



Evolucionando tu Cyberseguridad juntos

Soluciones IAM para la
educación superior



Introducción

Las instituciones de educación superior de todos los tamaños se enfrentan a un complejo creciente de amenazas a la ciberseguridad. La industria ha estado bajo un fuerte ataque durante varios años, con ataques de phishing, ransomware y denegación de servicio que aumentan en frecuencia y ferocidad. Al mismo tiempo, el éxito de los estudiantes ahora depende de una experiencia digital moderna, con el 87% de los estudiantes diciendo que el conocimiento tecnológico de una escuela fue un factor importante en su decisión de inscribirse.¹

Las instituciones se encuentran atrapadas, teniendo que elegir entre la experiencia del usuario o una ciberseguridad más estricta.

1. <https://www.ecampusnews.com/2018/09/04/5-technologies-that-will-help-colleges-meet-digital-age-students-expectations/>



Desafíos para implementar la administración de acceso e identidad (IAM)

Los controles críticos de IAM, como la autenticación multifactor (MFA) y el inicio de sesión único (SSO), pueden ser difíciles de implementar de manera cohesiva.

Si bien los controles de IAM son esenciales, implementarlos de manera cohesiva con recursos y presupuesto limitados a menudo da como resultado una estrategia inconexa y un aumento de los gastos generales.

Por ejemplo, el jefe cibernético de seguridad nacional de EE.UU cuenta con cifras que muestran que la autenticación multifactor podría evitar hasta un 80-90 % de los cyberataques², pero encontrar una solución única con todos los métodos de autenticación para apoyar a los estudiantes, profesores y personal es un desafío.

2. <https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of/>



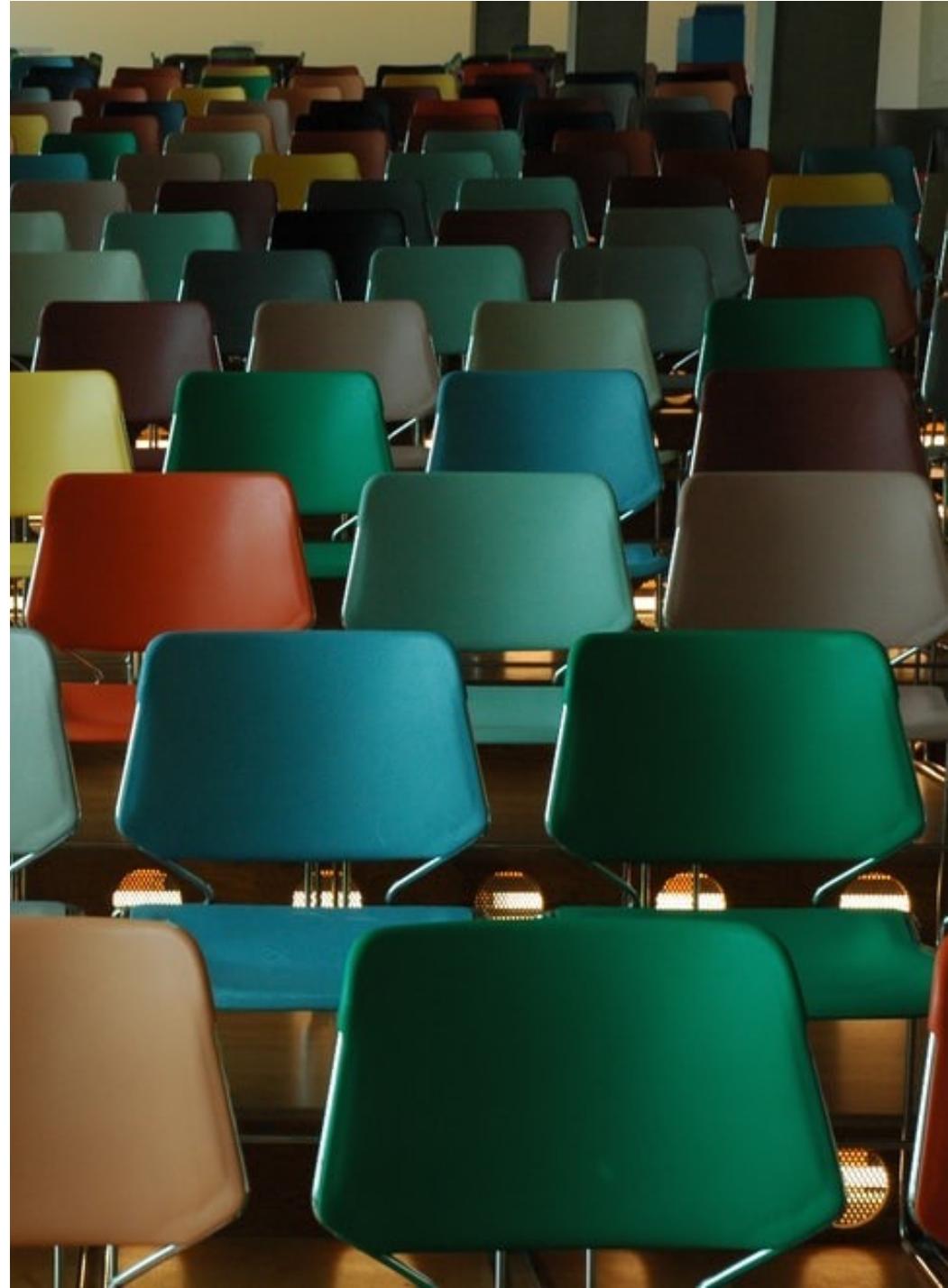
Tu propia estrategia de MFA ahora puede incluir varias soluciones en silos, como una para proporcionar un autenticador móvil, otra para tokens de inserción y otra para tokens de hardware, todas las cuales se administran con políticas de seguridad independientes.

