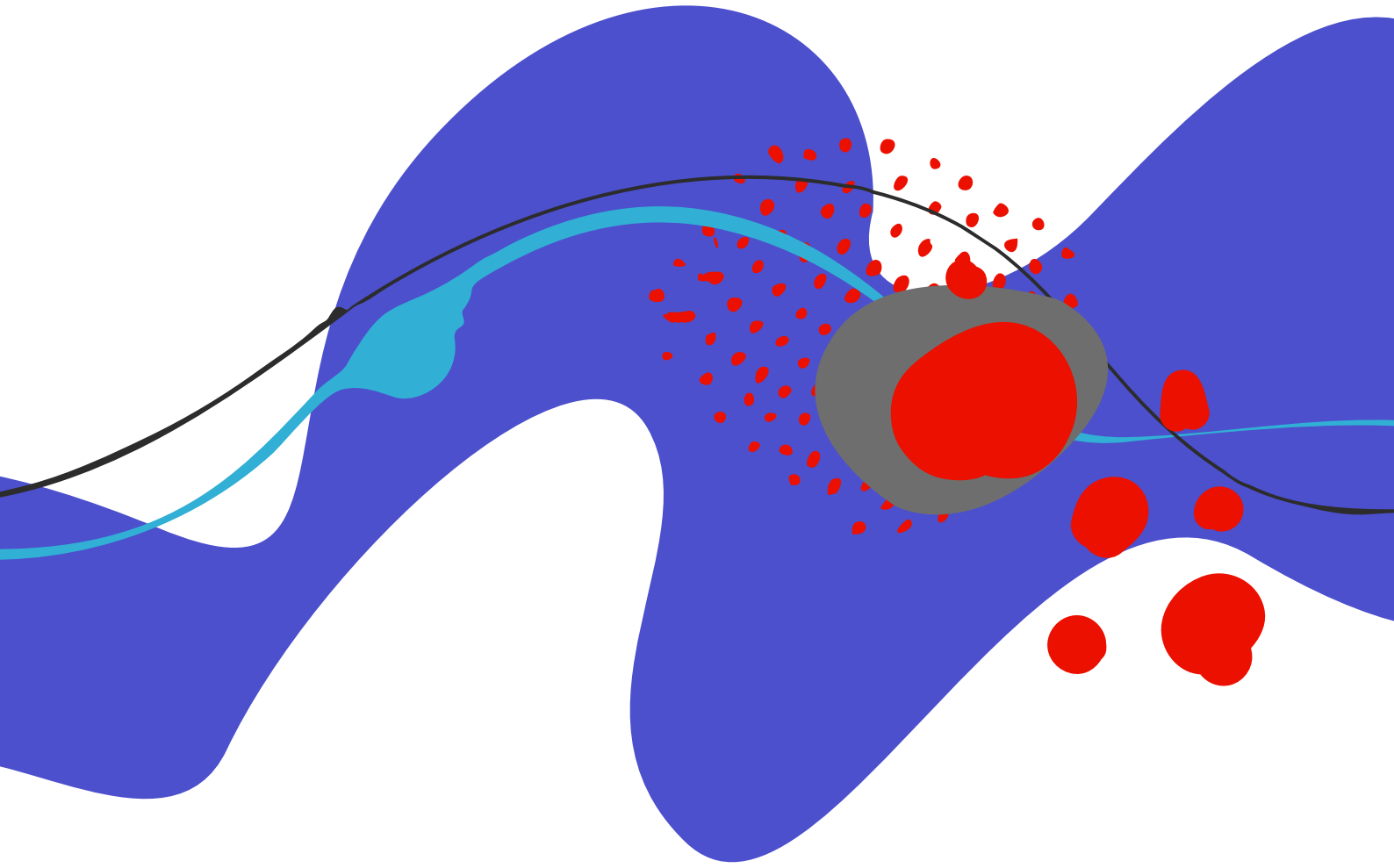
DOCUMENTO TÉCNICO

Servicios de gestión de identidades de servicios Resumen de seguridad



Índice de contenidos

Seguridad de Adobe

En Adobe®, nos tomamos la seguridad de tu experiencia digital muy en serio. Las prácticas de seguridad están profundamente integradas en nuestros procesos de operaciones, desarrollo de software interno y herramientas, y nuestros equipos multifuncionales implementan los controles de Adobe Secure Product Lifecycle (SPLC) a fin de evitar, detectar y responder ante los incidentes de forma oportuna. Además, nos mantenemos al día de las últimas amenazas y vulnerabilidades gracias a nuestra colaboración con partners, investigadores líderes, instituciones de investigación sobre seguridad y otras organizaciones del sector; y trabajamos de forma continua para incorporar tecnologías de seguridad avanzadas en los productos y servicios que ofrecemos.

En este informe técnico se describen el enfoque de defensa en profundidad y los procedimientos de seguridad que implementa Adobe para reforzar la seguridad de la experiencia de los Servicios de gestión de identidades de Adobe y tus datos.

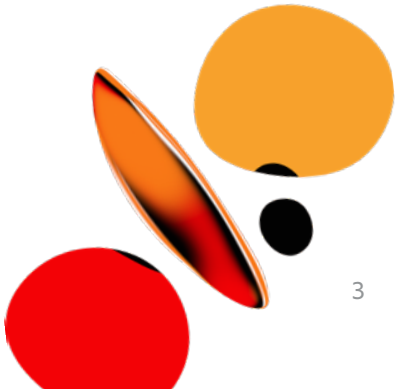
Acerca de los Servicios de gestión de identidades

Los Servicios de gestión de identidades gestionan la autenticación de usuarios finales para cada solución de Adobe y consta de tres (3) componentes:

