A SENSU CONTRARIO
RESPOSTAS XURÍDICAS

SEGURIDAD DE LAS CONTRASEÑAS

Para garantizar la seguridad en el tratamiento de los datos personales, es necesario que las contraseñas que se empleen en todo el proceso, tanto las de acceso a los equipos en los que se realiza como en la autenticación de los servicios *online* que los tratan (almacenan, procesan o transmiten información con datos personales) o en el cifrado de medios de soporte que los contienen (discos duros, memorias usb, etc.) se gestionen de forma correcta.

Actualmente las capacidades de cómputo disponibles permiten que cualquier atacante con los conocimientos y los equipos adecuados descifre la mayoría de claves simples que se suelen utilizar.

Os facilitamos algunas normas básicas para gestionar las contraseñas de forma segura:

- No se deben usar claves predecibles, especialmente cortas (menos de 15 caracteres) o únicamente numéricas, por ejemplo: *contraseña*, *12345*, *mellamopepa*, etc.
- No se debe usar la misma contraseña en varios equipos o servicios; **una contraseña para cada cosa**.
- Una contraseña es como un cepillo de dientes: **no la compartas**.
- No deben almacenarse las contraseñas en lugares visibles como libretas, *post-it's*, en documentos de texto en el Escritorio del equipo o en tu móvil, sobre la carcasa de tu disco duro, escrito en la parte inferior del teclado, etc.
- Cambiar periódicamente las contraseñas (al menos una vez cada 3 meses).

- En lo posible, **memoriza las contraseñas**. Existen diversos métodos para crear claves robustas memorizables partiendo de frases relevantes para ti y que posteriormente modificas con ciertas reglas.
- Si manejamos un gran número de contraseñas es recomendable emplear gestores especializados.
- Almacenar contraseñas en el navegador no es demasiado seguro. Si lo haces debes tener una llave maestra para bloquear la base de datos que las almacena; procura que esta sea una clave realmente robusta.
- Si vas a emplear algún gestor o el navegador, puedes utilizar métodos generadores de contraseñas aleatorias que incluyan caracteres alfanuméricos, caracteres especiales, espacios, mayúsculas, por ejemplo: *8M<@h_(es\ S#oGBy7(.}h#;>&e+V3[I~@\PE+*
- En los servicios que lo permitan es siempre buena idea emplear la verificación en dos pasos (A2F).

- Recomendaciones de la EFF para el uso de contraseñas
- Fichero con 1400 millones de contraseñas a disponibilidad de cualquiera
- Método seguro para generar contraseñas robustas memorizables
- 10 trucos nemotécnicos para crear contraseñas seguras y fáciles de recordar
- Diceware: método de generación de contraseñas seguras (VIDEO)
- Organiza tus cuentas y contraseñas con el gestor de contraseñas KeePass (VIDEO)
- ¿Qué es la verificación en dos pasos? (VIDEO)
- Extensión PassProtect para Chrome