UNIVERSIDAD D SEVILLA

Políticas de Seguridad

Política de contraseñas de la Universidad de Sevilla

Índice

1. Introducción

La Universidad de Sevilla (en adelante, US) establece una Política de Contraseñas acorde a los requisitos legales vigentes que debe ser aplicada a cualquier mecanismo de autentificación que utilicen los miembros de la Comunidad Universitaria para acceder a los Servicios de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) de la US.

Concretamente se aplica al Usuario Virtual de la Universidad de Sevilla (en adelante, UVUS), que es el mecanismo de acceso a los servicios más extendido, así como a los usuarios locales de las aplicaciones informáticas que no utilizan el UVUS como medio de autenticación y a los usuarios externos que acceden a la Red Informática de la Universidad de Sevilla (RIUS) a través de Redes Privadas Virtuales (VPN).

2. Ámbito de aplicación

La presente política es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, esté vinculado la US, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la US y tengan que utilizar contraseñas para acceder a ellos.

3. Vigencia

Esta política ha sido aprobada por la Comisión de Seguridad de la US con fecha 16 de diciembre de 2016, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la US pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en ella.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la US. Las versiones anteriores quedan anuladas por la última versión de esta política.

4. Revisión y evaluación

La gestión de esta política corresponde al Servicio de Informática y Comunicaciones (en adelante, SIC) de la US, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario, para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Cuando las circunstancias así lo aconsejen se revisará la presente política, que se someterá, de haber modificaciones, a la aprobación de la Comisión de Seguridad de la US.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica y organización general o cualquier otra cuestión que pueda provocarla.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. Referencias

La presente política se fundamenta en la legislación vigente en materia de seguridad de las Tecnologías de la Información y las Comunicaciones de ámbito europeo, estatal y autonómico, así como en las normas y procedimientos internos que resulten de aplicación a la Universidad en el marco de la Política de Seguridad de la Información.

6. Desarrollo de la política

Se aplica a todos los usuarios de los Servicios TIC de la Universidad de Sevilla la siguiente política de contraseñas:

- La longitud de la contraseña debe ser como mínimo de 8 caracteres, si bien se recomienda usar contraseñas más largas.

- La contraseña debe contener al menos 4 caracteres alfabéticos de los cuales serán, al menos, dos letras mayúsculas y dos minúsculas.
- La contraseña debe contener al menos 2 caracteres numéricos.
- El número máximo de repeticiones de caracteres adyacentes de la contraseña será 4.
- El número máximo de caracteres numéricos en secuencia de la contraseña será 4.
- La contraseña no podrá contener el nombre o apellido del usuario, ni el documento de identidad del mismo o su UVUS.
- No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.
- Guardar la información de contraseñas en un lugar seguro.
- Cambiar la contraseña al menos una vez al año.
- No utilizar para generar la contraseña palabras o nombres comunes que puedan figurar en diccionarios.
- No se podrán utilizar las tres últimas contraseñas empleadas.

Además de la anterior política de contraseñas aplicada a los UVUS, el usuario podrá observar las siguientes recomendaciones:

- Modificar la contraseña que le entreguen antes de hacer uso de ella aunque no esté obligado a hacerlo.
- Tener al menos un símbolo (cualquier otro carácter que no sea alfabético o numérico: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).

7. Responsabilidades

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC podrá proceder al bloqueo temporal o indefinido del usuario dependiendo de la gravedad y reiteración del incidente, siendo responsable el usuario titular.

Apéndice: Lenguaje de género

Esta política ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.

ANEXO: Acrónimos y glosario de términos

CCN-Cert

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

RedIris

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

TIC

Tecnologías de la Información y las Comunicaciones. Dispositivos que permiten trabajar el ciclo de vida completo de la información, es decir, crear, almacenar, tratar, enviar o borrar información.

UVUS

Usuario Virtual de la Universidad de Sevilla.

VPN

Virtual Private Network (Red Privada Virtual) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que los ordenadores que usan esta tecnología envíen y reciban datos sobre redes públicas con toda la funcionalidad, seguridad y políticas de gestión de una red privada.