

An aerial photograph of a crowd of people walking on a light-colored pavement. A network of thin grey lines connects various teal-colored circular nodes, which are positioned over the people, suggesting a digital or organizational network. The scene is brightly lit, casting long shadows.

# Administración de identidades y accesos para el ecosistema de su empresa

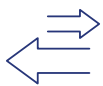
Plataforma de administración de identidades OneWelcome de Thales: la única solución verdadera IAM para B2B diseñada para optimizar la colaboración y mejorar la seguridad

[cpl.thalesgroup.com](http://cpl.thalesgroup.com)

**THALES**  
Building a future we can all trust

La colaboración efectiva con socios de negocio, proveedores y la cadena de suministro es esencial para el éxito de su empresa. A medida que usted ofrece portales para mejorar esa colaboración, se hace evidente la complejidad de administrar numerosas identidades y permisos de acceso. Los modelos tradicionales de administración de identidades se están esforzando para satisfacer las demandas de las empresas actuales. Estas demandas suelen implicar procesos administrativos laboriosos, tiempos de respuesta lentos e, involuntariamente, generan vulnerabilidades de seguridad y fricciones en la experiencia del usuario.

## Identificación de los desafíos de su IAM para B2B



Incorporar y desvincular socios de negocio nuevos y administrarlos de manera efectiva dentro del contexto de la estructura de la organización y de su ciclo de vida tiene una complejidad significativa.



Verificar usuarios mediante el seguimiento de sus atributos dinámicos, como certificados o autorizaciones, e incorporarlos en el control de acceso puede ser complicado y demandar mucho tiempo.



Si bien delegar la administración de identidades a sus socios de negocio puede reducir la carga administrativa, ya que ellos conocen a sus empleados mejor que nadie, esto presenta el desafío de tener que asegurarse de que se sigan buenas prácticas de seguridad y que se mantenga la integridad de los datos.



Cumplir los requisitos en materia de cumplimiento, en particular cuando se lidia con usuarios externos, exige mecanismos sólidos de información y control de parte de su DPO y CISO para evitar fraudes y sanciones.



Administrar a los usuarios de manera convencional a través de la asignación individual de acceso a un enfoque basado en políticas puede ser más eficiente y ofrecer un mejor control. Sin embargo, requiere una planificación y una coordinación cuidadosas para garantizar que el acceso se conceda o se revoque según los atributos y los roles de los usuarios.



Hacer que las aplicaciones nuevas y los portales estén rápidamente disponibles conservando la seguridad puede ser todo un desafío, en especial cuando los desarrolladores necesitan aprovechar las API de identidad y concentrarse en la funcionalidad de la empresa sin generar vulnerabilidades.

## Los grupos de usuarios B2B y la IAM

Garantizar la colaboración y la seguridad de datos perfecta en su red se basa en gran medida en proporcionar el acceso y la autorización adecuados a sus grupos de usuarios del sector B2B, sus empleados, así como a aplicaciones y recursos potenciales.

La colaboración empresa a empresa (B2B) puede incluir una variedad de usuarios: clientes corporativos, proveedores, el sector de fabricación de la cadena de suministro, coingeniería o proyectos, investigadores, personal a demanda y externalización de procesos de la empresa, personal temporal con contratos independientes, canales de distribución con distribuidores, agentes y espacios con diferentes marcas o shop-in-shop.

Por eso, usted necesita un enfoque híbrido que tenga en cuenta sus diversos grupos de usuarios del sector B2B.

La plataforma de administración de identidades OneWelcome de Thales, que está equipada con capacidades de vanguardia de IAM para B2B, es la única plataforma de IAM diseñada para hacer frente de manera directa a sus desafíos y le ofrece una implementación rápida de tan solo unas pocas semanas. Gracias a nuestra solución específica de IAM para B2B basada en la nube, puede administrar la amplia gama de grupos de usuarios de B2B, tales como clientes, proveedores y otros.

Además, entendemos el riesgo significativo que presentan los procesos de desvinculación incompletos dentro de muchas empresas. No revocar el acceso de empleados que ya no pertenecen a la empresa puede dejar a su organización vulnerable a brechas. Nuestra solución aborda esta situación de manera proactiva.

