



RANKING MÉTODOS DE AUTENTICACIÓN

(Y ELEGIR EL
CORRECTO)

—

No es ningún secreto que los ciberataques están incrementando, y lo han hecho desde hace algún tiempo. Aún más preocupante es la naturaleza impredecible de estos ataques, que varían en forma, complejidad, tamaño, intensidad e incluso propósito. Sin embargo, no todo es pesimismo y fatalidad. Si bien la eliminación de amenazas potenciales no es un enfoque factible actualmente, hay recursos y herramientas disponibles que cada empresa puede implementar para mantenerse mejor protegida, reducir el riesgo cibernético y mitigar los daños.

Informado para prevenir hasta el 90% de los ataques cibernéticos, el primer paso es implementar una política de Autenticación Multifactor (MFA). Para empresas de todos los tamaños en todas las industrias, esto es simplemente esencial y, a partir de noviembre de 2021, MFA es obligatorio para todas las entidades federales de EEUU según una orden ejecutiva emitida por la administración de Biden.

DAR EL SIGUIENTE PASO

Ahora que sabes qué es de misión crítica implementar la Autenticación Multifactor (MFA), debes **dar el siguiente paso** y decidir qué método (o métodos) es adecuado para cada persona, tanto externa como interna de tu empresa, incluidos empleados, socios, clientes y terceros. Si bien esto puede parecer una tarea desalentadora, en BIO-key estamos aquí para ayudarte a desglosar todo lo que necesita saber para dar el siguiente paso con confianza.

En esta guía, explicamos, analizamos, evaluamos y clasificamos diferentes métodos de autenticación compatibles con BIO-key PortalGuard® en la actualidad.

Las siguientes secciones se sumergen en los pros y los contras de cada método, con comparaciones directas entre sí en las siguientes categorías:

- > Seguridad
- > Conveniencia
- > Coste
- > Esfuerzo de implementación
- > Mantenimiento
- > Basado en teléfono o no

¿Te interesa saber cómo se compara cada método? Continúa leyendo para explorar las clasificaciones de autenticación.

El uso de la Autenticación Multifactor (MFA) puede prevenir hasta el 90 % de los ataques cibernéticos, y las aseguradoras y auditores cibernéticos comienzan a exigirlo en las empresas privadas.

TIPOS DE MÉTODOS DE AUTENTICACIÓN

Si estás tratando de saber qué método de autenticación es el adecuado para tu empresa, un buen lugar para comenzar es saber cómo se clasifica cada método.

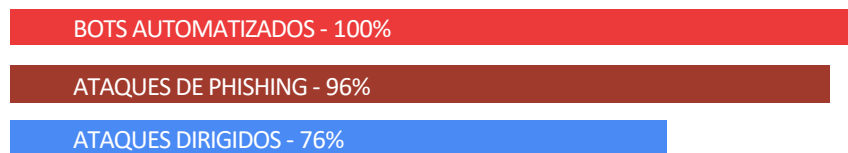
Hay tres categorías principales de métodos de autenticación:

Algo que sabes: estos factores de autenticación requieren que una persona recuerde y proporcione algo que sepa, como una contraseña o un número de identificación personal (PIN).


Algo que tienes: en este escenario de autenticación, el usuario debe demostrar que posee un elemento físico, como un token de hardware, un teléfono móvil o una tarjeta inteligente.

Algo que eres: este método de autenticación se basa en una información inherente al usuario, como una huella digital, un escaneo de la palma de la mano u otro tipo de biometría.

La implementación de la Autenticación Multifactor (MFA) puede ayudar a bloquear:



BIO-key PortalGuard admite los siguientes métodos de autenticación en las tres categorías:

 cosas que eres	BIO-key MobileAuth	WEB-key	Biometría basada en dispositivos
 cosas que tienes	Email OTP	SMS OTP	FIDO2 WebAuthn
 cosas que sabes	Apps de autenticación móvil	Notificaciones push	Preguntas de seguridad

Ahora que sabes cómo se clasifican y definen los métodos de autenticación, es igual de importante conocer los riesgos de elegir los métodos incorrectos y cómo implementar los métodos correctos correctamente.

RIESGOS DE ELEGIR EL MÉTODO INCORRECTO

Se recomienda encarecidamente tener algún tipo de Autenticación Multifactor (MFA). — cualquier forma de Autenticación Multifactor (MFA) es mejor que ninguna MFA.

Dicho esto, implementar la estrategia y el método incorrectos puede afectar la adopción del usuario y, a su vez, la seguridad general.