El inicio de sesión único (SSO) también está desarticulado en muchas instituciones, que a menudo incluyen una combinación de soluciones comerciales, de código abierto y de desarrollo propio, que aún dejan las aplicaciones críticas al margen, con solicitudes de contraseña que se interponen cuando los usuarios intentan acceder a ellas.

Por último, las políticas de contraseñas, como la caducidad y la complejidad de las contraseñas, a menudo dan lugar a solicitudes de restablecimiento de contraseñas debido a contraseñas olvidadas, lo que supone una carga para muchas mesas de ayuda cuando no hay capacidades de restablecimiento de contraseñas autoservicio (SSPR). Con cada llamada de restablecimiento de contraseña costando un promedio de \$70³ este es un coste importante para algunas instituciones.

Los equipos de IT están abrumados por tener que respaldar el cambio rápido hacia nuevas formas de educación, como las plataformas de aprendizaje remoto, y algunas instituciones están realizando reducciones drásticas en el personal de IT y los niveles de presupuesto debido a los impactos de la pandemia de COVID. En este entorno, tratar de implementar la ciberseguridad para mantener segura tu institución puede ser un desafío constante.

3. <https://thehackernews.com/2021/04/cost-of-account-unlocks-and-password.html>



Durante más de una década, las instituciones de educación superior han confiado en BIO-key debido a nuestra experiencia en educación superior.

"¡Solución de identidad versátil, segura, flexible y excelente!"



[Lee la reseña](#)

"Portalguard ha sido una solución excelente, integral y, lo que es más importante, versátil que nos ha permitido implementar SSO de forma rápida y casi sin problemas para más de 20.000 usuarios".



[Lee la reseña](#)

"Excelente producto en general, ¡nos ayudó a brindar una mejor experiencia para nuestros estudiantes, profesores y personal!"



[Lee la reseña](#)

Más de 200 instituciones, incluidas más de 65 universidades comunitarias, utilizan BIO-key hoy.



DESTACADO

Fundación para los colegios comunitarios de California (FCCC)

Desde 2014, BIO-key se ha asociado con la FCCC para ayudar a mejorar la postura de ciberseguridad del sistema.

- Con la confianza de más de 50 universidades y distritos
- Descuento especial a través del contrato CollegeBuys
- 2022 partner en educación
- Patrocinador anual de la cumbre tecnológica CISOA

“Desde que implementamos BIO-key PortalGuard, las llamadas a la mesa de ayuda para restablecer la contraseña se han reducido drásticamente. La implementación del inicio de sesión único no podría haber sido más sencilla y, desde entonces, la hemos integrado con SharePoint, Blackboard, Canvas, OWA y WebAdvisor. El producto es fácil de configurar y mantener. No podríamos estar más satisfechos con la forma en que este producto y la compañía han funcionado para nuestras necesidades.”

