Publicado en Ciudad de México el 13/10/2023

# [Passwordless, un cambio de paradigma en la autenticación](http://www.notasdeprensa.es)

## Las tecnologías sin contraseña o "passwordless" son una poderosa forma de autenticación en la era digital pero su adopción aún no es generalizada. La contraseña tradicional ha sido durante mucho tiempo la llave para acceder a servicios digitales; no obstante, a menudo se convierte en un problema para los usuarios y en el eslabón más débil de una estrategia de seguridad. Erik Moreno, director de Ciberseguridad en Minsait, comparte por qué utilizar passwordless es un cambio de paradigma y mentalidad

 Las tecnologías passwordless (sin contraseña) representan una nueva y poderosa forma de abordar la autenticación en la era digital. A pesar de haber estado presente en el mercado durante varios años, su adopción aún no es generalizada. La contraseña tradicional ha sido durante mucho tiempo el pilar fundamental para acceder a servicios digitales, redes sociales, banca en línea, sistemas empresariales y correo electrónico, entre otros. No obstante, las contraseñas a menudo se convierten en el eslabón más débil de una estrategia de seguridad. En entornos corporativos, los administradores de sistemas aconsejan la creación de contraseñas robustas, lo que implica la combinación de caracteres especiales, números y letras mayúsculas y minúsculas en una cadena larga y compleja. Esto, lamentablemente, dificulta que los usuarios las recuerden y, en consecuencia, opten por unas más simples y fáciles de recordar. También es sabido que las personas tienden a reutilizar sus contraseñas, lo que debilita considerablemente la cadena de protección. Además, existen sistemas y servicios que no demandan el uso de contraseñas robustas, lo que las hace muy fáciles de deducir. Los ciberdelincuentes han utilizado distintas técnicas para hacerse con millones de contraseñas. Una de ellas es el ataque de diccionario, que se emplea para intentar obtener credenciales de acceso a sistemas, cuentas en línea o dispositivos electrónicos, el cual se basa en la suposición de que las contraseñas utilizadas son palabras comunes o combinaciones de palabras que se encuentran en un diccionario, en lugar de ser contraseñas complicadas y únicas. Otra es el ataque de fuerza bruta, que consiste en hacer una prueba repetitiva de todas las combinaciones posibles de caracteres hasta dar con la contraseña correcta. A diferencia de los ataques de diccionario, los ataques de fuerza bruta no se basan en suposiciones específicas sobre las contraseñas, sino que prueban sistemáticamente todas las combinaciones posibles. Una mejor experiencia con seguridadPara abordar estos riesgos, se han utilizado gestores de contraseñas que sugieren patrones específicos basados en políticas de seguridad definidas y que almacenan contraseñas de forma segura. Sin embargo, esta solución no ha logrado eliminar el uso de contraseñas débiles. Por otro lado, la autenticación multifactor (MFA) ha registrado una adopción importante, gracias a que combina algo que  el usuario sabe (contraseña) con algo que tiene  (teléfono móvil o token) o algo que es (huella digital, iris, rostro). Aunque más segura, MFA aún implica el uso de contraseñas. Entonces, ¿cómo es posible mejorar la seguridad y la experiencia del usuario sin depender de estas claves? La respuesta se encuentra en la tecnología "passwordless", que busca eliminar completamente el uso de contraseñas tradicionales. La autenticación passwordless es un enfoque de seguridad que busca prescindir de contraseñas tradicionales. Contrario a depender de contraseñas que pueden ser vulnerables a ataques de fuerza bruta, ataques de diccionario o phishing, passwordless utiliza métodos de autenticación más robustos y convenientes como la autenticación biométrica, por token, por correo electrónico o SMS, por aplicaciones móviles y por clave pública. Este tipo de autenticación se basa en la criptografía simétrica, por lo que utiliza una clave pública y una privada. Si bien pudiera sonar complicado, este proceso es bastante sencillo, y lo es porque parte de que el usuario final no va a tener que conocer, ni memorizar una clave privada. Esta estará almacenada de forma segura en un dispositivo de confianza, como su teléfono inteligente. Otro de esos dispositivos de confianza puede ser una llave de seguridad USB, que es un dispositivo físico que se utiliza para proporcionar una capa adicional de seguridad en el proceso de autenticación en línea. Su principal función es ayudar a proteger cuentas y sistemas de acceso no autorizado al requerir que el usuario tenga físicamente la llave USB y la conecte al dispositivo en el que está intentando iniciar sesión. La ventaja de usar tecnologías sin contraseña como estas es que no tienen que usarse contraseñas complicadas; bastará con capturar un número de cuatro dígitos (PIN) fácil de recordar, autenticarse mediante la huella digital o rostro. La clave radicará en el dispositivo de confianza, sin el cual no se podrá tener acceso a servicios, sistemas o aplicaciones. Mayor simplicidadLos beneficios de esta tecnología passwordless son evidentes: No emplear más contraseñas. Ya no es necesario recordar contraseñas complicadas. Reducción del riesgo. El riesgo de ataques se reduce significativamente, ya que los ciberdelincuentes no pueden acceder sin el dispositivo de confianza. Simplicidad. El usuario no tendrá que recordar contraseñas complejas, ni las tendrá que reutilizar para diferentes servicios o sistemas. Con estos tres beneficios, los flujos de trabajo serán mucho más ágiles. Utilizar el reconocimiento de huellas digitales, el iris o el rosto se convierte en uno de los puntos más robustos de la ciberseguridad. Dejar de lado las contraseñas no es una idea nueva. Aún hay mucho que avanzar en su uso masivo y concientizar al usuario final de su efectividad. En una organización, el usuario es la primera línea de defensa y es vital fortalecerlo mediante un principio de ciberseguridad que es la comunicación y capacitación. En esta tarea deben participar organizaciones privadas, los gobiernos a través de distintos niveles de educación y la familia. En conclusión, passwordless no es una tecnología, no es una arquitectura; es un cambio de paradigmas y mentalidad, en el que debe hacerse consciente al usuario final de que existe una nueva forma de autenticarse de forma más confiable y conveniente. Sobre el autor:  Erik Moreno cuenta con 20 años de experiencia asesorando a organizaciones en decisiones estratégicas de seguridad, implementado mejoras operativas y tecnológicas en compañías tanto multinacionales de diversas industrias como: telecomunicaciones, energía, banca, TI, comercio electrónico y del sector gubernamental y experiencia en proyectos de seguridad nacional. Actualmente se desempeña como Director de Ciberseguridad en Minsait, una empresa de Indra en México.

**Datos de contacto:**

Gabriela Medina Guerrero

AB Estudio de Comunicación / Directora Asociada

5539663493

Nota de prensa publicada en: [https://www.mexicopress.com.mx/passwordless-un-cambio-de-paradigma-en-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Nacional Programación Software Ciberseguridad Innovación Tecnológica



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)