# Garantizar la seguridad de la autenticación móvil

## CÓMO AFRONTAR LOS PRINCIPALES RETOS Y CREAR SOLUCIONES SÓLIDAS DE AUTENTICACIÓN PARA LOS CONSUMIDORES

Las soluciones de autenticación móvil se encuentran entre las formas más seguras de implementar la autenticación multifactor (MFA), y agregan una capa demostrada de protección a las cuentas y servicios en línea de los consumidores. También son cómodos para los usuarios, porque aprovechan un dispositivo que la mayoría de la gente tiene al alcance de la mano.

Sin embargo, los métodos de autenticación móvil y firma de transacciones están cambiando rápidamente. El mercado ofrece una gran variedad de soluciones. Uno de los métodos que más se utilizan es el código seguro, conocido comúnmente como contraseña de un solo uso (OTP), que se envía por SMS a los teléfonos móviles de los clientes. Otras soluciones aprovechan tecnologías biométricas que utilizan el reconocimiento facial o de huellas dactilares.

Por desgracia, muchas de estas soluciones tienen grandes fallos de seguridad. De hecho, en investigaciones recientes se demuestra que la mayoría de las aplicaciones de autenticación móvil pueden ser violadas por malware. Las soluciones basadas en SMS son especialmente vulnerables. Por ejemplo, los intercambiadores de SIM utilizan los números de teléfono de las víctimas en sus propios dispositivos e interceptan los mensajes privados. Incluso los servicios de mensajería de texto que tienen licencia pueden utilizarse para redirigir los textos de las personas y obtener acceso a sus cuentas.

¿Qué pueden hacer las empresas para protegerse a sí mismas y a sus clientes? En este informe técnico, revisaremos lo que está en juego y desglosaremos los factores que dificultan la seguridad en la autenticación móvil. A continuación, describiremos los controles y protocolos necesarios para crear soluciones que sean seguras, perfectas y escalables.

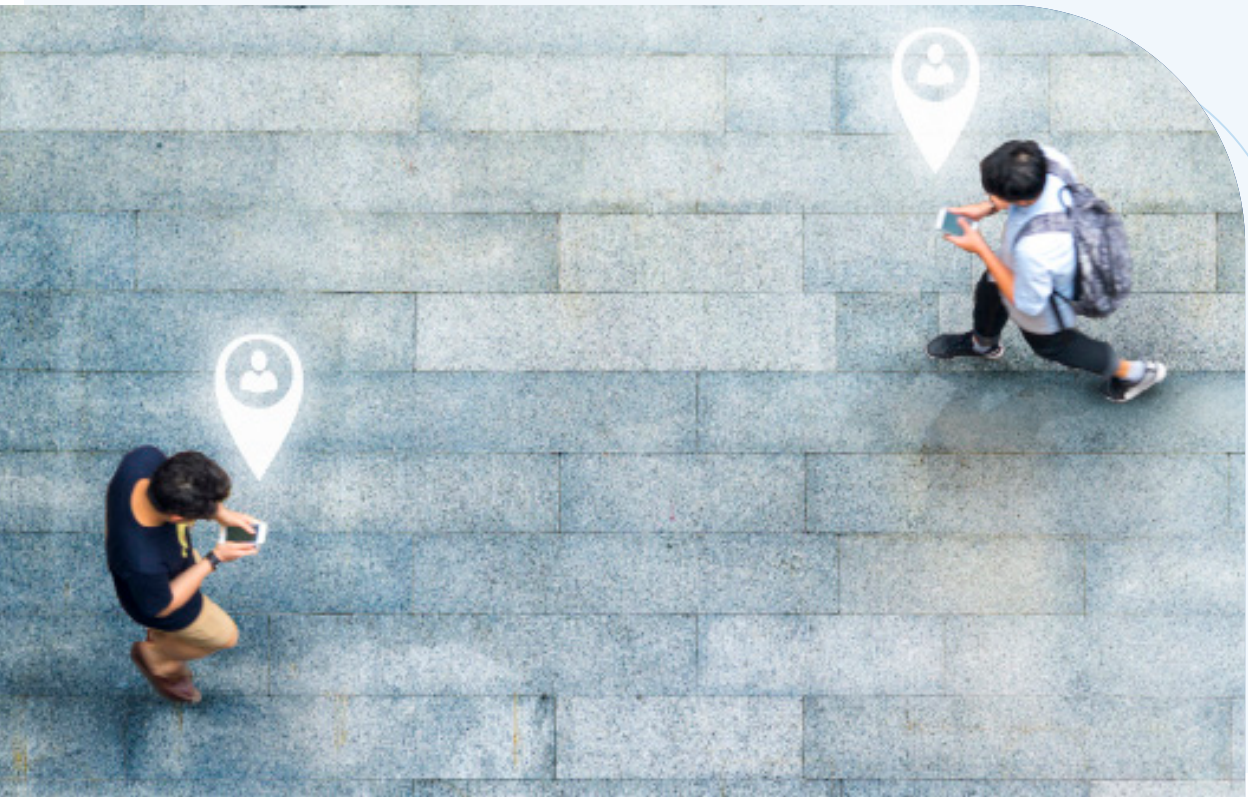
# ¿Qué hay en juego?

