Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Política de contraseñas de la Universidad de Oviedo

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Para lograr el cumplimiento de estos principios y requisitos, el Esquema Nacional de Seguridad establece una serie de medidas que deben implantarse en las administraciones públicas. Entre estas medidas están aquellas relacionadas con los sistemas de identificación y autenticación de los usuarios.

En el caso particular de la Universidad de Oviedo el acceso a servicios cuya naturaleza requiere la autenticación de los usuarios, se realiza normalmente con las credenciales que proporciona esta institución a los miembros de la comunidad universitaria. Estas credenciales están formadas por un par de datos, compuesto por un nombre de usuario y una contraseña que, según el Esquema Nacional de Seguridad, han de seguir **políticas rigurosas de calidad y renovación frecuente**, tal y como se establece en el Anexo II del Real Decreto.

I. Objetivo y ámbito de aplicación

Esta política de contraseñas tiene como objetivo regular la creación y uso de contraseñas, cuando este sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios de la Universidad de Oviedo.

Será de aplicación en todo el ámbito de actuación de la Universidad de Oviedo y sus contenidos emanan de las directrices de carácter más general definidas en la Política de Seguridad de la Información de esta institución. La política de contraseñas será de aplicación y de obligado cumplimiento para todos los usuarios que, de manera permanente o eventual, dispongan de credenciales corporativas de la Universidad de Oviedo.

El Servicio de Informática y Comunicaciones de la Universidad de Oviedo, como encargado del correcto funcionamiento de los servicios informáticos y de comunicaciones corporativos, velará por el cumplimiento de esta normativa en todo momento. Se advierte que esta política afecta no solo a los recursos gestionados directamente por este servicio sino también a cualquier equipo o servicio conectado a la red corporativa de la Universidad de Oviedo.

II. Política general

a. Las siguientes directrices generales son de obligado cumplimiento:

1. Todas las contraseñas tendrán que cambiarse, al menos, una vez al año. Se implementarán medidas técnicas para recordar a los usuarios esta obligación.
2. Las contraseñas no deberán almacenarse por escrito.
3. Las contraseñas son personales e intransferibles, por lo que no pueden comunicarse a usuarios distintos de su propietario.
4. La comunicación de una nueva contraseña al usuario se realizará por medios seguros que garanticen la confidencialidad. El usuario admitirá que la ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
5. Las contraseñas creadas de forma automática o bajo petición al Servicio de Informática y Comunicaciones, deberán modificarse por el usuario en un plazo no superior a un mes.
6. Las aplicaciones y servicios controlarán intentos repetidos de acceso a una cuenta, pudiendo llegar a bloquearla. En la medida de lo posible, se implementarán mecanismos de doble factor de autenticación.

b. Ni la Universidad de Oviedo como institución ni ninguno de sus servicios pedirán las contraseñas a los usuarios. El uso de las credenciales está limitado a la autenticación en el acceso a algunos servicios. Los correos electrónicos en los que se solicitan las credenciales de usuario deben ignorarse.

c. Cualquier sospecha de que una cuenta o contraseña puede haber sido comprometida deberá ser comunicada de forma urgente al Servicio de Informática y Comunicaciones de la Universidad.

III. Calidad de las contraseñas

a. Durante el proceso de renovación de una contraseña, no será posible utilizar una contraseña que el usuario haya utilizado con anterioridad

b. Las contraseñas tendrán un mínimo de 8 caracteres, siendo obligatorio incluir algún símbolo (&, *, =, etc.) y al menos dos grupos de los siguientes:

1. Letras minúsculas
2. Letras mayúsculas
3. Números

c. La contraseña no contendrá espacios en blanco.

IV. Recomendaciones

a. Las contraseñas no deberían estar basadas en algún dato propio que pueda obtenerse fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, etc.)

b. La contraseña de las cuentas universitarias no debería utilizarse en cuentas de otros servicios de Internet.

c. Los usuarios que disponen de distintas cuentas universitarias deberían utilizar distintas contraseñas.

d. Se desaconseja la utilización de las características de recuerdo de contraseñas que implementan algunos navegadores.

e. Las contraseñas deberían ser fáciles de recordar, debiendo presentar, en todo caso, las garantías necesarias.[1]

f. No deberían proporcionarse las credenciales de usuario cuando en el acceso a algún servicio mediante un navegador se produce un error relacionado con la validez de un certificado.

Política aprobada por el Equipo Rectoral de la Universidad de Oviedo, en Oviedo/Uviéu el día 17 de Julio de 2018

[1] Según recomendaciones del Centro Criptológico Nacional, un mecanismo útil suelen ser los llamados acrósticos, que consisten en seleccionar un carácter de cada palabra de una frase conocida y fácilmente memorizable. Un artículo interesante al respecto es *Best practices for passwords updated after original author regrets his advice* (https://www.theverge.com/platform/amp/2017/8/7/16107966/)