- Clifford Sharp, Network Systems Analyst,
Southwestern Community College



2022 STRATEGIC PARTNER

¿Por qué las instituciones eligen BIO-key?

Con BIO-key no tiene que administrar su estrategia de IAM solo. Nuestro equipo de éxito del cliente y los profesionales de la seguridad son expertos en educación superior. Piensa en ellos como parte de tu equipo porque eso es exactamente lo que son. Trabajarán contigo para comprender los requisitos únicos de tu institución y se asociarán contigo para asumir cualquier trabajo pesado, para que tu equipo de IT no tenga que hacerlo.

Implementar [BIO-key PortalGuard](#) es una "ganancia rápida" de ciberseguridad ya que ayuda a evolucionar tu postura de seguridad cibernética con los recursos que tienes.



La plataforma única y galardonada agrega y consolida soluciones de punto de seguridad bajo políticas de seguridad centralizadas



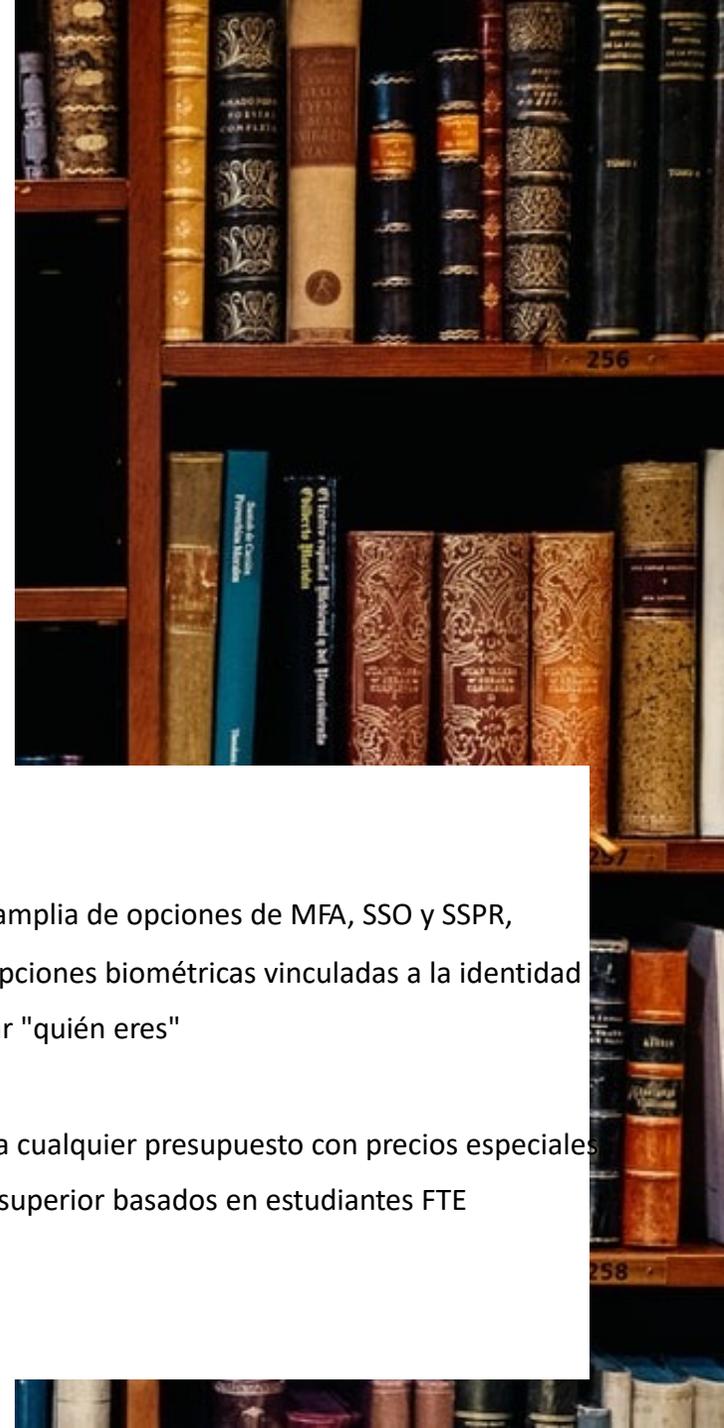
Increíble atención al cliente que combina el conocimiento del producto con la experiencia en IAM para garantizar que aproveche al máximo su solución



La gama más amplia de opciones de MFA, SSO y SSPR, incluidas las opciones biométricas vinculadas a la identidad para autenticar "quién eres"



Asequible para cualquier presupuesto con precios especiales de educación superior basados en estudiantes FTE



IAM beneficia a tu institución

Los clientes de BIO-key experimentan beneficios no solo para los estudiantes, profesores, personal y equipos de IT, sino también para su institución en general.

