

Kensington®

Llaves de Seguridad y Huella Dactilar VeriMark™

Su socio de confianza en la autenticación
multifactor y la ciberseguridad



Acceso Seguro sin Complicaciones

Las llaves de huella dactilar y de seguridad NFC están transformando la forma en que protegemos nuestro mundo digital. Las llaves de huella dactilar ofrecen autenticación rápida, fiable y sin contraseña utilizando datos biométricos únicos, lo que hace que el acceso no autorizado sea casi imposible. Las llaves de seguridad NFC añaden otra capa de comodidad y flexibilidad, especialmente para las personas que utilizan tanto PCs como dispositivos móviles. Son sencillas de usar y a menudo son más económicas que las opciones biométricas. Juntos, estas herramientas ofrecen una protección fuerte y multifactor que es fácil de usar, altamente segura y diseñada para mantener la información sensible a salvo sin ralentizarte.

Preguntas Principales

- ¿Cuál es el **objetivo clave** en el caso de uso?
- ¿Qué dispositivos o **navegadores** se deben admitir?
- ¿Se está utilizando **Windows Hello** o **Windows Hello para Empresas** o autenticación web?
- ¿Están los usuarios accediendo a **uno** o **varios** dispositivos?
- ¿Accederán **varios** usuarios al **mismo dispositivo** en diferentes momentos del día?
- ¿Qué **servicios** se están utilizando?





Tendencias de la Industria e Insights de Investigación

Panorama Actual de la Seguridad de Dispositivos

Kensington patrocinó un estudio, realizado por el especialista independiente en investigación de mercado Vanson Bourne, de 1,000 responsables de decisiones de TI senior responsables de la seguridad del hardware físico de su organización. Un hallazgo clave fue que el acceso no autorizado a los datos de la empresa en los dispositivos es la principal preocupación para el 43% de los encuestados, seguido por el 19% que se preocupa por la pérdida de datos sensibles debido a redes domésticas inseguras. Las organizaciones están recurriendo cada vez más a la autenticación multifactor (MFA) como defensa principal, con un 30% de los encuestados identificando la autenticación biométrica o multifactor como crítica para mitigar amenazas de seguridad.

Adopción de la Autenticación Biométrica

Un número creciente de organizaciones reconoce el valor de las soluciones de seguridad biométrica. Según nuestra investigación de mercado, el 71% de las organizaciones encuestadas utilizan actualmente huellas dactilares y/o llaves de seguridad para la autenticación de dos factores (2FA), mientras que un 26% adicional planea implementar estas medidas en un futuro cercano. La línea de productos VeriMark™ de Kensington ejemplifica la seguridad biométrica de vanguardia, combinando la comodidad sin contraseña con una protección de nivel empresarial. Como líder en la seguridad del lugar de trabajo moderno, Kensington ofrece soluciones que cumplen con la TAA y el GDPR, que se integran en infraestructuras existentes, permitiendo a las organizaciones abordar eficazmente las amenazas cibernéticas en evolución.

Fuente: Vanson Bourne, Investigación de seguridad de dispositivos, octubre-noviembre de 2024.

Seguridad Mejorada y Comodidad con VeriMark™ IT 2.0 y VeriMark™ Desktop 2.0



Las llaves biométricas como VeriMark™ IT 2.0 y VeriMark™ Desktop 2.0 se integran sin problemas con Windows Hello para ofrecer una seguridad mejorada y un acceso rápido y conveniente. Totalmente compatibles con los requisitos de Seguridad de Inicio de Sesión Mejorada (ESS) de Microsoft, combinan un reconocimiento avanzado de huellas dactilares con los últimos estándares de autenticación de Windows. VeriMark™ IT 2.0 y Desktop 2.0 garantizan inicios de sesión seguros, cifrado y protección en línea, ideales para salvaguardar datos sensibles mientras simplifican el acceso con un simple toque, lo que los convierte en una opción perfecta para profesionales modernos y entornos de IT.