Las apuestas por la seguridad de la autenticación móvil nunca habían sido tan altas. El volumen de ataques se elevó a nuevos niveles a medida que aumentaba la dependencia del mundo en todo lo digital. En el 2021, ocurrió un nuevo ciberataque cada 39 segundos. El costo de la ciberdelincuencia también está llegando a cifras cada vez más alarmantes. El costo para las organizaciones fue de $1 billón en el 2020, y se espera que supere los $10 billones anuales para el 2025.

Las credenciales de usuario comprometidas siguen siendo el principal medio que utilizan los atacantes para introducirse en una organización. De hecho, las estimaciones sugieren que las credenciales robadas se utilizaron en el 61% de todos los ataques. Durante el 2020 ocurrió un ataque importante donde los atacantes construyeron una red de 16,000 dispositivos móviles virtuales y después interceptaron los OTP de SMS para robar millones de dólares de las aplicaciones de banca móvil en cuestión de días.

Mientras tanto, en la primavera del 2021, los hackers robaron las criptomonedas de unas 6000 cuentas de Coinbase después de explotar un error de autenticación multifactor que les permitió recuperar la información de las cuentas de los usuarios, introduciendo el OTP que se envió mediante SMS.

Los daños son desalentadores, pero no menos que la creencia de que podrían haberse evitado con una mayor seguridad en la autenticación.



# Aspectos básicos de la seguridad en la autenticación móvil

La autenticación móvil permite a los usuarios aprovechar funciones específicas en los dispositivos móviles para verificar sus identidades y obtener acceso a una aplicación o llevar a cabo una transacción. La idea de convertir el teléfono inteligente en un autenticador siempre presente y fácil de usar tiene un atractivo obvio. Lamentablemente, proteger el proceso de autenticación móvil no es una tarea sencilla.

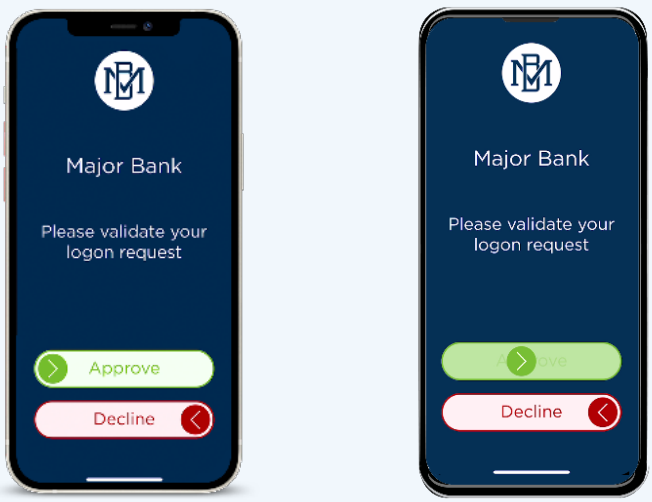
El proyecto Open Web Application Security Project (OWASP), una fundación sin fines de lucro que trabaja para mejorar la seguridad del software, ha establecido estándares de seguridad básicos. Pero, a diferencia de las aplicaciones web, las aplicaciones móviles ofrecen a los desarrolladores muchas posibilidades más en términos del sitio donde almacenan los datos y cómo aprovechan las funciones de seguridad integradas en un dispositivo para autenticar a sus usuarios. Eso significa que las pequeñas opciones de diseño pueden tener grandes implicaciones en la seguridad general de la solución.

