Guía de uso de las contraseñas en la Universitat Politècnica de València

Aprobada por el Comité de Seguridad de la Información de la UPV el 9 de enero de 2025

Ámbito de aplicación

Esta guía está dirigida a todos los usuarios de los servicios y recursos informáticos de la Universitat Politècnica de València. Desarrolla las directrices sobre contraseñas establecida en la **Normativa de Seguridad de la UPV**, que es de cumplimiento obligatorio para todos los miembros de la institución.

Índice

1. Cómo crear contraseñas robustas y memorizables

Las contraseñas robustas son aquellas que presentan una alta resistencia a ser adivinadas por un atacante, bien mediante fuerza bruta o con heurísticos dirigidos. A continuación, se ofrecen directrices detalladas sobre cómo crear contraseñas que cumplan con los estándares de seguridad exigidos por la UPV:

Contraseñas robustas

La robustez de una contraseña depende de dos factores clave:

- **Longitud:** Cuanto más larga sea una contraseña, más difícil será adivinarla. La UPV exige que las contraseñas tengan al menos 15 caracteres, y se recomienda que sean aún más largas cuando sea posible. Según las recomendaciones de NIST, una longitud de 64 caracteres es óptima para entornos críticos.

- **Aleatoriedad:** Las contraseñas deben componerse de caracteres de diferentes categorías (mayúsculas, minúsculas, números y símbolos). Cuanto más uniforme sea la probabilidad de aparición de cada símbolo, mayor será su robustez.

Condiciones mínimas para las contraseñas en la UPV:

- Al menos 15 caracteres.
- Utilizar caracteres de al menos tres de los siguientes grupos: letras minúsculas, letras mayúsculas, números y símbolos de puntuación.
- De estos, es obligatorio que al menos incluya un símbolo de puntuación.
- No se debe derivar de palabras del diccionario
- No se debe derivar del nombre del usuario o de algún pariente cercano.
- No debe provenir de información personal (como por ejemplo el número de teléfono, DNI, dirección, fecha de nacimiento), ni del usuario ni de ningún pariente cercano.
- Evitar repetir caracteres de forma consecutiva (máximo 2 iguales seguidos).
- No debe contener espacios en blanco.

Consejo adicional: Si se prevé el uso de teclados internacionales, es importante evitar caracteres específicos de un idioma, como la «ñ» o el símbolo «€», ya que pueden no estar disponibles en los teclados de otros países.

Contraseñas memorizables

Aunque es recomendable el uso de un gestor de contraseñas, a menudo es necesario memorizar contraseñas que usamos de manera recurrente (por ejemplo, la contraseña de *login* del ordenador o la contraseña del propio gestor de contraseñas).

Estrategias para crear contraseñas memorizables:

1. Crear una frase personal larga, fácil de recordar.
2. Aplicar un método de transformación personal a esa frase para generar una contraseña segura.

Ejemplos de frases:

- «Los acertijos matemáticos son tan antiguos como la propia humanidad»
- «Murciélago o colúmpiame contienen todas las vocales»
- «No quiero recordar más contraseñas, pero me obligan!»

Ejemplos de transformaciones:

- Tomar la primera y última letra de cada palabra de una frase.
- Seleccionar las primeras dos letras de cada palabra.
- Intercalar símbolos entre letras o palabras.

Es importante diseñar nuestras propias transformaciones.

Una vez se adquiere un poco de práctica, es muy fácil utilizar este tipo de contraseñas ya que solo es necesario pensar la frase mientras vamos aplicando la transformación.