Autenticación Fuerte

La autenticación biométrica utiliza la huella dactilar, que es única para cada usuario, lo que la convierte en un método de autenticación altamente seguro.

Bajo Riesgo de Olvidar o Perder

A diferencia de las contraseñas, los usuarios no pueden olvidar o perder sus datos biométricos.

Acceso Rápido y Conveniente

Autentícate en segundos con solo un toque—sin teclear, sin complicaciones.

Eleva la Seguridad Web con VeriMark™ Guard 2.1 a Través de MFA



Las llaves de seguridad como VeriMark™ Guard 2.1 son ideales para la autenticación multifactor (MFA) al acceder a servicios web que requieren una protección mejorada. Como solución certificada por FIDO®, combina la verificación biométrica o la introducción del PIN con autenticación basada en hardware para ofrecer una seguridad fuerte y resistente al phishing. Perfecto para plataformas financieras, aplicaciones empresariales o cuentas en la nube sensibles, VeriMark™ Guard 2.1 proporciona una defensa robusta contra el robo de credenciales mientras mantiene una experiencia de usuario rápida y fluida.

Altamente Seguro

Las llaves de seguridad utilizan una autenticación criptográfica fuerte que es extremadamente difícil de duplicar o manipular, lo que las hace resistentes a ataques de phishing y de ingeniería social. Como dispositivos certificados por FIDO2, U2F y CTAP2.1, apoyan estándares de seguridad modernos basados en hardware que ayudan a las organizaciones a cumplir con estrictos requisitos regulatorios como HIPAA y PCI DSS.

Fácil de Usar

Las llaves de seguridad son simples de usar y requieren una configuración mínima, lo que las convierte en una opción conveniente para los usuarios.

Accede a la Seguridad de Grado Empresarial Sin Contraseñas



La llave de seguridad VeriMark™ NFC+ ofrece una forma simple pero poderosa de asegurar el acceso a través de dispositivos. Combinan la conveniencia inalámbrica con encriptación de alta seguridad, permitiendo a los usuarios autenticarse simplemente tocando la llave cuando está insertada, o acercando la llave a un lector NFC. Estas llaves eliminan la necesidad de registrar datos biométricos, lo que las hace perfectas para puestos de trabajo compartidos o configuraciones rápidas. Con tecnología resistente al phishing y certificación FIDO®, ofrecen seguridad de grado empresarial a un precio asequible, asegurando tanto la usabilidad como el cumplimiento.

Integración con Windows Hello

VeriMark™ Access permite inicios de sesión rápidos en Windows sin contraseña con una simple configuración de llave de huella dactilar plug-and-play. Cuando la llave no está disponible, la aplicación móvil VeriMark™ Companion sirve como respaldo seguro, generando un código de un solo uso para asegurar un acceso ininterrumpido. La solución también soporta entornos multiusuario que requieren un cambio rápido y fluido entre usuarios.

Capacidades FIDO2

Certificadas para FIDO2 Nivel 2 y soportando CTAP2.1, estas llaves funcionan en las principales plataformas y navegadores, incluyendo Windows, macOS, iOS y Android. Esta llave proporciona una solución escalable y conforme para empresas que adoptan la seguridad sin contraseña.

Seguridad Donde, Cuando y Como la Necesites



Despliegue para Empresas

Los productos VeriMark™ están diseñados para una implantación empresarial escalable, ofreciendo una forma sencilla y rentable de implementar la autenticación sin contraseña. Con una amplia compatibilidad entre sistemas operativos, navegadores y plataformas de identidad, los productos VeriMark™ se integran sin problemas en los entornos de IT existentes. Soportan la gestión centralizada, cumplen con los estándares de conformidad FIDO2 y de la industria, y proporcionan seguridad resistente a phishing sin añadir complejidad.