## EL CASO DE LA AUTENTICACIÓN PUSH

La verificación mediante SMS se ha convertido en algo omnipresente para la mayoría de las personas. Fue el método de autenticación líder entre las instituciones financieras que HID Global encuestó en 2021, y el Instituto Ponemon estima que es utilizado por aproximadamente un tercio de los usuarios móviles, a pesar de sufrir importantes riesgos de seguridad.

Por el contrario, la autenticación basada en notificaciones push ofrece a las organizaciones una combinación más potente de seguridad, flexibilidad y facilidad de uso. Las notificaciones push utilizan técnicas criptográficas para vincular un dispositivo específico a la identidad de su propietario, lo cual hace imposible que los atacantes se hagan pasar por alguien si no tienen acceso físico al dispositivo. Es más seguro que la autenticación por SMS, ya que no requiere que los proveedores de servicios envíen información confidencial a los dispositivos de los clientes mediante una red que no es segura. Las claves pueden protegerse aún más cuando están unidas de forma segura al dispositivo mediante su elemento seguro, algo que veremos en las secciones posteriores de este artículo.

Además, la experiencia del usuario de las notificaciones push es más sencilla que en los sistemas SMS. Cuando aparecen notificaciones push en los teléfonos de los usuarios, solo tienen que validar la solicitud mediante una elección binaria para "Aprobar" o "Rechazar", en vez de crear una referencia y volver a escribir un OTP que recibieron por SMS.



