

# 9 retos de IAM en la educación y cómo resolverlos



# Tabla de contenido

<b>1.</b>	<b>Introducción</b>	<b>1</b>
<b>2.</b>	<b>Por qué IAM es importante para el sector educativo</b>	<b>1</b>
<b>3.</b>	<b>Retos de IAM en el sector educativo</b>	<b>2</b>
	Sistemas de TI obsoletos, desarrollados internamente, heredados y múltiples fuentes de datos	2
	El ciclo de vida cambiante del usuario	2
	Aprovisionamiento y desaprovisionamiento manual	3
	Falta de gestión de acceso privilegiado	3
	Gestión del acceso temporal de los usuarios transitorios y contingentes	4
	Flujos de trabajo manuales para autorizar el acceso	4
	Falta de integración con plataformas basadas en la nube	5
	Costo de la mesa de ayuda para las solicitudes de desbloqueo de cuentas y contraseñas	5
	Requisitos de cumplimiento y seguridad	5
<b>4.</b>	<b>Cómo AD360 cubre las necesidades de IAM de su institución</b>	<b>6</b>
	Automatice los ciclos de vida de los estudiantes y docentes	7
	Proporcione a los usuarios acceso a los recursos educativos desde el primer día	7
	Cree una mejor experiencia de usuario con el SSO y la gestión de contraseñas de autoservicio	7
	Acceso Just-in-time para los usuarios externos	7
	Dé a los usuarios el acceso suficiente a los recursos que necesitan	7
	Flujos de trabajo de delegación y aprobación	8
	Simplifique los métodos de autenticación mientras garantiza la seguridad	8
	Mejore la seguridad y el cumplimiento	8
	<b>Acerca de ManageEngine AD360</b>	<b>9</b>



# Introducción

La gestión de identidades y accesos (IAM) es la disciplina de seguridad que permite a las personas adecuadas acceder a los recursos correctos en el momento preciso y por las razones correctas. Las funciones de IAM, como la gestión del ciclo de vida de las identidades, los métodos de autenticación de usuarios, la gestión de políticas y funciones, y los flujos de trabajo basados en la aprobación, se utilizan para proteger y gestionar las identidades de los usuarios, lo que es fundamental para que la organización y las personas mantengan la seguridad adecuada. La IAM se ha convertido en un elemento esencial de los planes de seguridad de muchas organizaciones.

## Por qué IAM es importante para el sector educativo

Las instituciones educativas contienen datos confidenciales de estudiantes, personal, docentes, materiales de investigación, etc., que a menudo se pasan por alto cuando se habla de ciberseguridad. Deben proteger las identidades de sus usuarios y evitar el acceso no autorizado a la información confidencial de los usuarios, como datos de contacto, expedientes académicos, información financiera y datos sanitarios, ofreciendo al mismo tiempo sistemas fáciles de usar y fiables con una disponibilidad continua.

Recientemente, la gestión de identidades para la educación ha experimentado un enorme cambio. Hay un notable aumento del aprendizaje virtual, en el que las clases se imparten a distancia y en plataformas digitales. Ahora hay una cantidad masiva de datos que se deben mantener actualizados. Muchas instituciones educativas ya enfrentan crisis de seguridad e intentan por todos los medios responder a ellas. Proporcionar un entorno de aprendizaje seguro se ha convertido en una gran prioridad, ya que la tecnología y los recursos en la nube siguen desempeñando un papel cada vez más importante en las instalaciones educativas.

Las escuelas y universidades no sólo deben tener en cuenta a los empleados que utilizan sus sistemas, recursos e información, sino también a los usuarios externos, como los estudiantes. Además de los estudiantes, los docentes, el resto del personal y, dependiendo de la edad del alumno, los padres también tendrán acceso a estos recursos. A esto hay que añadir que los usuarios son cada vez más expertos en tecnología: esperan interfaces intuitivas y funcionalidades modernas. Por lo tanto, uno de los principales retos tecnológicos a los que se enfrentan las instituciones educativas es proporcionar una experiencia de usuario óptima al tiempo que se protege el acceso a sus sistemas.