Cumple con el GDPR

Puede utilizarse para respaldar las medidas de ciberseguridad de acuerdo con (y sin limitarse a) las leyes y reglamentos de privacidad, como el RGPD, BIPA y CCPA.

Compatibilidad

Las llaves de huella dactilar y de seguridad VeriMark™ están diseñadas para una amplia compatibilidad, ofreciendo autenticación segura y sin contraseña en múltiples plataformas y servicios. Esta funcionalidad multiplataforma hace de VeriMark™ una solución ideal para empresas e individuos que buscan una seguridad fuerte y resistente al phishing sin sacrificar la comodidad.

Puntos Fuertes de las Llaves de Seguridad de Huella Dactilar



Control de Acceso Biométrico

El beneficio destacado es que la posesión de la llave por sí sola no es suficiente, la huella dactilar del usuario debe coincidir. Esto reduce drásticamente el riesgo en caso de que la llave se pierda o sea robada. Solo los registrados pueden activar la respuesta criptográfica de la llave.

MFA Integrado en Un Dispositivo

Una llave de huella dactilar combina algo que eres (verificación biométrica) con algo que tienes (un dispositivo de seguridad físico). En la práctica, esto permite que el escaneo de huellas dactilares sirva como el paso de verificación del usuario, eliminando la necesidad de un PIN o contraseña separados al iniciar sesión. Esto crea una experiencia de inicio de sesión simplificada donde una sola acción se encarga tanto de desbloquear la llave como de la autenticación, mientras se siguen aplicando múltiples factores de autenticación fuertes.

Comodidad y Velocidad para el Usuario

Para muchos, usar una huella dactilar es más rápido y conveniente que escribir contraseñas o buscar un teléfono para un código OTP. Con una llave bien diseñada, el escaneo de huellas dactilares es casi instantáneo.

Retroalimentación Visual/Táctil

Las llaves biométricas suelen ofrecer algún tipo de respuesta (como un indicador LED) cuando una huella es aceptada, lo que puede generar una mayor sensación de confianza. Saber que la llave te verifica activamente añade una sensación de seguridad.

Principales Beneficios de las Llaves de Huella Dactilar VeriMark™

Seguridad Biométrica: Solo los usuarios registrados pueden acceder.

Inicio Rápido: Un toque y listo - sin necesidad de escribir.

Resistente al Phishing: Autenticación basada en hardware.

Portátil: Uso en múltiples dispositivos.

Regulatorio: Cumple con el GDPR y es compatible con TAA.



Puntos Fuertes de USB NFC Llaves de Seguridad



Compatibilidad Entre Dispositivos

El gran beneficio de las llaves habilitadas para NFC es que funcionan sin problemas tanto con PCs como con dispositivos móviles. Puedes conectar la llave a puertos USB estándar y acercarla a teléfonos o tablets mediante NFC para autenticarte de forma inalámbrica.

Facilidad de Uso en Móviles

Usar una llave de seguridad en un teléfono puede ser complicado si el teléfono no tiene un puerto USB disponible o tiene una funda, pero NFC lo soluciona. Acercar la llave en el teléfono es rápido e intuitivo y se comunica a través de un rango muy corto (dentro de unos pocos centímetros), lo que es conveniente y seguro (difícil de interceptar).

Ideal para Usuarios Compartidos o Rotativos

Las llaves NFC no almacenan huellas dactilares ni requieren una configuración biométrica individual, lo que las hace perfectas para entornos donde varias personas necesitan acceso, como equipos de primera línea, laboratorios estudiantiles, o plantas de fabricación.

Seguridad Sólida

Las llaves NFC mantienen el mismo nivel elevado de seguridad criptográfica que otras llaves de hardware. El NFC en sí está diseñado para comunicación a corta distancia, lo que limita enormemente cualquier riesgo de espionaje (un atacante tendría que estar físicamente a pocos centímetros durante su uso).

Principales Beneficios de las Llaves de Seguridad NFC+ VeriMark™

Interfaz Doble: Funciona tanto con USB como con NFC para un acceso flexible a dispositivos.

