Contraseñas - Su importancia y tips

Las contraseñas (junto al nombre de usuario u otro dato como su mail, que lo identifican) siguen siendo una de las formas más comunes de autenticación (soy quien digo ser). Por eso es tan importante elegirlas bien y ser cuidadosos en su uso.
A continuación, se detallan las características fundamentales de una contraseña segura hoy en día:

1. *Longitud sobre Complejidad*

- ***Mínimo recomendado:*** *Al menos* ***12 a 16 caracteres****. La longitud es actualmente el factor más crítico para resistir ataques.*
- ***Frases de contraseña (Passphrases):*** *En lugar de una palabra difícil (como* `P@$$w0rd!`*), utilizá una combinación de varias palabras aleatorias (ej.* `CaballoAzulTecladoSol`*). Son mucho más largas, más difíciles de descifrar para las máquinas y más fáciles de recordar para las personas.*

2. *Conposición sobre Variedad*

Aunque la longitud manda, sigue siendo una buena práctica incluir una mezcla de:
- ***Mayúsculas y minúsculas.***
- ***Números y símbolos*** *(como* `!`*, @, #, $).*
- ***Espacios:*** *Las normativas actuales (como las del NIST) recomiendan que los sistemas permitan el uso de espacios para crear frases más naturales.*

3. *Lo que DEBES evitar*

- ***Información personal:*** *No uses nombres de mascotas, familiares, fechas de nacimiento o equipos de fútbol.*
- ***Patrones predecibles:*** *Evita secuencias como* `123456`*,* `qwerty` *o sustituciones simples como cambiar una 'a' por un '@' (los atacantes ya conocen estos trucos).*
- ***Reutilización:*** *Nunca uses la misma contraseña en más de una cuenta. Si un sitio sufre una brecha, todas tus cuentas estarán en peligro.*

4. *Nuevas Reglas de Gestión (Estándares 2026)*

- ***No cambies tu contraseña por obligación:*** *A menos que sospeches que ha sido robada, los expertos ya no recomiendan cambios periódicos (cada 3 meses, por ejemplo), ya que esto suele llevar a contraseñas más débiles.*
- ***Adiós a las preguntas de seguridad:*** *Las respuestas a "nombre de tu primera mascota" son fáciles de encontrar en redes sociales. Evítalas o usa respuestas aleatorias.*
- ***Usa un Gestor de Contraseñas:*** *Es la única forma segura de tener contraseñas únicas y largas para cada sitio sin tener que memorizarlas todas.*

5. *El complemento indispensable: MFA*

Incluso la mejor contraseña puede ser robada. Por ello, es vital activar la ***Autenticación de Múltiples Factores (MFA)*** *o verificación en dos pasos. Prioriza métodos resistentes al phishing, como aplicaciones de autenticación o llaves físicas, sobre los códigos por SMS*