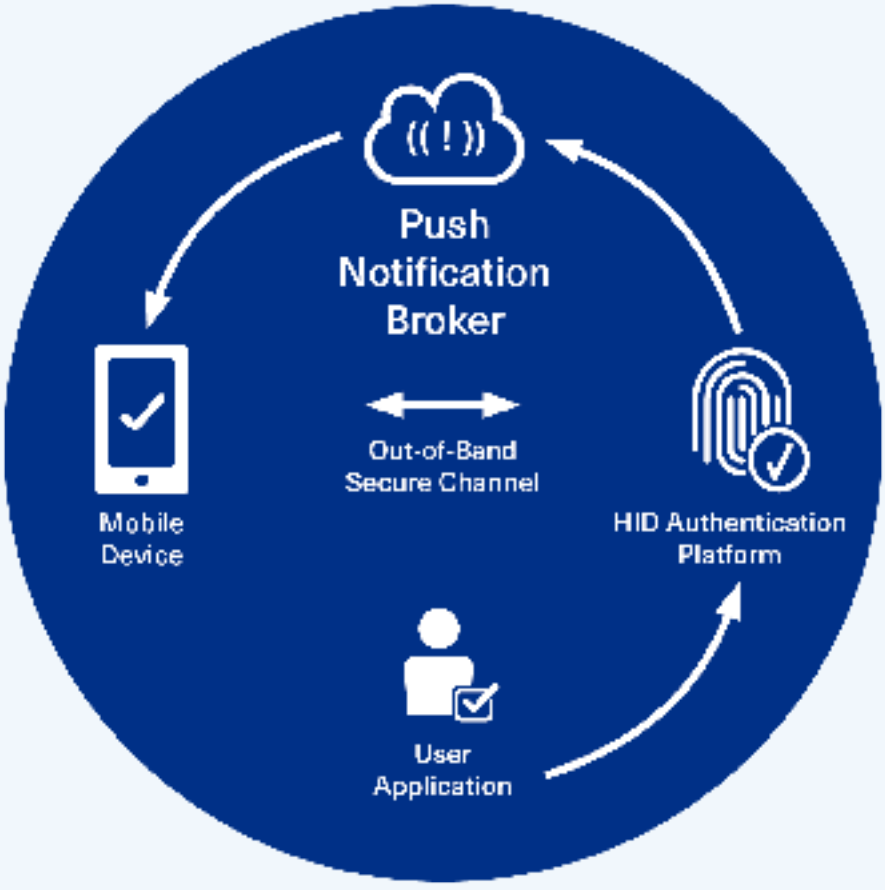

*Ejemplo de una solución HID Approve personalizada con deslizamiento para la autenticación*

## PROTECCIÓN DE TODO EL PROCESO DE AUTENTICACIÓN

Por lo general, los usuarios ven una parte muy pequeña del proceso de autenticación, porque la parte más grande ocurre en segundo plano. El ciclo de vida completo de la autenticación móvil abarca:

- Registro (y reconocimiento) del dispositivo del usuario
- Proporción de credenciales seguras al usuario
- Protección de las credenciales del usuario
- Protección de las comunicaciones entre el usuario, la aplicación y los servidores en el backend
- Protección de las solicitudes de datos confidenciales que se efectúan mientras la app de su empresa está en funcionamiento
- Mantener la seguridad durante todo el ciclo de vida del cliente
- Prevención de ataques de fuerza bruta

Hay desafíos en cada paso. En la siguiente sección, profundizaremos en estos desafíos y revisaremos soluciones específicas para resolverlos.



# Principales retos para la seguridad de la

Hay muchos factores que dificultan la seguridad de la autenticación móvil, desde la selección de las técnicas más eficaces hasta su integración en los sistemas de seguridad más amplios de su organización. En las páginas siguientes, revisaremos los ocho desafíos principales y describiremos cómo las soluciones de mayor calidad abordan estos problemas para proteger los datos y evitar ataques.

## 1. AUTENTICACIÓN DE LOS DISPOSITIVOS DEL USUARIO

**El desafío:** Una de las mejores formas de autenticar la identidad digital de alguien es reconocer cuándo utiliza su dispositivo. De lo contrario, los atacantes pueden hacerse pasar por el usuario y transferir sus datos a un clon real o virtual que es difícil de distinguir del real.

**Cómo se resuelve:** La tecnología anticlonación garantiza la detención de cualquier persona que intente acceder mediante un dispositivo clonado.

Las técnicas anticlonación más seguras se basan en el elemento seguro que se envía en casi todos los teléfonos inteligentes modernos. En el caso de iOS, se trata del Secure Enclave. En el caso de los dispositivos Android, consiste en el Trusted Execution Environment o TEE. Las computadoras portátiles cuentan con un módulo similar conocido como Trusted Platform Module (TPM). No importa cuál sea su nombre, aprovechar el elemento seguro del dispositivo permite que las soluciones de autenticación aprovechen al máximo las protecciones de seguridad de hardware integradas.

Pero eso no es todo. Las soluciones de autenticación más poderosas contienen varias capas de protección criptográfica para detener a los posibles clonadores, protegiendo las claves individuales con una clave de dispositivo única que se genera durante el proceso de provisión inicial. Incluso si se filtra esta clave del dispositivo, el atacante no podrá acceder a ninguna de las otras claves ni hacerse pasar por el dispositivo.

HID

## 2. PROVISIÓN DE DISPOSITIVOS DEL USUARIO

**El desafío:** El proceso de provisión permite a su empresa administrar las identidades de los usuarios y proporcionar una credencial para sus dispositivos móviles. Es esencial mantener este proceso seguro y a salvo de ataques.

