Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfono: 91 885 47 00
Fax: 91 885 47 47

Recomendaciones sobre el Uso de Contraseñas

Las contraseñas o *passwords* constituyen el mecanismo básico que se emplea para la autenticación de los usuarios para el acceso a 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 de toda la Universidad de Alcalá. Tenga en cuenta que cualquiera que conozca su contraseña será reconocido ante los servicios y aplicaciones de la Universidad de Alcalá como usted mismo. Todos los usuarios son responsables de sus contraseñas de acceso a servicios y aplicaciones y de los accesos que se produzcan haciendo uso de esas contraseñas.

Su usuario y contraseña le permite el acceso a los siguiente servicios y aplicaciones de la Universidad de Alcalá:

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

Creación de Contraseñas

El primer paso para garantizar que nuestra contraseña es secreta consiste en elegir adecuadamente la misma. Para elegir una contraseña fuerte debemos tener en cuenta las siguientes recomendaciones:

1. Se han definido las siguientes reglas, que deberán ser seguidas por todos los usuarios a la hora de la definición o creación de contraseñas:
   - Deberán tener una longitud igual o superior a 8 caracteres.
   - Deberán consistir en una combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, dígitos numéricos y signos especiales).
   - No conviene que posea caracteres idénticos consecutivos.
   - La contraseña no deberá ser igual a ninguna de las 3 últimas contraseñas usadas
2. Evite utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf”, “98765”…)
3. No utilice la letra *ñ* si viaja mucho y no sabe cómo ponerla en teclados no españoles

Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfono: 91 885 47 00
Fax: 91 885 47 47

4. Los usuarios no deben utilizar información personal en la contraseña: nombre del usuario, apellidos, fecha de nacimiento, aniversarios, nombres de familiares. En ningún caso deben emplearse datos tales como DNI o número de teléfono.
5. La contraseña no debe contener el nombre de usuario.
6. No deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar de forma sistemática palabras que extraen tanto de diccionarios como de bases de datos con las claves más comunes, en ocasiones construidas a partir de bases de datos de contraseñas filtradas en Internet. Estos diccionarios son cada vez más sofisticados lo que hace que debamos ser más cautelosos.
7. Si por algún motivo el usuario dispone de varias cuentas de la Universidad de Alcalá, no debería emplear la misma contraseña en dichas cuentas.
8. Los usuarios no deben emplear la misma contraseña que usan para la cuenta de la Universidad de Alcalá en otros servicios o aplicaciones (por ejemplo, cuentas de correo electrónico personales, redes sociales, aplicaciones móviles…).
9. Existen muchas guías y tutoriales sobre cómo elegir contraseñas. No elija en ningún caso ninguna de las contraseñas que se muestran como ejemplo.

Cambio de Contraseñas

Es recomendable cambiar de forma periódica la contraseña. Además, el usuario podrá iniciar en cualquier momento el proceso de cambio de contraseña desde la web https://pwd.uah.es. 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 debería 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.

1. Las contraseñas de las cuentas de usuario deben cambiarse al menos una vez al año. Se recomienda que se cambien al menos una vez cada 6 meses. Para cambiar su contraseña puede dirigirse a https://pwd.uah.es
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

SERVICIOS INFORMÁTICOS
Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfono: 91 885 47 00
Fax: 91 885 47 47

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 su contraseña y la almacene 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. No emplee la cuenta de correo de la Universidad de Alcalá para registrarse en ningún servicio (redes sociales, servicios de almacenamiento online como Dropbox, Linkedin…), excepto en el caso en que el servicio esté directamente relacionado con la Universidad. En caso de hacer eso, no elija para dicho servicio la misma contraseña. Cuando existe una filtración de contraseñas para algún servicio, los atacantes suelen emplear las cuentas afectadas con las correspondientes contraseñas para tratar de acceder a otros servicios. Si usted se ha registrado en un servicio externo con su cuenta de correo de la Universidad y la misma contraseña que en la Universidad, un incidente de seguridad en ese servicio externo puede poner en riesgo su cuenta de la Universidad.
12. Si tiene el correo corporativo de la Universidad de Alcalá reenviado a alguna otra cuenta externa, debe tener presente que el acceso a esa cuenta externa permitirá el acceso a todos los correos de su cuenta corporativa. Debe ser consciente que este tipo de prácticas aumentan el riesgo de que sus correos se vean expuestos.

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.

Universidad de Alcalá

SERVICIOS INFORMÁTICOS
Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfono: 91 885 47 00
Fax: 91 885 47 47

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 opciones, es positivo establecer la necesidad de introducir información adicional en caso de sucesos atípicos (por ejemplo, desde dispositivos no utilizados anteriormente) o activar la autenticación de doble factor o de dos pasos en determinados servicios . Con este sistema, el usuario, tras introducir correctamente su contraseña, debe introducir un código adicional que se suele recibir en el teléfono móvil, por ejemplo mediante un mensaje corto. En la actualidad, la mayor parte de los servicios de Internet de las grandes compañías (Google, Linkedin, Dropbox, Apple…) ofrecen estas opciones.

3. Considere la utilización de un programa de gestión de contraseñas como LastPass, PaswordSafe o KeePass.

Referencias:

Para la elaboración de este documento, se ha tomado como base las siguientes recomendaciones:

Guide to Enterprise Password Management. Recommendations of the National Institute of Standards and Technology (NIST). Special Publication 800-118. National Institute of Standards and Technology. 2009

Guía CCN-STIC 821. Normas de Seguridad en el Esquema Nacional de Seguridad. Apéndice V: Normas de Creación y Uso de Contraseñas. NP40. Centro Criptológico Nacional

Guía sobre riesgos y buenas prácticas en autenticación online. Instituto Nacional de Tecnologías de la Comunicación. 2012