Es crucial encontrar el método de autenticación que mejor se adapte a las necesidades de cada usuario, de lo contrario:



Los métodos que no funcionan para los usuarios hacen que duden o sean incapaces de adoptar MFA, razón por la cual un enfoque único para todos no funciona.



Los métodos de autenticación incorrectos pueden crear vulnerabilidades de seguridad basadas en brechas de usuarios (bolsillos de usuarios que no usan MFA y métodos débiles que aseguran activos sensibles/de alto riesgo).



Los métodos incorrectos conducen a un aumento innecesario de los costes de la empresa, ya que hay una sobrecarga sustancial debido al mantenimiento y múltiples soluciones que causan redundancias operativas.

“

Muchos proveedores de Autenticación Multifactor (MFA) permiten a los usuarios aceptar una notificación de aplicación de teléfono o recibir una llamada telefónica y presionar una tecla como segundo factor. El actor de amenazas Nobelium se aprovechó de esto y emitió múltiples solicitudes de MFA al dispositivo legítimo del usuario final hasta que el usuario aceptó la autenticación, lo que permitió que el actor de amenazas finalmente obtuviera acceso a la cuenta”.

Mandiant Cyber Security Threat Intelligence

SEIS CONSIDERACIONES CLAVE AL IMPLEMENTAR LA AUTENTICACIÓN MULTIFACTOR (MFA)

Al final del día, configurar la política de seguridad adecuada y elegir la estrategia de autenticación correcta es una cuestión de comprender completamente las necesidades únicas de tu empresa y la mejor solución disponible.

Debes estar familiarizado con los riesgos cibernéticos más apremiantes y confiar en la elección de los métodos de autenticación adecuados para abordarlos. En resumen, aquí hay algunas consideraciones clave que siempre se deben tener en cuenta al implementar MFA:

- Conoce a tus usuarios y sus requisitos únicos. Evalúa su riesgo para informar sus políticas de seguridad.
- Cuenta con una estrategia de comunicación para su implementación.
- Verifica sus requisitos de cumplimiento y seguro cibernético.
- Selecciona soluciones que tengan múltiples opciones frente a una talla única para todos.
- Ofrece más de una opción: incluye siempre uno o más métodos de autenticación de respaldo en caso de que el método principal deseado no esté disponible por algún motivo.

CLASIFICACIÓN Y ANÁLISIS DE CATEGORÍA

A continuación, hemos desglosado y realizado un análisis en paralelo de todos los métodos de autenticación compatibles con BIO-key PortalGuard en las siguientes categorías:

- > Seguridad
- > Coste
- > Conveniencia / Esfuerzo de uso
- > Implementación en curso
- > Mantenimiento
- > Basado en el teléfono o no

Si bien las principales decisiones de ciberseguridad tienen en cuenta muchos de estos, la gran mayoría de los clientes de BIO-key consideran con razón que los dos factores principales (Seguridad, Usabilidad) son los más críticos para tomar la decisión correcta para su estrategia de autenticación, que se reflejan en el gráfico. debajo.

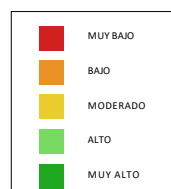
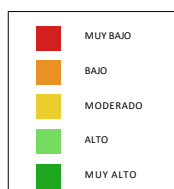
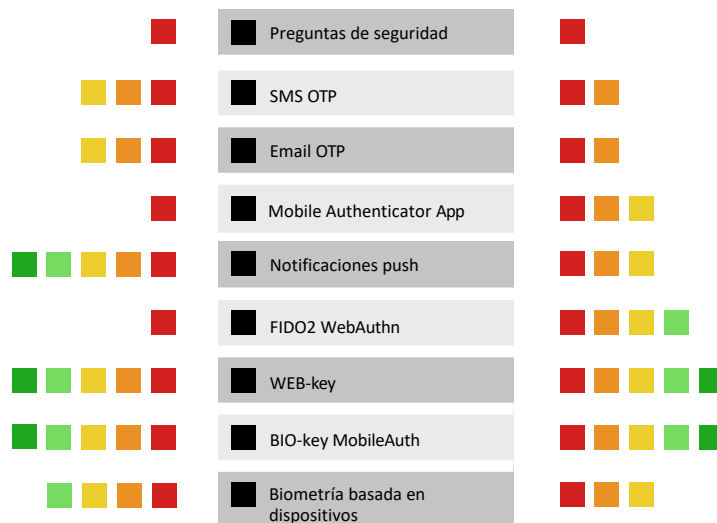
USABILIDAD

La facilidad de uso aumenta



SEGURIDAD

La seguridad aumenta



CUADRO COMPARATIVO







Si bien la seguridad y el coste son las principales prioridades para muchas empresas al comparar soluciones de autenticación, hay un total de seis factores a considerar. A continuación, analizamos y comparamos todos los métodos según los seis factores.