- **Mejore la seguridad en toda tu institución:** reduce el riesgo cibernético mediante la implementación de políticas de seguridad coherentes en todos los sistemas, plataformas, aplicaciones y dispositivos para reforzar la seguridad, incluida la autenticación multifactor.
- **Simplifica la vida de los estudiantes, profesores y personal** con una experiencia de inicio de sesión moderna: permita a los usuarios acceder fácilmente a los sistemas, independientemente de dónde se encuentren, qué hora sea y qué dispositivos estén utilizando.
- **Mejora la eficiencia y la eficacia de los equipos de seguridad:** la administración centralizada ayuda a optimizar los aspectos críticos de la gestión de identidades, autenticación y autorización.
- **Cumple a nivel normativo y con los requisitos del seguro cibernético:** pruebe dónde y cómo se utilizan las credenciales de usuario y demuestra que los datos están protegidos con los controles adecuados.



- **Aumenta la agilidad empresarial:** admite los nuevos servicios y sistemas que tu institución implementa con SSO y administración centralizada de políticas, para asegurar rápidamente el acceso a estos sistemas sin crear silos de seguridad adicionales.
- **Reduce costes de administración y de IT:** la administración simplificada de contraseñas evita las llamadas de restablecimiento de contraseña y simplifica la administración para los empleados y administradores de help desk, por lo que el tiempo dedicado a tareas mundanas ahora se puede dedicar a tareas de alta prioridad. Con una única solución IDaaS unificada, los costes se reducen a medida que se consolidan las soluciones en silos y se reduce o elimina la necesidad de comprar y mantener la infraestructura local.

Funcionalidades del PortalGuard

Simplicidad y flexibilidad para asegurar el acceso de empleados, clientes y proveedores.



Autenticación Multifactor (MFA)

Amplia gama de métodos de autenticación para una seguridad de identidad potente y flexible



Biometría vinculada a la identidad (IBB)™

Autenticación biométrica para los más altos niveles de integridad y conveniencia



Inicio de sesión único (SSO)

Reduce las solicitudes de contraseña y protege el acceso a todas las aplicaciones desde un solo IdP



MobileAuth™

App de autenticación multifactor que ofrece opciones de autenticación biométrica ligada a la identidad y tokens de inserción



Restablecimiento de contraseña de autoservicio (SSPR)

Reduce las llamadas de soporte de IT relacionadas con contraseñas hasta en un 95 %



Dispositivos de Hardware

Ofrece una variedad de dispositivos de hardware, incluidos escáneres de huellas dactilares USB Windows Hello calificados por Microsoft y tokens de hardware FIDO-key

Opciones de implementación
PortalGuard se puede implementar en tus instalaciones, en tu nube o como plataforma de identidad como servicio (IDaaS) en AWS.

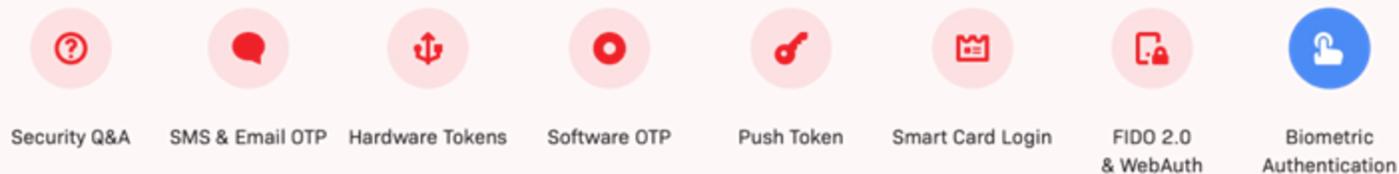
Autenticación Multifactor (MFA) flexible

Asegura todos los accesos y mantén segura tu institución

Agrega y consolida todos tus métodos de autenticación bajo políticas de seguridad administradas centralmente.