# Retos de IAM en el sector educativo

## Sistemas de TI obsoletos, desarrollados internamente y múltiples fuentes de datos

Los institutos y universidades llevan varios años utilizando software de código abierto, desarrollado internamente y obsoleto, debido a los limitados presupuestos de TI. Estos sistemas suelen ser difíciles de mantener, costosos de reparar y ofrecen un servicio al cliente deficiente. Tanto los usuarios como los equipos de seguridad de TI pueden frustrarse con las interfaces de usuario debido a las anticuadas infraestructuras de TI y soluciones de gestión de identidades. Con los sistemas de IAM desarrollados internamente, muchas tareas relacionadas con las identidades, como el desaproveamiento, son complejas, repetitivas y requieren mucho tiempo. Como resultado, estos sistemas ponen en riesgo a las universidades, ya que no se crearon para ser seguros.

Es habitual que los usuarios desempeñen múltiples funciones en el sector de la enseñanza superior. Los profesores pueden impartir clases, los estudiantes pueden trabajar como personal y los graduados pueden convertirse en egresados. Los sistemas de IAM tratan a cada uno de estos usuarios como un ID independiente, por lo que un usuario que tiene múltiples roles debe manejar varias credenciales de usuario para realizar sus actividades. Es importante mantener y proteger la información sobre el profesorado de la universidad y otros grupos afiliados. Estos datos se deben combinar y hacer accesibles.

## El ciclo de vida cambiante del usuario

En el sector educativo, a menudo surge el problema de tener usuarios con múltiples funciones. Cada semestre, los departamentos de TI deben ocuparse de dar de alta y de baja a miles de nuevos usuarios.

En el caso de los nuevos estudiantes, el equipo de administración se encarga de crear una cuenta en el portal de la universidad, generar una cuenta de correo electrónico y conceder acceso a las aplicaciones, los materiales del curso, la biblioteca y la conexión Wi-Fi. El estudiante debe poder obtener acceso antes de llegar al campus para recibir la orientación.

Cuando un estudiante termina un semestre y es promovido al siguiente nivel de clases, necesita acceso relacionado con el trabajo del curso. Ese acceso debe continuar hasta cierto tiempo antes de que el estudiante sea promovido para permitirle mover correos electrónicos o archivos fuera del sistema.

En el caso de los estudiantes que se gradúan, los administradores se encargan de desactivar las cuentas de usuario y eliminar el acceso a todas las aplicaciones y servicios.



En el caso de un miembro del personal, se le da acceso a datos sensibles, como información personal, y se le capacita sobre las responsabilidades relacionadas. Este empleado sigue teniendo acceso hasta que se marcha. Entonces, se debe revocar el acceso inmediatamente tras la desvinculación laboral.

## Aprovisionamiento y desaprovisionamiento manual

Las instituciones educativas manejan una enorme cantidad de datos confidenciales que incluyen información personal y datos financieros y crediticios de estudiantes, personal y profesores. Las universidades suelen tener períodos de mayor concentración a lo largo del año en los que se crean, gestionan, actualizan y eliminan miles de cuentas de usuario, generalmente al comienzo de un nuevo semestre. Esto puede provocar retrasos tanto en la incorporación, que crea una mala experiencia de usuario, como en la desvinculación, que podría suponer un riesgo para la seguridad.

Si los equipos de TI gestionan manualmente el acceso de los usuarios para cada requisito, el costo y el tiempo invertidos en ello serán significativamente altos. Gestionar las identidades manualmente aumenta los costos debido a la sobrecarga de la mesa de ayuda, las amenazas a la seguridad y el uso excesivo de licencias. Otro problema es la falta de auditoría de las cuentas de usuario. Para las instituciones educativas, esto hace que sea más difícil demostrar que se siguen las normas establecidas por los auditores externos.