MÉTODO	COSTE	SEGURIDAD	CONVENIENCIA
Preguntas de seguridad	MUY BAJO	MUY BAJO	MUY BAJO
SMS OTP	MODERADO	BAJO	MODERADO
Email OTP	MUY BAJO	BAJO	MODERADO
Mobile Authenticator App	MUY BAJO	MODERADO	BAJO
Notificaciones push	MODERADO	MODERADO	ALTO
FIDO2 WebAuthn	ALTO	ALTO	BAJO
WEB-key	BAJO	MUY ALTO	MUY ALTO
BIO-key MobileAuth	MODERADO	MUY ALTO	ALTO
Biometría basada en dispositivos	MODERADO	MODERADO	ALTO

METHOD	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
Preguntas de seguridad	BAJO	MODERADO	<input type="checkbox"/>
SMS OTP	BAJO	MUY BAJO	<input checked="" type="checkbox"/>
Email OTP	BAJO	MUY BAJO	<input type="checkbox"/>
Mobile Authenticator App	MUY BAJO	BAJO	<input checked="" type="checkbox"/>
Notificaciones push	MODERADO	MODERADO	<input checked="" type="checkbox"/>
FIDO2 WebAuthn	MODERADO	MODERADO	<input type="checkbox"/>
WEB-key	ALTO	BAJO	<input type="checkbox"/>
BIO-key MobileAuth	MODERADO	BAJO	<input checked="" type="checkbox"/>
Biometría basada en dispositivos	BAJO	BAJO	<input checked="" type="checkbox"/>

¿CUÁL ES TU PRIORIDAD?

Alternativamente, si tienes una cierta prioridad en mente, como una mayor seguridad para proteger datos confidenciales o una implementación fácil porque tienes un equipo de IT más pequeño, aquí hay algunas recomendaciones sobre los métodos de autenticación que podrían funcionar mejor:

Prioridad de solución	Método de autenticación
<p>Mayor seguridad</p> 	<ul style="list-style-type: none"> > WEB-key IBB > MobileAuth IBB
<p>Fácil de implementar</p> 	<ul style="list-style-type: none"> > App de Autenticador móvil > MobileAuth IBB
<p>No requiere un smartphone</p> 	<ul style="list-style-type: none"> > WEB-key IBB FIDO2 > WebAuthn Security > Preguntas
<p>Acceso seguro de terceros/proveedores</p> 	<ul style="list-style-type: none"> > App de Autenticador móvil > MobileAuth IBB
<p>Acceso remoto seguro (VPN)</p> 	<ul style="list-style-type: none"> > Notificaciones push > App de Autenticador móvil > MobileAuth IBB > WEB-key IBB
<p>Protege la estación de trabajo compartida</p> 	<ul style="list-style-type: none"> > WEB-key IBB

CONCLUSIÓN

La implementación de la Autenticación Multifactor (MFA) es un paso inicial clave para prevenir los ataques cibernéticos, pero decidir qué métodos se adaptan a las necesidades y los flujos de trabajo diarios de tus empleados, socios, clientes y terceros sigue siendo una tarea abrumadora. Sin embargo, después de comprender la clasificación de cada método de autenticación, por su seguridad, facilidad de uso y coste, puedes seleccionar e implementar rápidamente los mejores métodos que se adapten a tus usuarios.

ANEXOS: ANÁLISIS EN PROFUNDIDAD DE CLASIFICACIONES

MÉTODO DE AUTENTICACIÓN: PREGUNTAS DE SEGURIDAD

Las preguntas y respuestas de desafío son uno de los métodos de autenticación originales y más antiguos. Los usuarios proporcionan respuestas a las preguntas previamente registradas.

La inscripción la completa un administrador o el usuario durante el primer inicio de sesión en el sistema.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN MÓVIL
MUY BAJA	MUY BAJA	MUY BAJO	MUY BAJA	MODERADO	<input type="checkbox"/>

✗ Seguridad: Muy baja

Algo que sabes es la categoría menos segura de métodos. El conocimiento (respuestas) se puede obtener a través de la ingeniería social y cualquiera puede utilizarlo.

