

¿QUÉ ES LA AUTENTICACIÓN SIN CONTRASEÑAS?

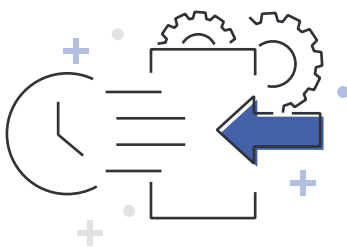
La autenticación sin contraseñas reemplaza el uso de contraseñas convencionales por otros **métodos de autenticación más seguros y robustos**. Huella digital, enlaces mágicos y tokens secretos son algunos de los ejemplos que las empresas están empezando a implementar. Estos sistemas alternativos aportan beneficios tanto a la empresa como a los usuarios.

OBJETIVOS DE LA AUTENTICACIÓN SIN CONTRASEÑAS

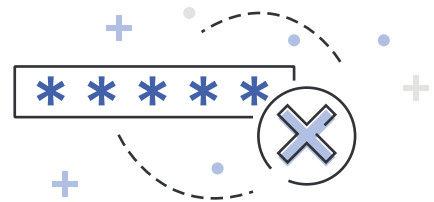


- ⊕ Proporcionar una seguridad mucho más sólida y robusta, debido a la temporalidad de los recursos de autenticación o la dificultad de replicación de los mismos.
- ⊕ Utilización en diversos escenarios sin distinción de la plataforma sobre la que se despliegue la aplicación o sistema.
- ⊕ Ofrecer una experiencia más amigable para el usuario respecto a los servicios o aplicaciones, ya que el usuario no tiene que recordar una contraseña. Verificará su identidad mediante datos biométricos, códigos o enlaces.

BENEFICIOS DE LA AUTENTICACIÓN SIN CONTRASEÑAS



Facilita el inicio de sesiones a servicios y aplicaciones de forma más rápida. Agiliza los trámites aumentando la productividad y reduciendo los costes de soporte técnico por actividades de restablecimiento de contraseñas.



No requiere esfuerzo en el mantenimiento de contraseñas. Se evita tener que recordarlas y, por consiguiente, olvidarlas o perderlas.



Servicio multiplataforma, es decir, no está restringido a un tipo determinado de dispositivo o servicio.



Protección contra amenazas como pueden ser los ataques de phishing, los de fuerza bruta o los de diccionario.



Cyberzaintza, la Agencia Vasca de Ciberseguridad, pone a disposición de cualquier organización su "**Catálogo de ciberseguridad**", donde encontrará a los proveedores especialistas en la autenticación sin contraseñas.