**Cómo se resuelve:** Algunas soluciones de autenticación móvil utilizan la criptografía de clave pública, la cual se basa en un par de claves privadas/públicas vinculadas matemáticamente, para activar los dispositivos de los usuarios. Las claves privadas de este par público/privado, generadas por el dispositivo del cliente, se consideran secretas y nunca salen del dispositivo, lo que disminuye la probabilidad de que las credenciales queden comprometidas. Esto funciona bien para la autenticación movil que puede efectuar intercambios directos con el servidor de autenticación durante las solicitudes de autenticación sin que haya intervención manual de un usuario (por ejemplo, las autentificaciones push).

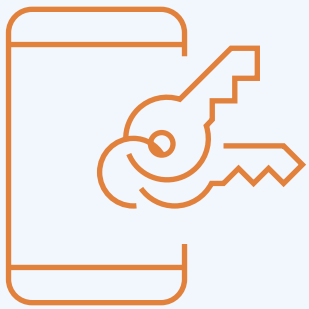
Pero en el caso de los autenticadores móviles que ofrecen una alternativa manual (como una contraseña de un solo uso), es inevitable el intercambio de material de las claves secretas entre el autenticador móvil y el servidor de autenticación. Hay dos facetas para garantizar la seguridad con respecto al intercambio del material secreto de la clave entre el cliente y el servidor:

1) La autenticación inicial del usuario para establecer un canal seguro para el intercambio de secretos

2) El propio canal seguro

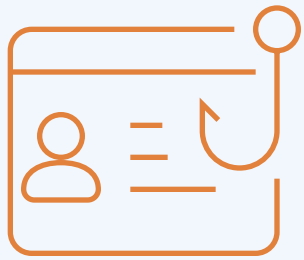
Las soluciones más seguras garantizan que la autenticación inicial sea única para cada usuario, se utilice una sola vez y caduque inmediatamente después de un registro correcto. Además, permiten que las organizaciones personalicen las reglas y configuraciones de seguridad específicas, desde la longitud y la composición alfanumérica del código de autenticación inicial hasta el número de reintentos permitidos si falla la autenticación inicial.

Otras consideraciones se relacionan con las políticas que rigen los procesos de provisión. Las mejores soluciones de autenticación permiten determinar si se expedirán o no credenciales para sistemas operativos antiguos, teléfonos desbloqueados o dispositivos que no tengan un elemento seguro. Ofrecen la posibilidad de elegir qué tipo de cifrado utilizar y facilitan la configuración de estas opciones, en vez de depender de lo que ya estableció el proveedor.



### 3. PROTECCIÓN DE LAS CREDENCIALES DEL USUARIO

**El desafío:** Las credenciales son vulnerables a una gran variedad de ataques y esquemas de phishing diferentes. Por lo tanto, se necesitan políticas sólidas para protegerlas.



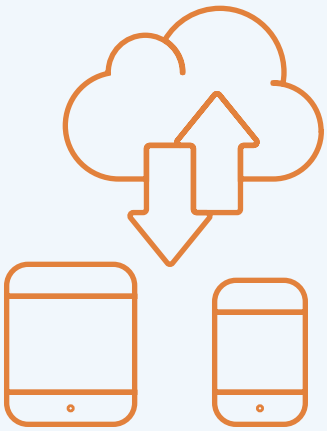
**Cómo se resuelve:** Las políticas para las contraseñas difieren entre organizaciones. Las mejores soluciones de autenticación móvil pueden adaptarse a estas diferencias, tanto si activan una notificación push inmediatamente después de introducir correctamente la contraseña como si requieren que los usuarios tomen primero medidas adicionales para autenticar su identidad, como introducir el PIN/contraseña del dispositivo o un marcador biométrico.