Por lo general, los usuarios tienen dificultades para recordar las respuestas y usan la misma combinación de preguntas y respuestas en todas las aplicaciones, lo que significa que cuando una cuenta se ve comprometida, puede comprometer fácilmente varias otras cuentas. Las respuestas simples pueden ser fáciles de adivinar, especialmente con una investigación rápida sobre el individuo.

✗ Conveniencia / Fácil de usar: Muy baja

Por lo general, se requiere que el usuario responda de 3 a 5 preguntas para autenticarse correctamente, lo que puede llevar algún tiempo.

Las respuestas pueden estancarse si no se usan con frecuencia y se olvidan fácilmente después de un largo período de tiempo.

Beneficio: no se requieren dispositivos adicionales.

✓ Coste: Muy bajo

Sin costes adicionales.

✓ Implementación: Muy baja

Es necesario definir las preguntas de seguridad adecuadas, así como los criterios de respuesta (longitud mínima, respuestas duplicadas, etc.).

⊖ Mantenimiento: Moderado

No deberían ser necesarias interacciones del equipo de IT. En circunstancias normales, el usuario elige y responde las preguntas por sí mismo.

Si el usuario olvida la respuesta o la envía incorrectamente, necesita que IT lo ayude a restablecerla. IT no puede simplemente restablecer las preguntas; necesitan verificar al usuario de alguna manera primero. Esto puede ser un inconveniente, especialmente para el acceso remoto.

MÉTODO DE AUTENTICACIÓN: SMS OTP

El método de entrega de SMS (a menudo denominado simplemente "teléfono") consiste en enviar un mensaje de texto SMS a un número de teléfono móvil registrado. Este mensaje de texto SMS contiene un código de acceso único (OTP) que solo se puede usar una vez para validar al usuario para una acción específica.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
BAJA	MODERADA	MODERADO	BAJA	MUY BAJO	<input checked="" type="checkbox"/>

Seguridad: Baja

Susceptible a ataques Man-in-the-Middle (MITM) ya que los SMS se envían en texto no cifrado.

Los teléfonos pueden ser robados. Con este método, el usuario no necesita desbloquear el teléfono para ver el texto y la OTP, ya que el contenido del texto se muestra directamente en la pantalla de bloqueo.

Los mensajes SMS en sí mismos pueden ser pirateados y redirigidos al teléfono de un pirata informático. El intercambio de SIM se puede usar para hacer que un proveedor de servicios inalámbricos asigne un número de teléfono diferente a una nueva tarjeta SIM. Las tarjetas SIM se pueden clonar y usar en diferentes teléfonos.

Conveniencia / Fácil de usar: Moderada

Casi todo el mundo tiene su teléfono encima y es de fácil acceso.

El código que se envía debe escribirse. Puede ser fácil escribirlo incorrectamente o no dentro del tiempo asignado, dependiendo de qué tan largo/complejo sea.

Si su teléfono no tiene energía, no puede autenticarse. Tampoco funciona si no tienes servicio. También puede llevar algún tiempo recibir el texto de autenticación si el servicio no es confiable.

Coste: Moderado

Es posible que se requiera que las empresas proporcionen un estipendio telefónico para los dispositivos personales utilizados para la autenticación. El coste puede ser de hasta \$50/mes por dispositivo para empleados.

Para la disponibilidad, se debe utilizar un proveedor de SMS alojado. Por ejemplo, Twilio cobra \$0.0075 por mensaje enviado/recibido. Este es un costo recurrente, no una compra única y aumentará a medida que crezca la empresa y su base de usuarios.

Implementación: Baja

Se necesita poco en el lado de IT aparte de configurar el proveedor de servicios de SMS alojado.

Mantenimiento: Muy bajo

IT solo necesitará actualizar los números de teléfono si un usuario obtiene uno nuevo, lo cual es poco común.

El proveedor de SMS alojado es responsable de las interrupciones en el servicio, pero cualquier interrupción afectará a los usuarios y se requerirán recursos de IT para administrar el acceso y las comunicaciones durante cualquier interrupción o interrupción.

MÉTODO DE AUTENTICACIÓN: EMAIL OTP

El método de entrega de email OTP implica enviar un email a una dirección de correo electrónico registrada. Este email contiene una OTP para validar al usuario para una acción específica.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
BAJA	MODERADA	MUY BAJO	BAJA	MUY BAJO	<input type="checkbox"/>

Seguridad: Baja

Las mejores prácticas requieren que la aplicación a la que intenta acceder no sea la fuente del segundo factor de autenticación. Esto es por cuestiones de seguridad y usabilidad. Por ejemplo, si estás intentando iniciar sesión en PortalGuard y obtener el inicio de sesión único (SSO) en tus aplicaciones, incluido el email, entonces no es factible recibir el código en tu email. El email se puede interceptar fácilmente con un ataque Man-in-the-Middle (MITM).