- Amplia gama de métodos de autenticación listos para usar
- Integre fácilmente las soluciones existentes (por ejemplo, DUO Security, Yubikey y MS Authenticator)
- Admite autenticación contextual y enfoques sin contraseña
- Los usuarios pueden seleccionar las opciones de autenticación que funcionen para ellos
- Políticas de seguridad granular configuradas para el grupo, la unidad organizativa o el individuo
- Protege los inicios de sesión del navegador y del escritorio

Increased Security Assurance



Completa tu MFA con biometría vinculada a la identidad

La biometría vinculada a la identidad (IBB) ofrece el más alto nivel de integridad al vincular una biometría a la identidad digital del usuario.

- Datos biométricos almacenados centralmente
- Datos biométricos hash no reversibles
- Gestión estricta de sesiones
- Capturado en escáneres de huellas dactilares o a través de BIO-key MobileAuth™



No se puede entregar, compartir, olvidar ni robar.



Perfecto para situaciones en las que los teléfonos y tokens de hardware no funcionan, no son confiables o seguros



Inscripción controlada por la empresa



Asequible y fácil de implementar

SSO para eliminar contraseñas y SSPR para reducir las llamadas al help desk

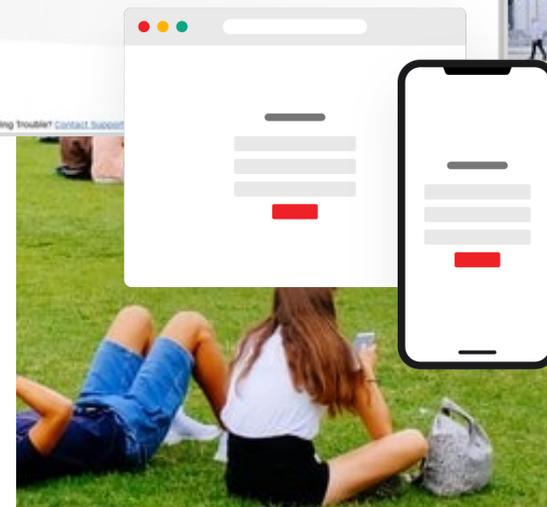
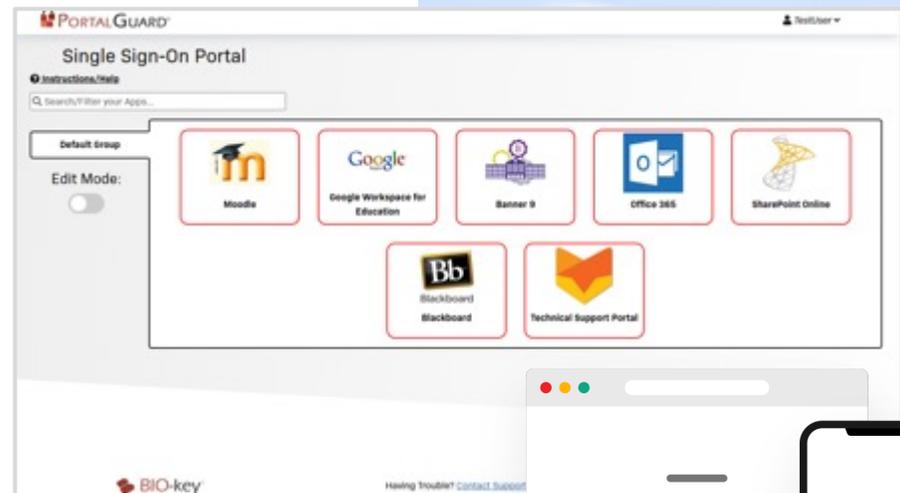
Los clientes que utilizan las capacidades del restablecimiento de contraseña autoservicio (SSPR) de PortalGuard reducen las llamadas al help desk en un 95% o más.