De hecho, la tarea de proteger las credenciales de los usuarios a menudo requiere pensar detenidamente en el contexto y la conveniencia. Las contraseñas de 15 caracteres pueden ser más seguras que un PIN de cuatro dígitos, pero también son más difíciles de recordar para las personas, y mucho más aún introducirlas en un teléfono móvil. La biometría ofrece una excelente combinación de seguridad y comodidad, y la mayoría de los dispositivos móviles ahora cuentan con capacidades biométricas integradas. Las mejores soluciones permiten a las organizaciones elegir como deben aprovecharlas y usarlas junto con cualquier otra técnica.

### 4. GARANTIZAR LAS COMUNICACIONES SEGURAS

**El desafío:** Los datos confidenciales que pasan a través de canales no seguros pueden ser interceptados. Por lo tanto, la comunicación entre los usuarios, las soluciones de autenticación móvil y los servidores backend debe estar cifrada.

**Cómo se resuelve:** Antes de intercambiar cualquier mensaje, su solución de autenticación móvil debe garantizar que se está comunicando con el servidor correcto. La fijación de certificados se logra restringiendo los certificados que se consideran válidos para dicho servidor. Esto establece una confianza explícita entre su solución de autenticación y sus servidores, y disminuye su dependencia de organizaciones de terceros.



Para la seguridad a nivel de transporte, es esencial confiar en el protocolo TLS. TLS 1.2 protege la capa de transporte para que todos los mensajes intercambiados entre la solución de autenticación y el servidor, así como cualquier notificación enviada al dispositivo móvil, estén protegidos. Por otra parte, para la seguridad a nivel de mensaje, la información dentro de ese túnel de seguridad también debe cifrarse.

Las mejores soluciones de autenticación van un paso más allá. En particular, no requieren que se envíe ningún dato confidencial del usuario en las notificaciones push, y en vez de ello, se confía en un canal privado y seguro entre la aplicación y el servidor para recuperar el contexto de la solicitud. Esto mejora la seguridad al limitar la posibilidad de exposición y compromiso.

## 5. BLOQUEO DE ATAQUES EN TIEMPO REAL

**El desafío:** Con el aumento de las vulnerabilidades de día cero, es esencial que todas las aplicaciones incluyan mecanismos que puedan detectar y detener los ataques en tiempo real.

**Cómo se resuelve:** El protocolo Runtime Application Self Protection, o RASP, es un conjunto de controles y técnicas que sirven para detectar, bloquear y mitigar los ataques que se realizan mientras la aplicación está en ejecución. Esto evita la ingeniería inversa y la modificación no autorizada del código, sin intervención humana.

Las mejores soluciones de su clase utilizan una defensa de varias capas para reducir la probabilidad de que un solo control omitido pueda causar una brecha peligrosa. Estas defensas incluyen:

- El oscurecimiento del código hace que sea más difícil entender para un ser humano cómo descompilar el código fuente sin alterar la ejecución del programa.
- Las tecnologías de detección de manipulaciones como ASLR, las revisiones de las listas de propiedades (también conocidas como revisiones .plist) garantizan que nada ponga en peligro la aplicación ni su entorno, ni altere alguna función.
- La detección de fuga y emuladores permite a las empresas crear e imponer políticas sobre cuáles tipos de dispositivos son y no son de confianza.

## 6. OPTIMIZACIÓN DE LA ADMINISTRACIÓN DEL CICLO DE VIDA DE LA AUTENTICACIÓN

**El desafío:** Las claves criptográficas y los certificados que se envían a los dispositivos tienen ciclos de vida finitos para reducir el riesgo de que resulten comprometidos. Entre más corto sea el ciclo de vida, más segura será la clave. Por supuesto, los ciclos de vida más cortos en las claves también requieren que las organizaciones cuenten con planes estrictos de administración y renovación, y una solución que no obligue a los usuarios a registrarse de nuevo constantemente en el servicio.

**Cómo se resuelve:** Las mejores soluciones de autenticación facilitan configurar la duración de la clave. También cuentan con un mecanismo que permite al servidor renovar las claves de un dispositivo antes de que expiren, sin la intervención explícita del usuario. Esto permite que las empresas sigan las prácticas recomendadas de seguridad sin interrumpir el servicio a sus clientes.