- **Adobe Identity Service**. Gestiona la autenticación y la validación de los usuarios finales, incluido el inicio de sesión único (SSO) de la federación y el tiempo de ejecución;
- **Adobe Admin Console**. Ofrece una ubicación centralizada para gestionar los derechos de Adobe en toda la organización. Adobe Admin Console gestiona los usuarios, el servicio en la nube y el derecho de las licencias de escritorio, la configuración de la federación y la seguridad de la prevención contra la pérdida de datos; y
- **Adobe User Management API (UMAPI)**. Permite que las organizaciones gestionen los usuarios empresariales y los derechos de la Adobe Admin Console al nivel de la API.

Multilicencia para usuarios designados

La plataforma IMS de Adobe gestiona los derechos y los identificadores únicos, también llamados “licencias de usuario con nombre”, que permiten a los usuarios finales autenticarse en sus aplicaciones de escritorio y servicios en la nube de Adobe implantados.



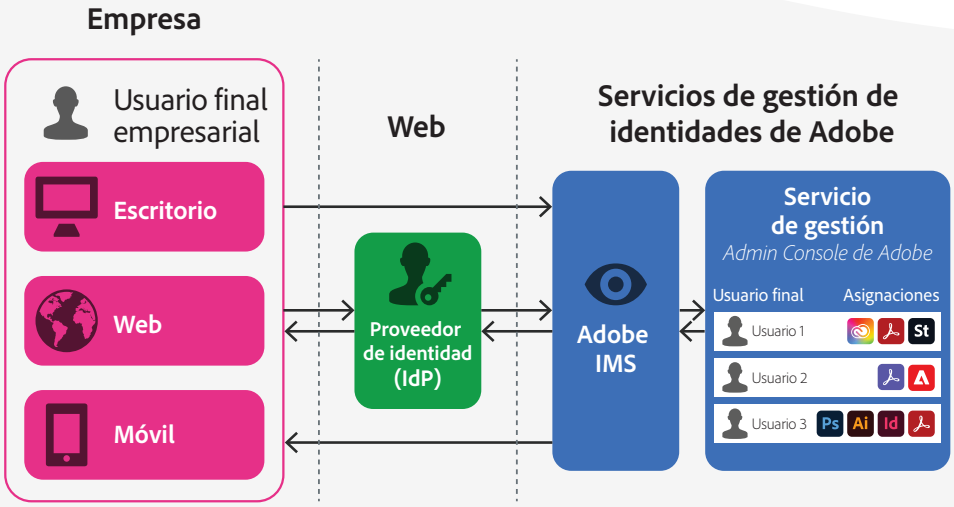


Figura 1: Arquitectura de los servicios de gestión de identidades de Adobe

La figura 1 (arriba) muestra la interacción de un usuario final con el IMS de Adobe utilizando licencias de usuario con nombre. En el ejemplo, el usuario final ha instalado las aplicaciones de Adobe en su ordenador de sobremesa o en sus dispositivos móviles. Cuando un usuario final intenta activar o iniciar una aplicación móvil o de escritorio de Adobe o acceder a un servicio en la nube de Adobe, ese punto final se comunica con el IMS de Adobe.