Seguridad Resistente al Phishing: Protección basada en hardware contra el phishing y el robo de credenciales.

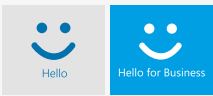
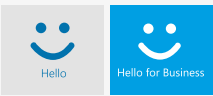
Certificado FIDO2 Nivel 2: Cumple con los principales estándares de la industria para la autenticación sin contraseña y soporta CTAP2.1.

Multiplataforma: Compatible con Windows, macOS, Android, iOS y los principales servicios y navegadores.

No se Necesita Configuración Biométrica: Rápido de implementar—no se requiere registro de huellas dactilares.



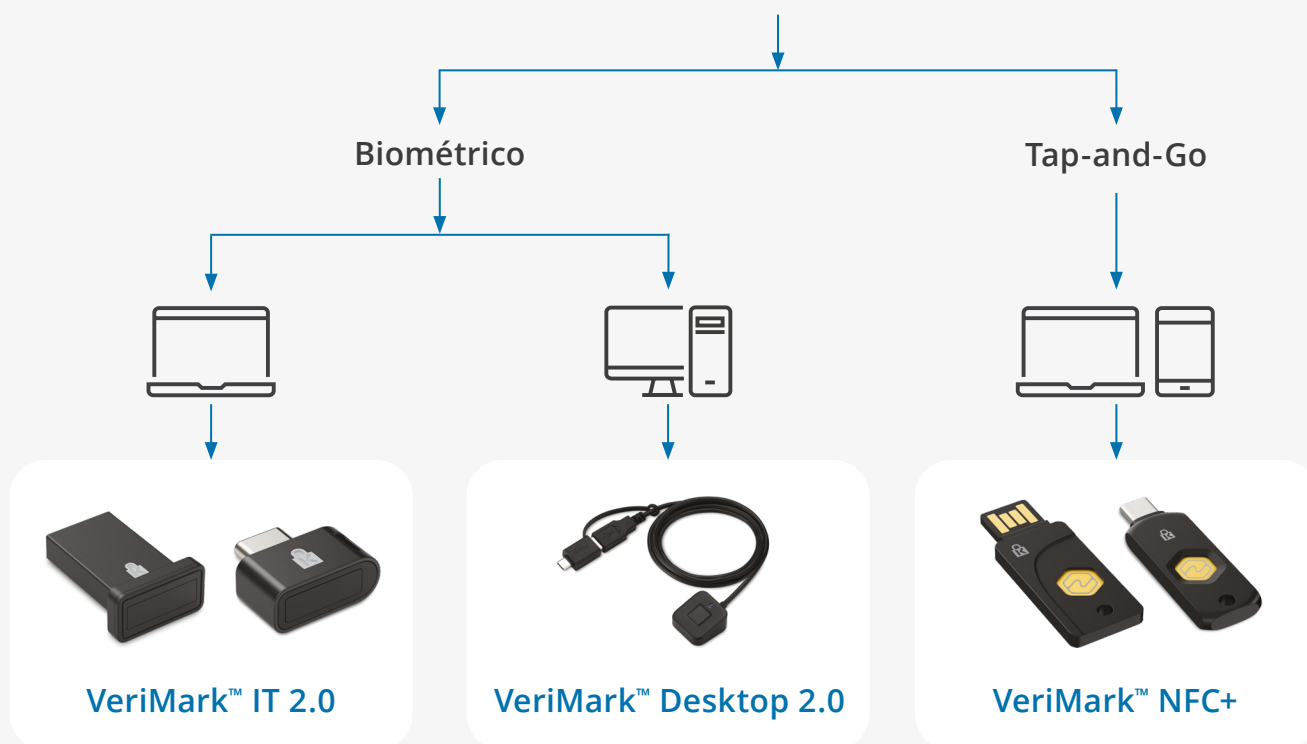


	LLAVE DE HUELLA DACTILAR VERIMARK™ IT 2.0	VERIMARK™ LLAVE DE HUELLA DACTILAR DE ESCRITORIO 2.0	VERIMARK™ GUARD 2.1 LLAVE DE SEGURIDAD DE HUELLA DACTILAR	LLAVE DE SEGURIDAD VERIMARK™ NFC+
Elemento #	USB-A - K64740WW USB-C® - K64705WW	K64741WW	USB-A - K65050WW USB-C® - K65051WW	USB-A - K64738WW USB-C® - K64739WW
Windows Hello			No compatible	No compatible de forma nativa, pero se puede acceder a través de software (VeriMark™ Access) + Aplicación móvil complementaria
Seguridad de inicio de sesión mejorada de Microsoft (ESS)	Compatible con Windows 11	Compatible con Windows 11	No compatible	No compatible
FIDO2 y FIDO U2F	No compatible WebAuthn Compatible	No compatible WebAuthn Certificado FIDO U2F		
CTAP	No compatible	No compatible	Soporta CTAP2.1 y es compatible hacia atrás con CTAP2.0	Soporta CTAP2.1 y es compatible hacia atrás con CTAP2.0
Dispositivo				
Sistema operativo				
Google, Amazon, Apple y Servicios de Microsoft				
Servicios Web				
Administradores de Contraseñas				



	LLAVE DE HUELLA DACTILAR VERIMARK™ IT 2.0	VERIMARK™ LLAVE DE HUELLA DACTILAR DE ESCRITORIO 2.0	VERIMARK™ GUARD 2.1 LLAVE DE SEGURIDAD DE HUELLA DACTILAR	LLAVE DE SEGURIDAD VERIMARK™ NFC+
Elemento #	USB-A - K64740WW USB-C® - K64705WW	K64741WW	USB-A - K65050WW USB-C® - K65051WW	USB-A - K64738WW USB-C® - K64739WW
Certificado Para				