## 7. PREVENCIÓN DE ATAQUES DE FUERZA BRUTA

**El desafío:** Los ataques de fuerza bruta utilizan pruebas y errores para deducir la información del inicio de sesión y las claves de cifrado. Es sencillo y sorprendentemente eficaz. De hecho, los investigadores de ciberseguridad de la empresa de seguridad de Internet ESET detectaron 55 mil millones de intentos de ataques de fuerza bruta entre mayo y agosto del 2021, más del doble de los 27 mil millones de ataques que se detectaron entre enero y abril del mismo año.

**Cómo se resuelve:** Las soluciones de autenticación móvil se basan en una gran variedad de técnicas diferentes para contrarrestar este tipo de ataques. Las soluciones más sólidas permiten personalizar la configuración, de acuerdo con sus necesidades y políticas específicas. Entre las técnicas más eficaces se incluyen:


- Los bloqueos de retardo activan una serie de retardos que aumentan cuando los usuarios introducen un PIN o una contraseña incorrectos, antes de que puedan intentarlo de nuevo.
- Los bloqueos del contador hacen que las contraseñas no sean válidas después de cierto número de intentos fallidos.
- Los bloqueos silenciosos no avisan a los usuarios cuando introducen un PIN o una contraseña incorrectos, simplemente bloquean a las personas fuera del sistema.

# Garantizar la protección continua

**El desafío:** Los proveedores de seguridad se jactan de grandes logros, pero ¿cómo puede asegurarse de que sus soluciones hacen lo que dicen y pueden mantenerse al día con el panorama de la seguridad en constante cambio?

**Cómo se resuelve:** Las auditorías por parte de terceros y las revisiones del cumplimiento de las certificaciones, internas y externas, son la forma más eficaz de garantizar que las soluciones de autenticación sean estables y seguras. Las revisiones internas deben verificar la solución mediante un conjunto de controles de seguridad basados en los estándares de la industria: el OWASP Application Security Verification Standard (ASVS).

Mientras tanto, las auditorías de penetración externas, como la Certificación de Sécurité de Premier Niveau (CSPN), otorgada por la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI), deben certificar la solidez de la solución basándose en un análisis de conformidad y rigurosas pruebas de intrusión.

# Creación de soluciones de autenticación móvil seguras y escalables

La MFA ha sido aclamada por su capacidad para detener los ataques. Sin embargo, cada vez más, las soluciones de la MFA se han convertido en un objetivo para los hackers. Y dado lo dañina y costosa que puede ser incluso una sola filtración, es claro que ha llegado el momento de que las organizaciones tomen en serio la seguridad de la autenticación móvil.

Proteger el proceso de autenticación móvil y garantizar un recorrido que abarque desde el registro de dispositivos del usuario hasta la administración de credenciales y las auditorías de seguridad, no es tarea fácil. Con una cuidadosa consideración y técnicas que aprovechen al máximo las funciones de seguridad a nivel de dispositivo, es posible crear soluciones que le protejan contra un panorama de amenazas en constante expansión.


## ¿NECESITA AYUDA PARA PROTEGER SUS SISTEMAS DE AUTENTICACIÓN MÓVIL?

- Visite la página web de Authentication and HID Approve
- Descargue el nuevo libro electrónico en HID Approve: Autenticación push sencilla y firma de transacciones
- Solicite una demostración de autenticación directamente en el calendario de nuestros expertos


hidglobal.com

Norteamérica: +1 512 776 9000 | Llamada gratuita: 1 800 237 7769
Europa, Medio Oriente y África: +44 1440 714 850
Asia Pacífico: +852 3160 9800 | Latinoamérica: +52 (55) 9171-1108
**Para obtener más números de teléfono internacionales, haga clic aquí**





2022-04-12-iams-ensuring-mobile-authentication-security-wp-es PLT-06607
Parte de ASSA ABLOY