La aplicación en la que se inicia sesión confía inherentemente en que el email del usuario no se ve comprometido, lo que a veces puede ser el caso, especialmente con el aumento de los ataques de phishing.

Conveniencia / Fácil de usar: Moderado

Los usuarios que intenten iniciar sesión para acceder al email no podrán recibir la OTP por correo electrónico como se explicó anteriormente.

La entrega se basa en la retransmisión SMTP, lo que podría causar un retraso en función de la conexión.

Los filtros de correo no deseado/filtros de email a menudo detectan estos emails que requieren que el usuario busque el email o no pueda recibirlo.

Coste: Muy bajo

Hay una gran cantidad de relevos SMTP gratuitos (por ejemplo, Gmail, Office365, Yahoo)

Muchas empresas ya cuentan con una retransmisión SMTP interna, ya que es la opción más segura.

Implementación: Baja

La integración con un retransmisor SMTP es rápida y fácil si está utilizando un retransmisor público (no recomendado para producción). Es necesario administrar más si estás utilizando tu propio relé interno, pero esto tampoco requiere mucho tiempo.

Mantenimiento: Muy bajo

Hay más responsabilidad para IT en comparación con el método SMS OTP, ya que no tendría un proveedor de servicios que administre el SMTP por ti.

MÉTODO DE AUTENTICACIÓN: APPS DE AUTENTICADOR MÓVIL

Estas aplicaciones generan un código de acceso único basado en el tiempo (TOTP) y se instalan en el dispositivo del usuario. Al autenticarse, se le pedirá al usuario que busque y abra la aplicación en su dispositivo y luego ingrese el TOTP que se muestra.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
MODERADA	BAJA	MUY BAJO	MUY BAJA	BAJO	<input checked="" type="checkbox"/>

Seguridad: Moderada

El único ataque viable es un ataque de fuerza bruta (PortalGuard tiene defensas integradas contra esto en forma de límites de tachado y bloqueos de cuenta).

Si un pirata informático obtiene la clave secreta, no se necesita ningún ataque, ya que tendrá acceso a todas las OTP que se generan hasta que se reemplace la clave.

Conveniencia / Fácil de usar: Baja

Es sencillo inscribirse, ya que la mayoría de las aplicaciones utilizan un código QR para iniciar la inscripción. Cada código suele durar 30 segundos, lo que puede ser demasiado poco para los usuarios que intentan escribir el código antes de que caduque.

La mayoría de las implementaciones, pero no todas, aceptan 1 o 2 ciclos de código antes para tener en cuenta cualquier problema de sincronización del reloj.

Aunque la mayoría de las aplicaciones de autenticación se usan en dispositivos móviles, si usa una aplicación de autenticación TOTP de escritorio, puede copiar y pegar el código rápidamente en lugar de escribirlo.

Coste: Muy bajo

Es posible que se le solicite a la empresa que proporcione un estipendio telefónico para los dispositivos personales utilizados para la autenticación. El costo puede ser de hasta \$50/mes por dispositivo para empleados.

Hay muchas opciones gratuitas como Google Authenticator y Microsoft Authenticator.

Hay varias aplicaciones "premium" de pago, como Twilio, Authy y DUO Security.

Implementación: Muy baja

PortalGuard solo requiere marcar una casilla de manera simple y fácil para habilitar este método.

Mantenimiento: Bajo

El único requisito del equipo de IT sería si un usuario obtiene un teléfono nuevo o no puede acceder a la aplicación móvil. Será necesario olvidar el viejo secreto y crear uno nuevo.

MÉTODO DE AUTENTICACIÓN: NOTIFICACIONES PUSH

Un token push es un segundo factor "fuera de banda" vinculado a un dispositivo móvil. Este segundo factor permite a los usuarios finales confirmar o denegar una solicitud de autenticación interactuando con su dispositivo móvil en tiempo real. No es necesario recordar ningún código: simplemente toque sí o no en la pantalla para confirmar la solicitud de autenticación.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
MODERADA	ALTA	MODERADO	MODERADA	MODERADO	<input checked="" type="checkbox"/>

Seguridad: Moderada

Muy seguro, los ataques MITM no son posibles.

Fuera de banda es más seguro y requiere el uso de un dispositivo separado.

Las notificaciones automáticas no están vinculadas a la persona, lo que puede ser problemático si se roba o se pierde un teléfono.

