

		Origen: MyGes
<b>Política de gestión de contraseñas</b>		
Fecha: 20 agosto 2025	Información Pública: Carácter Interno	N.º revisión: 03

La presente **Política de Gestión de Contraseñas** se alinea con los siguientes marcos normativos y estándares internacionales:

- **PCI DSS v4.0:** Cumplimiento de los requisitos relacionados con la identificación y autenticación de usuarios (Requisitos 8.2, 8.3 y 8.4).
- **ISO/IEC 27001:2022:** En coherencia con los controles del Anexo A relativos a la gestión de identidades y credenciales de acceso (A.5.17 Control de acceso basado en privilegios, A.5.18 Gestión de información de autenticación secreta de usuarios).

Para dar cumplimiento a lo establecido en esta política, deberán observarse las siguientes indicaciones relativas a la composición de las contraseñas:

- Longitud mínima: **doce (12) caracteres.**
- Debe incluir, al menos, un carácter de cada una de las siguientes categorías:
  - Letra **MAYÚSCULA** (A – Z).
  - Letra **minúscula** (a – z).
  - **Número** (0 – 9).
  - **Carácter especial**, pudiendo ser cualquiera de los siguientes:

, ; . : - \_ \$ % & / + = ) ( < > \*

Además de los requisitos de complejidad establecidos para la creación de contraseñas, se deberán cumplir las siguientes normas de uso y administración:

- **No contener el nombre completo** de ninguna persona, **ni** la cuenta completa de la **dirección de correo electrónico.**
- **No considerar las cinco (5) últimas contraseñas** ya usadas anteriormente.
- **Número máximo de Intentos fallidos: cinco (5).**
- **Tiempo de bloqueo:** se mantendrá **hasta** que un **superior** jerárquico **autorice el desbloqueo.**
- Obligación de **cambiar la contraseña** en el **primer inicio de sesión.**
- **Caducidad** de la contraseña: **noventa (90) días**