Normativa de uso y creación de contraseñas

Índice

1. OBJETIVO

El objetivo de la presente normativa 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 de la UPV/EHU.

La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

2. ÁMBITO DE APLICACIÓN

Esta Norma es de aplicación a todo el ámbito de actuación de la UPV/EHU, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la universidad. La presente Norma será de obligado cumplimiento para todas las personas usuarias de manera permanente o eventual, que utilicen los servicios de la UPV/EHU, incluyendo el personal de organizaciones externas cuando sean personas usuarias o posean acceso a los Sistemas de Información de la UPV/EHU.

La presente Normativa ha sido aprobada por el Comité de Seguridad TIC de la UPV/EHU, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la universidad pone a disposición de las personas usuarias para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

3. NORMATIVA

3.1 USO DE CONTRASEÑAS

Con carácter general, todas las aplicaciones y sistemas informáticos de la UPV/EHU estarán dotados de mecanismos destinados a la identificación de forma inequívoca e individualizada de las personas que están autorizadas a acceder a ellos. Este requisito descarta toda posibilidad de utilización de identificativos de grupo o identificadores genéricos en los Sistemas de Información de la UPV/EHU.

3.2 AUTENTICACIÓN BASADA EN CONTRASEÑAS

En la UPV/EHU se distinguen tres tipos de cuentas diferentes, cada una con sus funcionalidades especificas:

- Cuentas de Personas Usuarias
- Cuentas de aplicación (usadas por un software o una máquina)

- Cuentas de administración (usadas para la administración de equipos y/o software)

Todas ellas deberán de seguir las directrices a la hora de la generación de la contraseña que se recogen en **Procedimiento de Uso y Creación de contraseñas**. Dichas medidas deberán implementarse en los sistemas de la UPV/EHU para que se haga cumplir con las características que se detallan en él. En los sistemas, aplicaciones etc que no se pueda controlar o gestionar por configuración, deberá, así mismo, cumplir con estos requisitos y será responsabilidad final de la persona usuaria el cumplirlas.

Tanto el identificador de acceso como las contraseñas de acceso a cuentas privilegiadas de sistemas y/o aplicación serán **diferentes** de las que se utilicen como cuentas de usuario, quedando registrado por el administrador del sistema la correspondencia de cuenta/usuario.

3.3 CAMBIO O RECUPERACIÓN DE CONTRASEÑA

La gestión o cambio de las contraseñas se realizarán siguiendo los procedimientos habilitados para tal fin.

Si una persona usuaria 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 hubiere sido comprometida, de manera inmediata.

Cuando a un usuario se le cree o cambie la cuenta/contraseña, deberá cambiar esta última, permaneciendo la cuenta bloqueada hasta el cambio de esta. Como medida de seguridad, si la UPV/EHU tiene conocimiento que la contraseña de un usuario es de dominio público, ésta será cambiada y se notificará al usuario de su cambio por los cauces establecidos.

4. RESPONSABILIDADES

Todas las personas usuarias de la UPV/EHU, son responsables de conocer las normas que afectan al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

5. INCUMPLIMIENTO DE LA NORMATIVA

Cuando se determine un incumplimiento de la presente Normativa, se aplicarán las medidas correctivas y disciplinarias necesarias, debiendo informar al Comité de Seguridad de la información de la UPV/EHU, de acuerdo con la gravedad de la infracción y conforme a las normas oficiales.

6. REVISIÓN Y EVALUACIÓN

La gestión de esta Normativa de Seguridad corresponde al Comité de Seguridad TIC (Tecnologías de la Información y Comunicación) de la UPV/EHU, 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.

Si existen circunstancias que así lo aconsejen, se revisará la presente Normativa de Seguridad, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad de la UPV/EHU.

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, organización general, etc.

Será el Responsable de Seguridad de la Información el encargado de la custodia y divulgación de la versión aprobada de este documento.

7. REFERENCIAS

Internas:

- Política de Seguridad de la Información aprobado por el Consejo de Gobierno del 21 de Marzo de 2013:
  https://www.euskadi.eus/web01-bopv/es/bopv2/datos/2013/05/1302239a.shtml
- Procedimiento de Uso y Creación de Contraseñas

Externas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Documentos y Guías CCN-STIC.

Versión	Aprobada el:
1.0	20 de noviembre de 2024