Tipo de Llave				
Tipo de conexión	USB-A o USB-C®	USB-A with USB-C® Adapter	USB-A o USB-C®	USB-A o USB-C® y NFC
Clave de Acceso	Compatible a través de biometría	Compatible a través de biometría	Compatible a través de biometría	Compatible a través de NFC o Tap-and-Go
Tipo de Autenticación por Huella Dactilar	Match-in-Sensor™	Match-in-Sensor™	Match-in-Sensor™	-
Puntuación de Datos	Datos de la plantilla de huellas dactilares en la llave	Datos de la plantilla de huellas dactilares en la llave	Datos de la plantilla de huellas dactilares en la llave	-
Tasa de Falso Rechazo (FRR)	2 %	2 %	2 %	-
Tasa de Falsa Aceptación (FAR)	0,001 %	0,001 %	0,001 %	-
Facilidad de Lectura	365 grados	365 grados	365 grados	-

Inicio de sesión seguro para Windows Hello



Inicio de sesión seguro para Web Services





La llave de seguridad USB-C® NFC+ de VeriMark™ está diseñada para fortalecer la seguridad digital en servicios basados en la web. Esta llave de seguridad USB-C® habilitada para NFC está certificada para FIDO2 Nivel 2 y ofrece autenticación segura, conveniente y multiplataforma tanto para consumidores como para usuarios empresariales. Al eliminar las vulnerabilidades de las contraseñas con MFA basado en hardware, proporciona protección de nivel empresarial contra el phishing y el robo de identidad.

- Seguridad certificada FIDO2 Nivel 2
- Soporte del protocolo FIDO CTAP2. 1
- Interfaz dual USB-C® + NFC
- Simplicidad y software complementario
- Compatibilidad entre plataformas
- Compacto y portátil
- Clasificación IP68 y resistente a los golpes



También disponible - USB-A

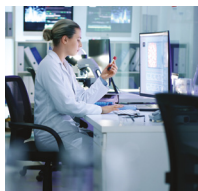


[Aprende más](#)



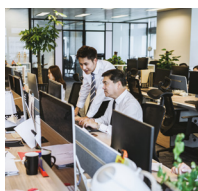
Llaves de Huella Dactilar – Casos de Uso y Propósitos Ideales

Las llaves de huella dactilar combinan autenticación biométrica con seguridad basada en hardware. Son más adecuadas para entornos donde la garantía de identidad individual es crítica.