Muchos teléfonos tienen autenticación biométrica incorporada. ID táctil, ID facial

El usuario puede ver si alguien intentó acceder a su cuenta si recibe un impulso cuando no intenta iniciar sesión.

Conveniencia / Fácil de usar: Alta

La mayoría de las personas tienen sus teléfonos a mano o cerca.

Este método no requiere que el teléfono tenga servicio o conexión a internet.

No hay necesidad de escribir un código. Es un simple Aceptar o Denegar con un toque en la pantalla.

La notificación push aparece directamente en su teléfono sin abrirlo. No hay manera de interceptar.

Coste: Moderado

Es posible que se le solicite a la empresa que proporcione un estipendio telefónico para los dispositivos personales utilizados para la autenticación. El costo puede ser de hasta \$50/mes por dispositivo para empleados.

Los servicios pagos pueden ser costosos, como Twilio Authy (\$0.09/auth) y DUO Security (\$3-\$9/usuario/mes).

El coste puede aumentar rápidamente con entornos más grandes y puede ser difícil de predecir cuando sus organizaciones escalan rápidamente.

Implementación: Moderada

Este método debe integrarse mediante una API con PortalGuard. PortalGuard ya se integra con BIO-key MobileAuth, Twilio Authy y DUO Security "listos para usar".

Mantenimiento: Moderado

Según el proveedor, se necesitará algo de esfuerzo de IT para inscribir a los usuarios.

MÉTODO DE AUTENTICACIÓN: FIDO2 WebAuthn Hardware Tokens

FIDO2 (también conocido como WebAuthn) se diferencia de FIDO U2F en que está diseñado para un enfoque sin contraseña para la autenticación segura. Funcionalmente, los tokens FIDO2 admiten el mismo uso que FIDO U2F, aunque utilizan un estándar de la industria diferente y una API basada en navegador. Los tokens FIDO2 admiten uno de dos tipos de uso: hacer clic para autenticar o autenticación en el dispositivo. Hacer clic para autenticar requiere un toque/clic del token mientras que la autenticación en el dispositivo detecta la solicitud FIDO2 y responde automáticamente, lo que permite que la acción de autenticación continúe sin ninguna acción adicional por parte del usuario.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
ALTA	BAJA	ALTO	MODERADA	MODERADO	<input type="checkbox"/>

✓ Seguridad: Alta

Algo que tiene no verifica a la persona que usa el token. Algunos tokens tienen escáneres biométricos integrados en el token en forma de sensor de huellas dactilares; sin embargo, estos simplemente verifican los datos biométricos en el dispositivo y no verifican los datos biométricos de forma centralizada con tu empresa. El nivel de seguridad depende del manejo adecuado del token por parte del usuario. Los tokens se pueden robar, compartir o perder fácilmente.

Si la estación de trabajo a la que se accede es compartida, los tokens a menudo se dejan en la ranura USB de la estación, lo que permite compartir y acceder a muchos usuarios con el mismo token.

✗ Conveniencia / Fácil de usar: Baja

Estos tokens de hardware independientes se pierden fácilmente. Por lo general, se dejan en los puertos USB de los ordenadores compartidos. Esto provoca tanto un riesgo de seguridad como un inconveniente para los usuarios y IT.

El proceso de autenticación es relativamente fácil con un simple enchufe en el dispositivo y un flujo de trabajo de autenticación de un solo toque. Los tokens se pueden usar para la autenticación sin contraseña por conveniencia. Sin embargo, esto se consideraría una autenticación de un solo factor si no se combina con nada más.

✗ Coste: Alto

Hay un coste único de compra de tokens, con precios que van desde \$ 25 a más de \$ 100 para FIPS Verified por un solo token.

FIPS Verified a menudo es necesario para algunas organizaciones gubernamentales o contratistas. Otras empresas pueden requerirlo si así lo desean.

Al comprar tokens, se recomienda comprar 2-3 por usuario. Esto explica las llaves perdidas/rotas. A medida que tu empresa crezca, será necesario comprar más tokens. A menudo, un descuento por volumen está disponible para cantidades más grandes, según el proveedor.

⊖ Implementación: Moderada

IT necesita comprar, distribuir y administrar las claves de hardware.

La mayoría de las aplicaciones pueden realizar la inscripción de autoservicio, pero algunas requerirían que IT inscribiera previamente los tokens para sus respectivas cuentas de usuario, lo que puede llevar mucho tiempo.

⊖ Mantenimiento: Moderado

Si se pierde una clave, IT debe borrar el token actual del sistema para que no se pueda usar y emitir uno nuevo.