En función del tipo de identidad del usuario nombrado (véase la siguiente sección), Adobe IMS permite al usuario final iniciar la sesión directamente o pasa el control al proveedor de identidades (IdP) del cliente, que realiza una autenticación SSO federada. Cuando la autenticación es correcta, Adobe IMS verifica los derechos del usuario final y completa su acción solicitada. El usuario final nombrado puede ahora utilizar el software o los servicios a los que tiene derecho.

Tipos de identidades de usuario

Para las implantaciones en empresas, Adobe admite tres (3) tipos de identidad de usuario con nombre:

Business ID es una opción alojada por Adobe y gestionada por la empresa para las organizaciones que utilizan direcciones de correo electrónico fuera de su propio dominio reclamado como identificación del usuario o para los clientes que no han reclamado ningún dominio a efectos de identidad. El Adobe Business ID es la opción preferida para las organizaciones que trabajan con contratistas externos o autónomos que no tienen un ID de organización o un correo electrónico.

Enterprise ID es una opción alojada por Adobe y gestionada por la empresa para las cuentas creadas por los administradores de TI de la organización empresarial. La organización posee y gestiona las cuentas del usuario y todos los activos asociados. Las cuentas de usuario se gestionan a través de la Adobe Admin Console y/o la UMAPI. Los administradores pueden establecer políticas de autenticación para estos usuarios, pero Adobe gestiona completamente la autenticación y las credenciales del usuario.

Federated ID es una cuenta gestionada por la empresa en la que todos los perfiles de identidad son proporcionados por un sistema de gestión de identidades de inicio de sesión único y son creados, poseídos y controlados por la organización de TI de la empresa. Adobe se integra con cualquier proveedor de identidades compatible con SAML 2.0. Las cuentas de usuario se autentican a través del proveedor de identidades y se autorizan a través de la Adobe Admin Console. El proveedor de identidades de la organización controla completamente el establecimiento y la aplicación de las políticas de autenticación. Adobe también admite la conexión y la sincronización con los servicios de Microsoft Azure Active Directory y Google Workspace Directory mediante OpenID Connect para los servicios de identidad federados.

La mayoría de las organizaciones empresariales utilizan identificaciones empresariales o federadas para sus empleados, contratistas y autónomos, siempre que su correo electrónico esté dentro de los dominios reclamados por las empresas. Adobe recomienda el uso de los Business ID si el correo electrónico del usuario final no está dentro de un dominio de la empresa. Para obtener más información, consulta la página Tipos de identidades en Adobe HelpX.

Más adecuado para el uso individual o personal, Adobe no recomienda el uso del tipo de identidad Adobe ID para las implantaciones empresariales.

Gestión de identidades del usuario

Los clientes empresariales pueden gestionar las identidades de los usuarios de forma manual o automática.

Gestión de identidades manuales

Los administradores pueden gestionar manualmente los usuarios, ya sea de forma individual añadiendo, eliminando o cambiando usuarios de uno en uno dentro de Adobe Admin Console o de forma masiva cargando una hoja de cálculo CSV de usuarios en Adobe Admin Console.