## Falta de gestión de acceso privilegiado

La mayoría de las instituciones educativas carecen de un sistema adecuado de gestión de acceso privilegiado. Uno de los mayores riesgos de seguridad en el panorama cibernético es el posible uso indebido de las cuentas privilegiadas. Estas cuentas, constantemente son el objetivo de los actores maliciosos que buscan infiltrarse en información valiosa o causar daños a una organización.

Las escuelas y universidades no sólo tienen la tarea de proporcionar un acceso seguro a las aplicaciones y recursos, sino que también se enfrentan a la responsabilidad de gestionar correctamente los derechos de acceso. Esto puede complicarse aún más cuando los estudiantes reciben nuevas asignaturas y cursos cada trimestre, lo que provoca ajustes adicionales. Los profesores y empleados también necesitarán acceder a nuevas aplicaciones y datos con regularidad.



Uno de los riesgos de seguridad más desapercibidos a los que puede enfrentarse su escuela o universidad es que los empleados adquieran demasiados derechos de acceso debido a un cambio de rol o responsabilidad. Con frecuencia, las aplicaciones y las cuentas de servicio poseen excesivos derechos de acceso privilegiado y también tienen otras graves deficiencias de seguridad.

## Gestión del acceso de usuarios temporales

Las instituciones educativas, especialmente los colegios universitarios, deben tratar con usuarios transitorios a gran escala. Los estudiantes y profesores entran y salen del sistema. A veces se toman varios semestres libres o puede que no vuelvan nunca. Cuando los estudiantes tienen que esperar para acceder a recursos críticos, como materiales de cursos en línea y tareas, la experiencia del usuario final se ve afectada negativamente.

Las facultades y universidades también suelen contratar profesores temporales en lugar de profesores asalariados a tiempo completo. Aunque esto puede ahorrar dinero, crea una serie de retos para los departamentos de TI que deben gestionar las identidades de estos trabajadores temporales. La mayoría de los sistemas de IAM no tienen una forma sencilla de gestionar los usuarios externos que no existen en las bases de datos autorizadas de RR.HH. ni en los sistemas de información de estudiantes. Cuando los trabajadores se marchan, no existe un proceso para notificarlo al departamento de TI y, a menudo, nadie realiza la diligencia debida. La institución se queda con cuentas huérfanas a las que los antiguos trabajadores temporales siguen teniendo acceso. Esto supone un riesgo para la seguridad, sobre todo si esas personas tienen acceso a datos confidenciales.

## Flujos de trabajo manuales para autorizar el acceso

Los profesores y estudiantes necesitan acceder a los recursos utilizados en sus cursos. Si un usuario cambia de trabajo o abandona el sistema escolar, puede que no haya tiempo suficiente para asegurarse de que se actualizan o eliminan los permisos de acceso.

El personal de TI se encarga de autorizar el acceso con frecuencia. Además, estas solicitudes se envían en persona, por correo electrónico o en formularios en papel. Como resultado, cuando los estudiantes cambian de puesto o de clase, obtienen nuevos privilegios o incluso se convierten en egresados, puede haber retrasos, errores y posibles problemas de cumplimiento y seguridad. Gestionar el acceso de los usuarios manualmente para cada demanda es difícil y propenso a errores.



## Falta de integración con plataformas basadas en la nube

En un mundo en el que la mayoría de los sectores están pasando del software on-premises a los servicios en la nube, el sector educativo también está cambiando y utilizando algunas plataformas basadas en la nube, como Microsoft 365 y Google Workspace, que son ofrecidas y controladas por un proveedor externo fuera de la red del sistema escolar.

La gestión de identidades puede resultar difícil en este tipo de aplicaciones. Las instituciones que implementan software en la nube deben asegurarse de que se integra con las identidades existentes para maximizar el valor de sus inversiones y mantener los sistemas on-premises seguros y accesibles. Por lo tanto, es una gran carga para el equipo de TI garantizar que las identidades se extienden a las aplicaciones en la nube.