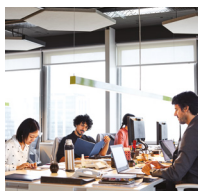
Sanidad

- Acceso seguro a los registros de pacientes (cumplimiento de HIPAA).
- Prevenir el acceso no autorizado a dispositivos médicos o terminales.
- Inicio de sesión biométrico para clínicos que utilizan puestos de trabajo compartidos.



Finanzas y Banca

- Acceso seguro a plataformas de trading o paneles financieros.
- Prevenir el robo de credenciales en entornos de alto riesgo.
- Cumplir con los requisitos regulatorios (por ejemplo, PCI-DSS, GDPR).



Gobierno y Sector Público

- Utilizado en instituciones federales para MFA biométrico.
- Soporta FIDO2 y Windows Hello para Empresas.



Educación

- Los profesores y el personal utilizan llaves de huella dactilar para un inicio de sesión seguro.
- Previene el acceso no autorizado en laboratorios de computación compartidos.



IT Empresarial

- Utilizado para la gestión de acceso privilegiado.
- Reduce la carga del servicio de asistencia por restablecimientos de contraseñas.
- Soporta auditorías y control de acceso centralizado.



Llaves NFC – Casos de Uso y Propósitos Ideales

Las llaves NFC ofrecen autenticación tap-and-go y son ideales para entornos móviles, multiusuario o de cara al consumidor.



Retail y Punto de Venta

- Tocar para autenticar en terminales de POS.
- Cambio rápido entre cuentas de personal.
- Prevenir transacciones no autorizadas.



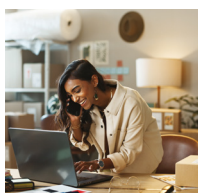
Transporte y Logística

- Los conductores utilizan llaves NFC para acceder a herramientas de planificación de rutas.
- Inicio de sesión seguro en sistemas de gestión de flotas.
- Ideal para entornos difíciles (calificación de impermeabilidad IP68).



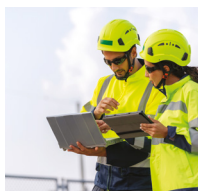
Educación

- Los estudiantes tocan para iniciar sesión en dispositivos compartidos.
- Los administradores de IT gestionan el acceso sin necesidad de inscripción biométrica.



Consumidor y PYMES

- Inicio de sesión sin contraseña para dispositivos personales.
- Configuración fácil para usuarios no técnicos.
- Compatible con Apple ID, Google, Microsoft y más.



Sector Público - Trabajo de Campo

- Inicio de sesión rápido para trabajadores móviles.
- No es necesario registrar la huella dactilar ni memorizar un PIN.
- Funciona sin conexión y en múltiples plataformas.



Todas las especificaciones están sujetas a cambios sin previo aviso. Es posible que los productos no estén disponibles en todos los mercados. Kensington y el nombre y diseño de ACCO son marcas comerciales registradas de ACCO Brands. Kensington The Professionals' Choice es una marca comercial de ACCO Brands. Todas las demás marcas comerciales registradas y no registradas son propiedad de sus respectivos propietarios. Thunderbolt y el logo de Thunderbolt son marcas comerciales de Intel Corporation en EE. UU. y/u otros países. © 2026 Kensington Computer Products Group, una división de ACCO Brands. CBT54577ES

PARA MÁS INFORMACIÓN CONTACTE CON: +34 932 38 44 00 • sales.es@kensington.com

Kensington
The Professionals' Choice™