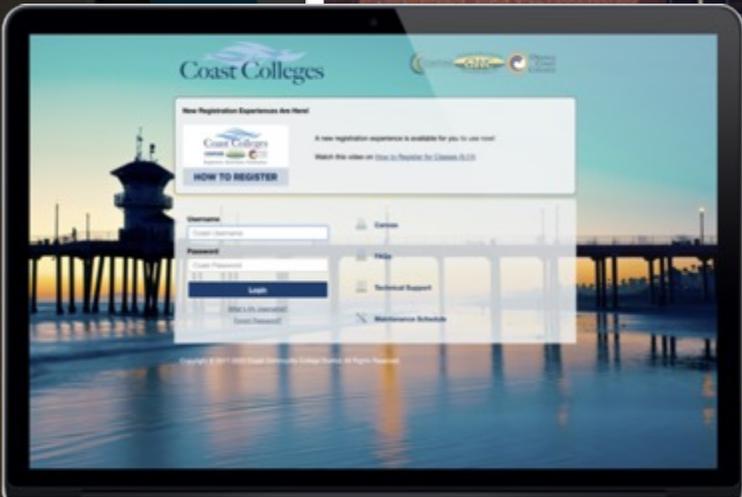
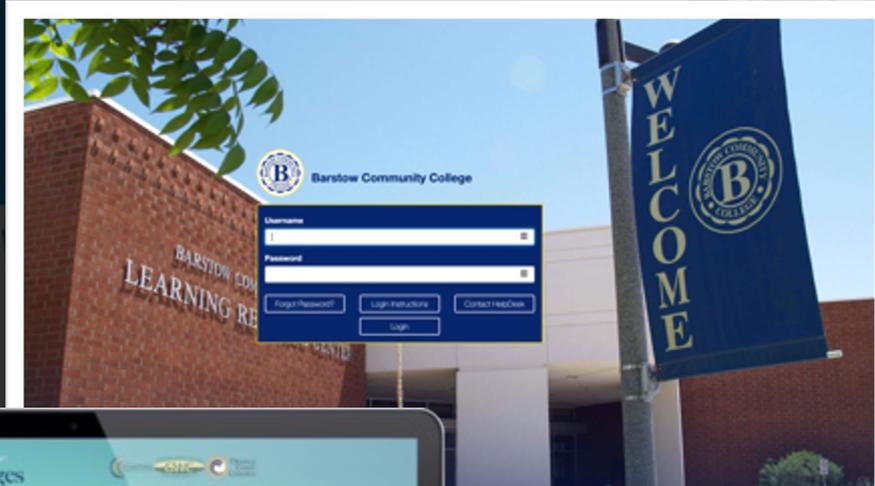
Inicio de sesión único (SSO)

- Proteja las aplicaciones locales, heredadas, de cliente grueso y web desde un único proveedor de identidad (IdP)
- Los estándares admitidos incluyen SAML 2.0, Shibboleth, WS-Federation, OAuth 2.0, OpenID Connect 1.0, CAS 3.0+

Restablecimiento de contraseña autoservicio (SSPR)

- Admite restablecimiento de contraseña, desbloqueo de cuenta, caducidad de contraseña, recuperación de contraseña y nombre de usuario y recuperación de contraseña sin conexión
- Disponible para inicios de sesión de navegador y escritorio/SO





UX totalmente personalizable para una experiencia de inicio de sesión moderna y de marca que encantará a los estudiantes, profesores y personal.

¿Quieres aprender más?

[Contáctanos](#)

Mientras tanto, aquí hay recursos para que aprenda más sobre seguridad cibernética, las soluciones de BIO-key y cómo las instituciones las están usando hoy. Recursos adicionales están disponibles en nuestra web [Resource Center](#).

- **WHITEPAPER:** [Cybersecurity in Education](#)
- **WEBINAR:** [The Future of IAM for Education: How Colleges are Combating the Increase in Cyberattacks](#)
- **WEBINAR:** [NICC's Journey to a Secure Student Experience](#)
- **DATA SHEET:** [BIO-key PortalGuard](#)
- **COMPETITIVE:** [5 Reasons DUO Security Customers Choose PortalGuard](#)
- **CASE STUDY:** [Contra Costa Community College District](#)
- **CASE STUDY:** [Southwestern Community College District](#)



Acerca de BIO-key International

BIO-key International es un proveedor confiable de administración de acceso e identidad (IAM) y soluciones biométricas vinculadas a la identidad 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 autenticación biométrica líderes en la industria, inicio de sesión único, autenticación multifactor, autenticación adaptable y restablecimiento de contraseña autoservicio.

Respaldado por décadas de experiencia, BIO-key tiene un historial comprobado de entrega exitosa de proyectos de IAM, sólidas relaciones con los socios y bajo costo total de propiedad.



Más información disponible en www.BIO-key.com

Aprende más en:

<https://www.bio-key.com/es/experiencia-en-educacion/>

