**Requerimientos de seguridad para contraseñas**

A continuación, se resumen las políticas de seguridad establecidas para contraseñas.

Estos lineamientos están basados en la publicación “NIST Special Publication 800-63B”; concretamente, en los apartados “5.1.1.1 Memorized Secret Authenticators” y “5.1.1.2 Memorized Secret Verifiers”.

* Longitud mínima: 8 caracteres; máxima, 32.
* Regla de composición: deberán incluir al menos una letra minúscula [a-z] y una letra mayúscula [A-Z], al menos un número [0-9] y al menos uno de los siguientes caracteres especiales: [@#$%].
* No se permitirá ningún otro carácter.
* Siguiendo las consideraciones del marco NIST, la password *no* expirará en forma arbitraria. Entendemos que una práctica de rotación induce a los usuarios a escoger passwords menos seguras y, en definitiva, la rotación se basa en patrones simples y predecibles.
* Toda nueva password será comparada contra un diccionario con las “10.000” passwords más comúnmente utilizadas, no permitiéndose el uso de aquellas passwords allí listadas.

**Referencias:**

NIST Special Publication 800-63B  
<https://pages.nist.gov/800-63-3/sp800-63b.html>

OWASP Top 10 – 2017  
<https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>

Top 10.000 de contraseñas más comunes  
<https://github.com/danielmiessler/SecLists/tree/master/Passwords>