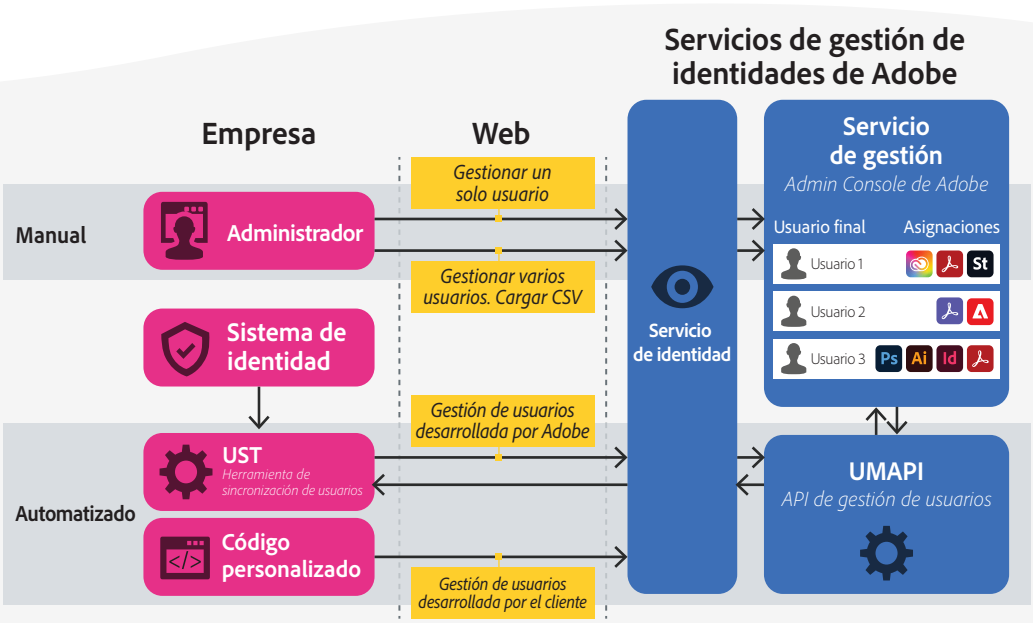


Figura 2: Opciones de gestión de identidades de usuario

Gestión automatizada de identidades

Si un administrador desea gestionar automáticamente los usuarios, puede hacerlo de una de las tres (3) maneras:

- Añade, actualiza o elimina usuarios de forma programada mediante un código desarrollado a medida utilizando **UMAPI**.
- Sincroniza todos los usuarios con los servicios de Microsoft Azure Active Directory y Google Workspace Directory mediante el estándar abierto para la sincronización en la nube **SCIM (System for Cross-domain Identity Management)**.
- Sincroniza usuarios específicos del directorio de la empresa y, a continuación, añade usuarios a los grupos de licencias apropiados o elimínalos de ellos en la Adobe Admin Console mediante **Adobe User Sync Tool (UST)**, un conjunto de scripts en Python desarrollados y mantenidos por Adobe.

Herramienta User Sync

UST lee los datos de identidad de todos los grupos del Protocolo Ligero de Acceso a Directorios (LDAP) del servicio del directorio empresarial, como Microsoft Active Directory y otros directorios compatibles con OpenID Connect, y realiza llamadas REST seguras a UMAPI para crear, actualizar o eliminar usuarios de los servidores de Adobe.