## Costo de la mesa de ayuda para las solicitudes de desbloqueo de cuentas y contraseñas

Un problema común al que se enfrentan las instituciones educativas es la ausencia de equipos dedicados a la mesa de ayuda de TI, posiblemente debido a la falta de fondos para invertir. Es frecuente que los usuarios olviden sus contraseñas, que éstas caduquen o que sus cuentas se bloqueen. Se ponen en contacto con el equipo de TI para restablecer sus contraseñas o desbloquear sus cuentas.

Las llamadas a la mesa de ayuda y las llamadas frecuentes no son difíciles de resolver para el personal de TI, pero quitan tiempo que podría emplearse en otras tareas. El número de llamadas para resolver los problemas relacionados con contraseñas es especialmente alto al principio del curso o del semestre, porque muchos usuarios olvidan sus contraseñas tras un largo descanso. Como resultado, la mesa de ayuda se congestiona y el usuario final no puede hacer nada de lo que necesita.

## Requisitos de cumplimiento y seguridad

Todas las instituciones educativas manejan grandes cantidades de información personal y sensible, lo que las convierte en objetivos principales para la violación de datos. Tras un ataque exitoso a una institución educativa, los ciberatacantes tendrán acceso a información personal, incluyendo fechas de nacimiento, nombres completos, direcciones, información de pago a través de contraseñas débiles, hackers externos, etc. Mantener la seguridad de estos datos es esencial para generar confianza en una institución y evitar filtraciones o violaciones de datos.



# Cómo AD360 cubre las necesidades de IAM de su institución

AD360 es una solución unificada para la gestión de identidades y accesos (IAM). Esta solución ayuda a los administradores a gestionar los ciclos de vida de los usuarios, proteger las cuentas privilegiadas, controlar el acceso e implementar la autenticación multifactor (MFA) adaptativa avanzada.

Las funciones clave de AD360 son:



## Gestión del ciclo de vida del usuario

AD360 permite a los administradores crear, modificar y eliminar cuentas cuando los usuarios cambian de rol o abandonan la organización. Puede modificar usuarios de forma masiva aplicando plantillas personalizadas o importando datos de un archivo CSV. Para desaprovisionar usuarios, puede desactivar o eliminar cuentas de forma masiva basándose en la política de su organización.



## Gestión de accesos

AD360 ayuda a los administradores a asegurarse de que cada usuario tiene los privilegios y el acceso adecuados. Mantenga una pista de auditoría del acceso de cada usuario a los recursos mientras gestiona los permisos y derechos concedidos a los usuarios.



## Inicio de sesión único (SSO)

AD360 proporciona funciones de SSO empresarial con políticas de seguridad basadas en OU y grupos, lo que facilita a los usuarios el acceso a todas sus aplicaciones en la nube.



## MFA

AD360 admite autenticadores como YubiKey, Duo Security, RSA SecureID, etc. También puede configurar la MFA para usuarios específicos en función de dominios, OU y membresías a grupos.



## Delegación de la mesa de ayuda basada en roles

AD360 permite a los administradores delegar tareas administrativas a usuarios no administrativos a través de un flujo de trabajo establecido para garantizar una delegación completamente segura. Pueden delegar tareas con un alcance limitado a una OU o grupo específicos.

## 1. Automatice los ciclos de vida de los estudiantes y docentes

- ✘ Cree automáticamente cuentas de usuario en AD, Microsoft 365 y Google Workspace utilizando datos de archivos CSV, soluciones HCM y bases de datos Microsoft SQL y Oracle.
- ✘ Modifique los registros de los estudiantes existentes de forma masiva utilizando plantillas basadas en grados y años.
- ✘ Modifique automáticamente las cuentas de los estudiantes existentes (por ejemplo, sus permisos de carpetas y membresía a grupos) utilizando plantillas basadas en reglas en función del año o el cambio de curso.
- ✘ Automatice los procesos de flujo de trabajo para eliminar el acceso a grupos, aplicaciones educativas y carpetas de los estudiantes que se han graduado o desertado, deshabilite sus cuentas y buzones de correo, archívelos durante un número específico de días y, a continuación, elimine la cuenta después de que finalice el período de retención.