Recomendamos la lectura de este breve documento del INCIBE con muchos ejemplos:

https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras

2. Uso adecuado de las contraseñas

A parte de tener contraseñas robustas y memorizables, hay que cuidar la forma en las que las utilizamos, es por ello por lo que:

- **No reutilizar contraseñas:** Cada servicio debe tener una contraseña única. Evita usar la misma contraseña para cuentas de la UPV y servicios externos (por ejemplo, redes sociales o servicios de correo electrónico externos). Se han dado muchos casos de robos de contraseñas en servicios de poca importancia (y normalmente poco asegurados), que luego se han utilizado con éxito para hacer ataques importantes.
- **Nunca compartir contraseñas con otras personas:** Compartir una contraseña compromete el control y la seguridad sobre la misma. A parte de revelar la contraseña puede que estés dando información sobre la estrategia que utilizas para crear contraseñas.
- **Comprobar la seguridad del entorno:** Al ingresar una contraseña, asegúrate de que el entorno es seguro, evitando que otras personas puedan ver lo que escribes, o que haya cámaras grabando. Esto es especialmente importante cuando lo haces en el móvil, ya que suele utilizarse en lugares en los que se está más expuesto que cuando usamos nuestro ordenador personal.

3. Renovación periódica de las contraseñas

Todas las contraseñas en la UPV deben renovarse, al menos, una vez cada 12 meses. Esta periodicidad equilibra la usabilidad con la seguridad. Se recomienda un cambio más frecuente si hay indicios de que una contraseña pueda haber sido comprometida.

El cambio periódico de contraseñas limita mucho el tiempo que disponen los atacantes para descifrarla, en caso de haberla obtenido de un servidor, y utilizarla. Recordemos que, en muchas

ocasiones, los que roban las contraseñas no solo los mismos que las utilizan, sino que las ponen a la venta en la *deep web*. Todo este proceso de descifrado y venta puede requerir meses o años.

Precaución ante intentos de phishing: Es frecuente que los atacantes utilicen correos electrónicos falsos para solicitar cambios de contraseña. Recuerda que los correos legítimos de la UPV no incluirán enlaces directos para el cambio de la contraseña.

4. Importancia de las contraseñas

En el ámbito de la informática, las personas somos el eslabón más débil. En especial, el uso de contraseñas débiles es todavía un gran problema de seguridad. Aunque existen más formas de autenticarse, y ha habido muchos intentos de substituir las contraseñas por otro mecanismo que sea más fácil de usar, no parece que en el corto plazo se vaya a conseguir.

Actualmente existen tres formas para autenticar a una persona:

1. Algo que **sabes** (se guarda en nuestra memoria): contraseñas.
2. Algo **tienes** (un objeto que solemos llevar con nosotros), y que siempre debe ser un segundo dispositivo distinto al equipo informático desde el que estamos trabajando. Habitualmente es el móvil (llamada telefónica, SMS, etc.) o una aplicación (por ejemplo, las apps de autenticación de Microsoft y Google, entre otras).
3. Algo que **eres** (una característica única y difícil de replicar de nuestro cuerpo): huella dactilar, reconocimiento facial, etc.

La autenticación biométrica (algo que eres) es muy cómoda de utilizar, pero tiene el gran inconveniente de ser de un solo uso. Esto es, si nos roban las huellas y fabrican un dedo de goma con nuestras huellas, ya nunca podremos volver a utilizarlas para autenticarnos de forma segura. Por otra parte, los objetos que podemos utilizar para autenticarnos (algo que tienes) pueden perderse o estropearse. Por tanto, a fecha de hoy, las contraseñas (algo que sabes) son el mecanismo más robusto de autenticación, siempre que sean contraseñas robustas y memorizables.

5. Gestores de contraseñas

Dado el elevado número de contraseñas que manejamos a diario, se recomienda encarecidamente el uso de gestores de contraseñas. Estos permiten almacenar contraseñas complejas y únicas para cada servicio, sin necesidad de recordarlas todas.
Un buen gestor de contraseñas no impone límites de longitud, lo que permite generar contraseñas más largas y aleatorias para cada servicio.

Consulta la guía del CSIRT de la Generalitat Valenciana para más detalles sobre la elección y uso adecuado de un gestor de contraseñas: Guía CSIRT.

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Bibliografía:

- Guía de uso de gestores de contraseñas – CSIRT GVA
- Directrices NIST sobre contraseñas 2024
- NIST SP 800-63B: Recomendaciones sobre autenticación digital
- NIST SP 800-63B Actualización 2024