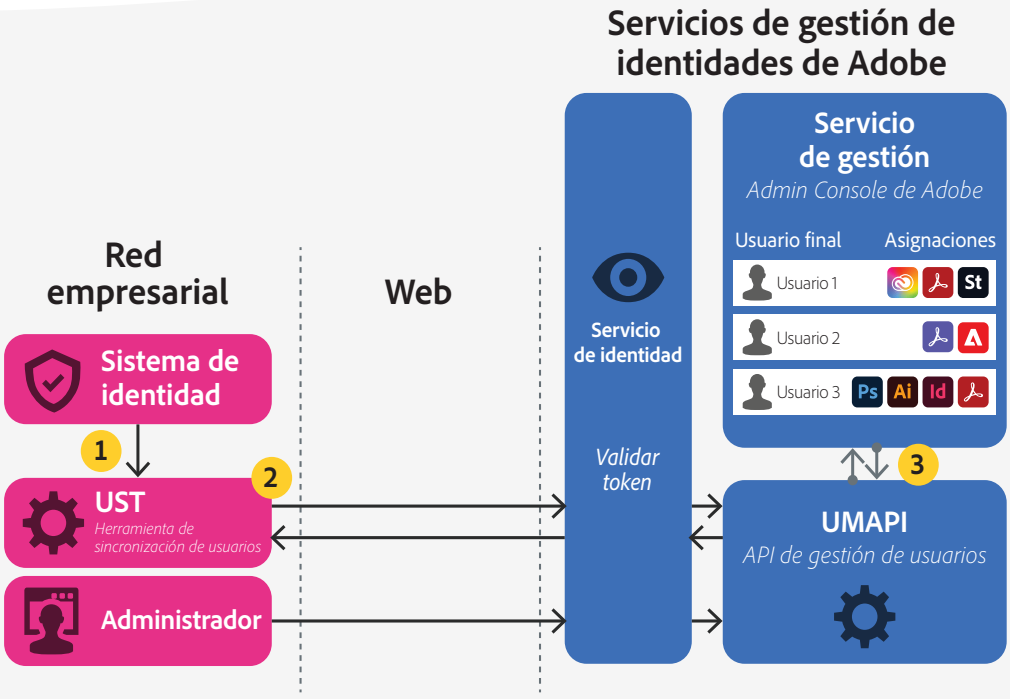


Figura 3: La herramienta de sincronización de usuarios (UST)

Cada vez que la UST se ejecuta:

1. Solicita los registros de los empleados de los grupos del directorio de la empresa. Los grupos y la consulta LDAP pueden personalizarse para adaptarse al entorno específico de la empresa.

2. Solicita a Adobe Admin Console los usuarios actuales y las configuraciones de producto asociadas. La herramienta UST se conecta con la UMAPI a través de llamadas REST por HTTPS utilizando un token de acceso verificado y codificado, que se genera a partir de un JWT firmado y codificado (token web JSON);

3. determina qué usuarios deben crearse, eliminarse o actualizarse en función de las reglas definidas en los archivos de configuración; y

4. realiza los cambios necesarios en la Adobe Admin Console a través de UMAPI, autorizando a los usuarios el software y los servicios adecuados.

La UST puede mantener automáticamente los derechos de Adobe de los usuarios de la empresa sincronizados con sus agrupaciones en el servicio de directorio. Por ejemplo, si se añade un usuario al directorio LDAP, la próxima vez que se ejecute la UST, la UMAPI extraerá la información del usuario del directorio y lo añadirá al grupo adecuado dentro de la Adobe Admin Console. Si un usuario se modifica o se elimina del directorio LDAP, la UST llamará a la UMAPI y realizará la acción correspondiente en la Adobe Admin Console.

Puedes encontrar instrucciones más detalladas sobre cómo instalar, registrar y ejecutar la UST en la página de Configuración de la Herramienta de Sincronización de Usuarios en Adobe HelpX.

Hay más detalles sobre la gestión de usuarios en la página de usuarios de la Adobe Admin Console en Adobe HelpX.

Autenticación de usuarios y Flujo de datos de autorización

Adobe permite la autenticación y autorización de usuarios de dos (2) maneras:

Autenticación y autorización interactivas se produce cuando un usuario inicia sesión explícitamente en una aplicación de escritorio o servicio en la nube de Adobe e introduce su información en un cuadro de diálogo de la interfaz de usuario. En este caso, la autorización se realiza a la perfección y, para el usuario final, parece ser parte del proceso de autenticación.

Adobe también admite la autenticación multifactor (MFA), que proporciona una capa adicional de seguridad al exigir a los usuarios finales que introduzcan conocimientos adicionales específicos para ellos después de que el usuario final se haya autenticado mediante la verificación inicial en dos pasos en la interfaz de usuario. Adobe ofrece políticas para aplicar la MFA a los usuarios de Adobe ID y Business ID. Incluso en el caso en que se implemente la MFA, la autorización se realiza a la perfección y, para el usuario final, parece ser parte del proceso de autenticación.

La autenticación y autorización automatizadas se produce cuando un usuario final se autentica inicialmente mediante la autenticación interactiva. La autenticación automatizada utiliza un token de identificación único para que el usuario final no tenga que volver a conectarse mientras dure la sesión, y la autorización también se produce sin problemas. Cada vez que un usuario final interactúa con una aplicación o servicio y no se le pide que inicie sesión explícitamente, ese usuario final está aprovechando la autenticación automática. Cuando un usuario sale de una sesión, las autorizaciones se vuelven a comprobar en su próxima conexión para verificar los derechos de acceso.