## 2. Cree una mejor experiencia de usuario con el SSO y la gestión de contraseñas de autoservicio

- ✘ Permita a los estudiantes y profesores restablecer contraseñas y desbloquear cuentas de AD, Microsoft 365 y otras aplicaciones empresariales sin asistencia de TI.
- ✘ Proporcione a los usuarios acceso con un solo clic a las aplicaciones educativas habilitadas mediante SAML, OpenID Connect y OAuth.

## 3. Proporcione a los usuarios acceso a los recursos educativos desde el primer día

- ✘ Conceda membresías de grupo relevantes justo en el momento de crear el usuario utilizando plantillas de creación de usuarios, que dan a los estudiantes acceso a los recursos relevantes.
- ✘ Asigne y modifique automáticamente el acceso a carpetas compartidas de los usuarios nuevos y existentes para los materiales del curso.
- ✘ Cree plantillas automatizadas mediante la función de orquestación para proporcionar acceso a las aplicaciones de aprendizaje.
- ✘ Cree una cuenta de Microsoft 365 o Google Workspace para los nuevos estudiantes durante el aprovisionamiento de usuario.

## 4. Acceso Just-in-time para los usuarios externos

- ✘ Conceda a determinadas personas acceso a recursos sensibles durante un tiempo limitado.
- ✘ La duración autorizada del acceso se puede especificar al crear políticas de acceso justo a tiempo (JIT).

## 5. Dé a los usuarios el acceso suficiente a los recursos que necesitan

- ✘ Vea informes detallados sobre qué usuarios tienen acceso a las carpetas y recursos confidenciales de los alumnos.
- ✘ Conceda a los usuarios (estudiantes, profesores, personal no docente) el acceso mínimo necesario durante el tiempo requerido para evitar usos no deseados.



## 6. Flujos de trabajo de delegación y aprobación

- ❌ Implemente flujos de trabajo de aprobación para garantizar que todas las solicitudes de acceso, creación y modificación se supervisan antes de su aprobación y para evitar cambios no deseados.
- ❌ Delege las solicitudes repetitivas de los alumnos, como el restablecimiento de contraseñas, el desbloqueo de cuentas y las modificaciones de usuarios, y conceda la membresía a grupos o el acceso a carpetas a los profesores y el personal.

## 7. Mejore la seguridad y el cumplimiento

- ❌ Reciba alertas en tiempo real sobre cambios en archivos y carpetas, creación de usuarios y modificaciones de usuarios para ver quién ha cambiado qué archivo o carpeta, cuándo y desde dónde.
- ❌ Realice copias de seguridad y restaure todos los objetos de AD, Azure AD, Microsoft 365, Google Workspace y Exchange para proteger los datos frente a desastres.
- ❌ Detecte ataques de ransomware configurando alertas en tiempo real y respuestas a amenazas para actividades sospechosas de los usuarios, como inicios de sesión maliciosos e intentos de eliminar datos, y apague los equipos infectados.

## 8. Simplifique los métodos de autenticación mientras garantiza la seguridad

- ❌ Configure políticas de contraseñas personalizadas para OU y grupos.
- ❌ Proporcione una MFA simplificada basada en la capacidad del usuario.
- ❌ Configure la MFA para los inicios de sesión en equipos, aplicaciones en la nube, Microsoft Exchange y VPN de alumnos y profesores.





## Acerca de ManageEngine AD360

AD360 es una solución integrada de gestión de accesos e identidades (IAM) para controlar el acceso a los recursos, reforzar la seguridad y garantizar el cumplimiento. Desde el aprovisionamiento de usuarios, la gestión de contraseñas de autoservicio, el monitoreo de cambios de Active Directory, hasta el inicio de sesión único (SSO) para las aplicaciones empresariales, AD360 le ayuda a realizar todas las tareas de IAM con una interfaz sencilla y fácil de usar.

Con AD360, simplemente puede elegir los componentes que necesita y comenzar a abordar los desafíos de IAM en entornos on-premises, de nube e híbridos desde una sola consola.

[\\$ Cotizar](#)

[↓ Descargar](#)