MÉTODO DE AUTENTICACIÓN: WEB-key (Identity-Bound Biometrics)



WEB-key es una plataforma de biometría ligada a la identidad (IBB) de nivel empresarial de BIO-key. IBB crea una identidad biométrica única centralizada que se puede usar para verificarte en cualquier lugar. El método principal para capturar la biometría es mediante el uso de un escáner de huellas dactilares.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
MUY ALTA	MUY ALTA	BAJO	ALTA	BAJO	<input type="checkbox"/>

✓ Seguridad: Muy alta

La inscripción controlada por la empresa evita la transferencia de cuentas y garantiza que solo las personas aprobadas puedan usar los privilegios de la cuenta.

Hay una menor susceptibilidad a los ataques de autenticación comunes, ya que los métodos de autenticación de IBB no se pueden olvidar, compartir, intercambiar, robar o falsificar.

La privacidad de los datos biométricos se garantiza a través de hash y salting criptográficos irreversibles para hacer que la información sea inaccesible y utilizable para posibles malhechores.

La detección de vida incorporada proporciona una fuerte detección de ataques de presentación (PAD) por parte de impostores que intentan usar imágenes escaneadas o falsificaciones.

IBB elimina las preocupaciones en torno a un único punto de fallo al eliminar los dispositivos físicos como posibles vulnerabilidades (como las presentes con la biometría local o nativa del dispositivo).

✓ Conveniencia / Fácil de usar: Muy alta

Admite una amplia gama de casos de uso y proporciona una experiencia más consistente para todos los usuarios. Solo se requiere una inscripción única para configurar el acceso a través de múltiples dispositivos y ubicaciones.

Admite usuarios itinerantes que acceden a sistemas seguros en estaciones de trabajo compartidas. Ofrece opciones fáciles de usar cuando los métodos telefónicos no funcionan o no están permitidos.

Admite la autenticación de múltiples factores cuando su servidor está fuera de línea, usando PortalGuard Desktop.

✓ Coste: Bajo

Compra única de escáneres de huellas digitales sin costos recurrentes como tokens de hardware, lo que resulta en un coste total de propiedad (TCO) bajo para implementaciones a gran escala. Asequible y rápido de implementar a cualquier escala con precios directos para lograr un ROI medible en 90 días o menos.

✗ Implementación: Alta

Se necesita un esfuerzo adicional para la configuración. El servidor de claves WEB debe instalarse y configurarse, junto con el software de claves WEB que se instala en las estaciones de trabajo.

Los escáneres de huellas dactilares deben comprarse y distribuirse, y también deben instalarse los controladores.

✓ Mantenimiento: Bajo

Hay un mantenimiento mínimo del servidor de claves WEB, ya que debe ser autohospedado. La mayor parte del esfuerzo de IT involucrado está en la configuración inicial. Una vez que está funcionando, se necesita poca interacción de IT. Todas las acciones son de autoservicio, excepto las acciones del administrador de back-end.

MÉTODO DE AUTENTICACIÓN: *BIO-key MobileAuth* (Identity-Bound Biometrics)

BIO-key MobileAuth es una aplicación móvil MFA fácil de usar que no requiere hardware nuevo y un rápido proceso de inscripción y registro de código QR que se puede completar en segundos. MobileAuth ofrece PalmPositive como un método de autenticación y una forma de biometría ligada a la identidad que utiliza un simple escaneo de la palma de la mano para autenticar al individuo.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
MUY ALTA	ALTA	MODERADO	MODERADA	BAJO	☒

✓ Seguridad: Muy alta

Un escaneo de la palma de la mano es 400 veces más preciso que Apple Touch ID y tecnologías relacionadas.

Combina "algo que tienes" y "algo que eres" para mayor seguridad.

La biometría vinculada a la identidad está vinculada al individuo, no a un dispositivo, lo que significa que las credenciales no se pueden robar, interceptar, falsificar, olvidar ni intercambiar.

✓ Conveniencia / Facilidad de uso: Alta

Un proceso de inscripción y registro de código QR rápido y fácil que toma solo unos segundos.

Debes sacar tu teléfono para acceder a la notificación automática y escanear tu biometría cada vez que te autentiques.

⊖ Coste: Moderado

Los estipendios telefónicos para los planes telefónicos de los empleados pueden costar hasta \$50 al mes por dispositivo.

⊖ Implementación: Moderada

Los usuarios deberán descargar la aplicación MobileAuth de BIO-key e inscribirla en PortalGuard según las instrucciones de IT.