Con la **plataforma de administración de identidades OneWelcome** de Thales, obtiene:

- **Estructuras organizacionales:** niveles de acceso a medida por departamento, unidad de negocio o relación para responder a las necesidades exclusivas de sus partes interesadas y socios.
- **Control de acceso preciso:** acceso basado en roles y atributos para minimizar el riesgo de ingresos no autorizados, mejorando la seguridad.
- **Impacto mitigado de amenazas:** evita amenazas potenciales al restringir accesos innecesarios y mejorar sus mecanismos de defensa.
- **Colaboración eficiente:** promueve de manera segura el trabajo en equipo entre los equipos internos, socios y contratistas para la ejecución perfecta de los proyectos.
- **Cumplimiento y auditoría:** garantiza el cumplimiento de la legislación con el seguimiento meticuloso de las actividades de los usuarios para su tranquilidad.
- **Escalabilidad SaaS:** se implementa en una plataforma IAM para B2B a demanda, que puede ampliarse fácilmente para satisfacer las cambiantes demandas de las empresas.

# Uso de nuestra plataforma de lanzamiento de aplicaciones

Los socios podrán tener acceso a una plataforma de lanzamiento de aplicaciones segura para acceder a las aplicaciones de la empresa autorizadas para su rol u organización. Ofrece una puerta de acceso controlada y centralizada para que los empleados accedan a diversas aplicaciones de la empresa, garantizado que los datos y los sistemas confidenciales estén protegidos contra el acceso no autorizado y las ciberamenazas. A continuación, presentamos la descripción de una típica plataforma de lanzamiento de aplicaciones segura:



## Autenticación y autorización de usuarios

Los usuarios primero deben autenticarse a través de un proceso de autenticación de múltiples factores (MFA), que puede incluir algo que el usuario conoce (contraseña), algo que posee (tarjeta inteligente o token) y algo de su persona (datos biométricos, como huella dactilar o reconocimiento facial). Una vez autenticado, el sistema verifica el nivel de autorización y el rol del usuario para determinar a qué aplicaciones tiene permitido acceder.



## Inicio de sesión único (SSO)

La plataforma de lanzamiento suele ofrecer funcionalidad de SSO y permite a los usuarios acceder a múltiples aplicaciones con un único conjunto de credenciales. Esto mejora la practicidad y reduce el riesgo de brechas de seguridad relacionadas con contraseñas.



## Catálogo de aplicaciones

Los usuarios disponen de un catálogo organizado de las aplicaciones de la empresa en las que tienen permiso de uso. Este catálogo puede incluir aplicaciones web, aplicaciones de escritorio y aplicaciones virtualizadas.

En resumen, una plataforma de lanzamiento de aplicaciones segura es el núcleo central que prioriza la seguridad al tiempo que simplifica y optimiza el acceso de los usuarios a las aplicaciones de la empresa. Cumple la función esencial de proteger datos confidenciales, reducir el campo de ataque y garantizar que solo el personal autorizado pueda tener acceso a información y sistemas críticos.



## Políticas de control de acceso

La plataforma de lanzamiento aplica políticas de control de acceso para garantizar que los usuarios puedan acceder solamente a las aplicaciones y datos que están autorizados a ver o modificar.

El control de acceso basado en roles (RBAC) se usa comúnmente para determinar qué usuarios pueden acceder a qué recursos.



## Integración con administración de accesos e identidades (IAM)

La integración con los sistemas IAM garantiza que la identidad y los permisos del usuario se administren de manera uniforme en toda la organización.



## Cumplimiento y requisitos de información

La plataforma de lanzamiento de aplicaciones ayuda a las organizaciones a cumplir los requisitos reglamentarios en materia de cumplimiento al permitir reunir consentimientos, generar informes y proporcionar datos para las auditorías de cumplimiento.

## ¿Por qué Thales?

Thales tiene una tradición y una reputación reconocida en identidades y seguridad digital. La solución de IAM para B2B de Thales fue diseñada desde cero para atender a la gama completa de los grupos de usuarios del sector B2B y para impulsar la colaboración empresarial. Thales tiene una larga trayectoria al servicio de las industrias que poseen estrictos requisitos de seguridad. La seguridad está en nuestro ADN. Esto se extiende a nuestras soluciones IAM, donde las marcas líderes del mundo depositan su confianza en nuestra experiencia, respaldada por un equipo especializado de más de 15 000 especialistas del sector y múltiples referencias.

Exploremos cómo nuestro enfoque puede reforzar su estrategia de administración de identidades y mejorar los procedimientos de compromiso de sus socios, garantizando que su organización continúe siendo resiliente y segura en un entorno digital en constante cambio.

# THALES

Building a future we can all trust

## Contáctenos

Para conocer todas las ubicaciones de las oficinas y la información de contacto, visite [cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)

[cpl.thalesgroup.com](https://cpl.thalesgroup.com)

