



Las contraseñas deben ser **GESTIONADAS DE FORMA SEGURA EN TODO SU CICLO DE VIDA**: desde su creación, pasando por su almacenamiento y terminando por la destrucción.



Los mecanismos de **DOBLE FACTOR DE AUTENTICACIÓN "2FA" AUMENTAN LA SEGURIDAD DE LA CUENTA**, son especialmente indicados para acceder a información sensible o servicios críticos.



Los **GESTORES DE CONTRASEÑAS** son un tipo de herramienta que **AYUDA A SU ADMINISTRACIÓN DE FORMA SEGURA**, especialmente útiles cuando el número de contraseñas es elevado.



Deben cumplir una serie de requisitos para que sean **ROBUSTAS** como **TAMAÑO, TIPOS DE CARACTERES** a incluir o su **PERIODO DE VALIDEZ**.



Las contraseñas son un tipo de **INFORMACIÓN PERSONAL E INTRANSFERIBLE**, nadie a excepción de su propietario debe conocerlas.



Es recomendable utilizar **UNA CONTRASEÑA PARA CADA SERVICIO**, de esta manera en caso de robo solamente se comprometerá un servicio y no todos.



Cambiar las **CONTRASEÑAS POR DEFECTO POR OTRAS CONSIDERADAS ROBUSTAS** siempre es recomendable.