La configuración básica deberá realizarse con el equipo de BIO-key PortalGuard para habilitar esto en las políticas de seguridad de PortalGuard.

✓ Mantenimiento: Bajo

El mantenimiento continuo es mínimo para IT. Los usuarios deberán descargar la aplicación si obtienen un teléfono nuevo o pierden o rompen el actual.

MÉTODO DE AUTENTICACIÓN: Integrado

Biometría basada en dispositivos

La biometría integrada basada en dispositivos se refiere a métodos biométricos en los que todo el procesamiento, la comparación y la autenticación de la biometría se completa en el dispositivo. Esto incluye métodos como Touch ID y Face ID en dispositivos iOS, autenticación biométrica en dispositivos Android y Windows Hello en dispositivos Windows.

SEGURIDAD	CONVENIENCIA	COSTE	IMPLEMENTACIÓN	MANTENIMIENTO	BASADO EN EL MÓVIL
MODERADA	ALTA	MODERADO	BAJA	BAJO	<input checked="" type="checkbox"/>

Seguridad: Moderada

Estos datos biométricos integrados de sistema en un chip no son los más seguros, ya que lo que se autentica ante la parte que confía suele ser el certificado o el token del dispositivo, en lugar de verificar los datos biométricos reales (también conocido como la persona).

Esto casi siempre se puede omitir con una contraseña o PIN. Esto significa que es tan seguro como el PIN. El usuario es quien tiene el control de la inscripción de cualquier dato biométrico en el dispositivo, lo que permite que los usuarios no autorizados se inscriban sin que la parte que confía lo sepa, eliminando cualquier nivel de confianza de que solo los usuarios autorizados obtienen acceso.

Conveniencia / Fácil de usar: Alta

Integrado en el dispositivo del usuario. Este método se utiliza para desbloquear el dispositivo y realizar otras tareas todos los días. Muchas personas se sienten cómodas, familiarizadas y ya están inscritas para usar este tipo de autenticación, lo que hace que los usuarios lo sientan como una segunda naturaleza.

No se necesita instalación y poca configuración.

Los usuarios deben inscribir y configurar cada dispositivo individual, ya que la autenticación está vinculada al dispositivo específico en el que se captura la biometría. Por esta razón, estos métodos biométricos son inconvenientes cuando los usuarios tienen múltiples dispositivos, usan estaciones de trabajo compartidas y/o trabajan en múltiples ubicaciones.

Coste: Moderado

Smartphones con biometría integrada puede ser muy costoso, especialmente en comparación con los teléfonos sin esa función. Para los empleadores, es posible que se requieran estipendios telefónicos y pueden costar hasta \$50/mes por dispositivo.

La biometría de Windows Hello requiere un escáner de huellas dactilares incorporado o una cámara especializada. Los dispositivos, como las computadoras portátiles con estas características integradas, pueden costar más que los que no las tienen. Por ejemplo, una cámara web incorporada estándar no se puede usar para el reconocimiento facial, ya que no puede detectar la profundidad y la vivacidad, lo que requiere la compra de un dispositivo por separado.

Implementación: Baja

Dado que estos métodos son nativos del dispositivo, se requiere poca o ninguna implementación. No hay instalación adicional, y el usuario simplemente necesita registrar su rostro/huella digital con el escáner o la cámara incorporados.

Mantenimiento: Bajo

IT necesita suministrar los dispositivos para permitir la biometría. Es posible que se requiera soporte para ayudar a los usuarios a inscribirse en cada dispositivo o ubicación a la que intentan acceder, ya que la autenticación se maneja localmente.

ACERCA DE BIO-KEY INTERNACIONAL

BIO-key International es un proveedor confiable de administración de acceso e identidad (IAM) y soluciones biométricas vinculadas a la identidad (IBB) que permiten un acceso conveniente y seguro a dispositivos, información, aplicaciones y transacciones de alto valor. BIO-key ofrece la simplicidad y la flexibilidad necesarias para asegurar la experiencia digital moderna para usuarios locales y remotos, al tiempo que alivia la carga de los equipos de IT.

BIO-key PortalGuard es una plataforma de identidad como servicio (IDaaS) completamente unificada con opciones de identidad biométrica líderes en la industria, inicio de sesión único, autenticación multifactor, autenticación adaptable y restablecimiento de contraseña de autoservicio. Respaldo por décadas de experiencia, BIO-key tiene un historial comprobado de entrega exitosa de proyectos de IAM, sólidas relaciones con los socios y bajo coste total de propiedad.