraseña (credenciales) permite entre otros el acceso a los siguiente servicios y aplicaciones de la Universidad de Alcalá:

- Autenticación local para acceso al puesto de trabajo (equipos conectados a dominio)
- MiPortal
- Correo Electrónico
- Red Privada Virtual (VPN)
- Aula Virtual
- Servicios de Intranet
- Acceso a la red inalámbrica eduroam

1. Requisitos obligatorios de las Contraseñas

Las contraseñas de todos los usuarios que tengan cuenta en la Universidad de Alcalá deben cumplir los siguientes requisitos:

1. Deberán tener una longitud igual o superior a 12 caracteres.
2. Estar compuesta por uno o más caracteres de estos 4 grupos:
   - Letras mayúsculas (de la A a la Z)
   - Letras minúsculas (de la a a la z)
   - Números (del 0 al 9)
   - Símbolos (caracteres no alfanuméricos): ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
3. La contraseña no deberá ser igual a ninguna de las 6 últimas contraseñas usadas.
4. No contendrá el nombre de cuenta del usuario o partes de su nombre completo.
5. No se deben utilizar palabras que se encuentren en diccionarios en ningún idioma.
6. La contraseña se deberá cambiar al menos una vez al año. Pasado el tiempo de caducidad de la contraseña, la cuenta será bloqueada.

UNIVERSIDAD DE ALCALÁ – PATRIMONIO DE LA HUMANIDAD – WORLD HERITAGE – WWW.UAH.ES

2. Recomendaciones sobre uso de Contraseñas

Aparte de los requisitos básicos detallados en el apartado anterior, proporcionamos las siguientes recomendaciones a la hora de crear una contraseña:

- Evite utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf”, “98765”…)
- No utilice la letra ñ si viaja mucho y no sabe cómo ponerla en teclados no españoles.
- No se debe utilizar información personal en la contraseña: nombre de usuario, apellidos, fecha de nacimiento, aniversarios, nombres de familiares, DNI o número de teléfono.
- Si por algún motivo el usuario dispone de varias cuentas de la Universidad de Alcalá, no debería emplear la misma contraseña en dichas cuentas.
- Existen muchas guías y tutoriales sobre cómo elegir contraseñas. No elija en ningún caso ninguna de las contraseñas que se muestran como ejemplo.

Aparte de la caducidad establecida de un año, es recomendable cambiar de forma periódica la contraseña. El cambio de contraseña podrá realizarse por vía telemática accediendo a un servidor web seguro. Si tiene algún problema en el proceso de cambio, puede comunicarse el Centro de Atención al Usuario (CAU) de los Servicios Informáticos de la Universidad.

Debe tener presente que en ningún momento se le solicitará la contraseña por correo electrónico o SMS de modo que debe ignorar cualquier petición recibida por esas vías de comunicación. Si recibe algún correo electrónico en el que se le solicita su contraseña, por favor póngalo en conocimiento del CAU.

Algunas recomendaciones orientadas al cambio de contraseñas son las siguientes:

1. Se recomienda que se cambien al menos una vez cada 6 meses.
2. No emplee reglas predecibles o secuenciales de cambio. Por ejemplo, evite crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña, e.g., pasar de Aksjaksj-2014 a Aksjaksj-2015
3. 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 hubiera sido comprometida, de manera inmediata.
4. Las contraseñas proporcionadas por la Universidad de Alcalá tras la petición de cambio de contraseña de un equipo y/o aplicaciones, son consideradas contraseñas “provisionales”. 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.

UNIVERSIDAD DE ALCALÁ – PATRIMONIO DE LA HUMANIDAD – WORLD HERITAGE – WWW.UAH.ES

3. Protección de Contraseñas

Con respecto a la custodia confidencial de las contraseñas, recomendamos las siguientes buenas prácticas:

1. Las contraseñas no deben compartirse con nadie. Las contraseñas deben tratarse como información confidencial de la Universidad de Alcalá.
2. La contraseña es una información sensible orientada a identificarle de forma unívoca que no debe compartirse con compañeros de trabajo o colaboradores.
3. Las contraseñas no deben incluirse en ningún tipo de comunicación electrónica.
4. En ningún caso se le solicitará que incluya la contraseña en ningún cuestionario o formulario que reciba por correo electrónico.
5. No es recomendable incluir sugerencias (*hints*) para recordar contraseñas. No habilite tampoco la funcionalidad de 'pregunta secreta' y si es obligatorio, no incorpore información verídica relacionada con usted.
6. No escriba jamás su contraseña en ordenadores públicos, compartidos o aquellos en que se desconozca su nivel de seguridad o se estime que pueden estar monitorizados de forma remota, por ejemplo, si se conecta desde un cibercafé o un terminal de acceso a Internet de un aeropuerto.
7. No escriba ni almacene su contraseña cerca de su lugar de trabajo habitual. Tampoco guarde sus contraseñas en un fichero en su ordenador, teléfono móvil o *tablet* salvo que dicho fichero se almacene cifrado.
8. No escriba su contraseña si el acceso a la web del servicio no se realiza mediante protocolo web seguro ('https')
9. No emplee la opción 'Recordar contraseña' que ofrecen los navegadores, especialmente cuando se trate de ordenadores compartidos.
10. Ante cualquier sospecha de que su contraseña ha podido ser comprometida, avise al CAU y cámbiela.
11. Nunca debe registrarse en aplicaciones, sitios o servicios de uso personal (cuentas de correo electrónico personales, redes sociales, almacenamiento personal …) con la cuenta corporativa de la UAH y bajo ningún concepto se debe utilizar la misma contraseña. En el caso de que el servicio pudiera estar relacionado con la Universidad, no elija para dicho servicio la misma contraseña. Cuando existe una filtración de contraseñas para algún servicio, los atacantes suelen emplear las credenciales afectadas para tratar de acceder a otros servicios. Si usted se ha registrado en un servicio externo con la misma cuenta de correo y contraseña que en la Universidad, un incidente de seguridad en ese servicio externo puede poner en riesgo su cuenta de la Universidad.

La mayor parte de las recomendaciones que aparecen en este documento son extensibles a cualquier otra contraseña de otras cuentas externas a la UAH que usted pueda tener. Adicionalmente a las anteriores, y para servicios externos, es recomendable atender a las siguientes buenas prácticas:

1. Si al registrarse en un servicio se le proporciona una contraseña, cámbiela inmediatamente.
2. En muchas ocasiones, los servicios de Internet ofrecen distintas opciones de seguridad que deben ser configuradas por los usuarios. Es recomendable activar estas opciones y configurarlas. Entre estas se encuentran:
    - Establecer la necesidad de introducir información adicional en caso de sucesos atípicos (por ejemplo, desde dispositivos no utilizados anteriormente).
    - Activar la autenticación de doble factor o de dos pasos (2FA o MFA) en determinados servicios. Con este sistema, el usuario, tras introducir correctamente su contraseña, debe introducir un código adicional que se suele recibir en una aplicación instalada en otro dispositivo (teléfono móvil, tablet, extensión de navegador …etc.). La mayor parte de los servicios de Internet de las grandes compañías (Google, Linkedin, Dropbox, Apple…)

UNIVERSIDAD DE ALCALÁ – PATRIMONIO DE LA HUMANIDAD – WORLD HERITAGE – WWW.UAH.ES

obligan a la utilización de este sistema.

3. En algunos casos puede ser útil la utilización de un programa de gestión de contraseñas.