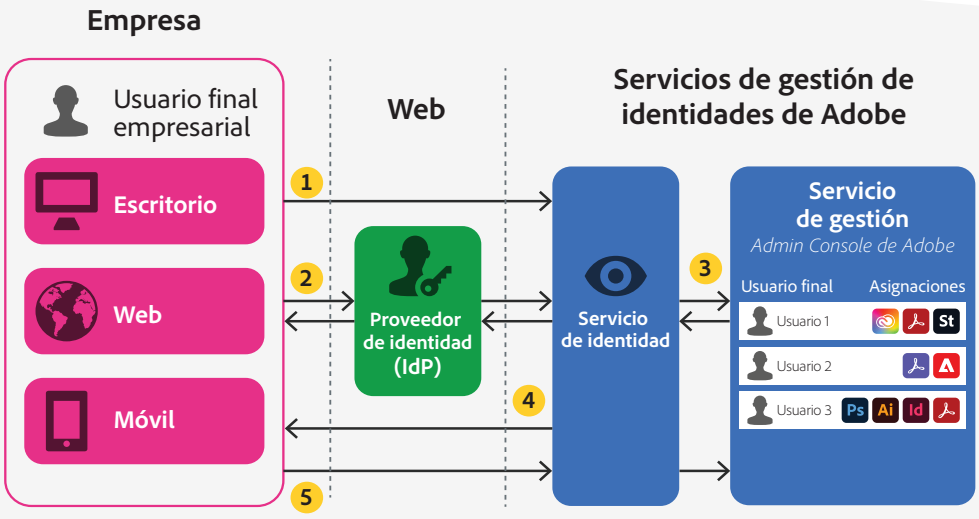


Figura 4: Flujo de datos de autenticación de usuarios de Adobe

Aunque el flujo de datos de autenticación del usuario depende del tipo de identidad específica del usuario, el proceso de autenticación suele incluir los siguientes pasos, que se corresponden con los números del diagrama anterior:

1. El usuario final inicia una aplicación de escritorio o solicita el acceso a un servicio en la nube de Adobe por primera vez. Si utilizan un Business ID o un Enterprise ID, inician la sesión con Adobe IMS.

2. Si la organización utiliza el Federated ID, cuando el usuario final introduce su dirección de correo electrónico o solo el dominio (por ejemplo, @dominiodelaempresa) en el campo de nombre de usuario, Adobe IMS inicia una solicitud SAML, que redirige al usuario final a su proveedor de identidad para que inicie la sesión con sus credenciales corporativas.

3. Una vez que el usuario se ha autenticado correctamente, Adobe IMS lleva a cabo las comprobaciones de aplicación de derechos y políticas necesarias y redirige al usuario al servicio en la nube de Adobe correspondiente o habilita las licencias de aplicaciones de escritorio adecuadas.

4. Adobe IMS almacena un token de dispositivo en el ordenador del usuario final y lo utiliza para generar un token de acceso (similar a un token de sesión de aplicación). Juntos, estos dos tokens se utilizan para generar una licencia firmada para la aplicación, que se cifra y se almacena con el token del dispositivo en la configuración del usuario final. Como el token es independiente del sistema operativo, si el usuario reinicia su sistema, no necesita volver a autenticarse en la aplicación de escritorio o el servicio en la nube de Adobe.

5. En este punto, el usuario final puede utilizar simultáneamente cualquier aplicación de escritorio o servicio en la nube de Adobe sin tener que volver a autenticarse manualmente en cada aplicación (es decir, autenticación automática). Cuando el usuario lanza una nueva aplicación de escritorio en la misma sesión, se pone en contacto con Adobe IMS e intercambia el ID y el token del dispositivo por un token de acceso. Las comprobaciones de la política y las confirmaciones de los derechos tienen lugar durante este proceso. Si, por cualquier motivo, se modifican o revocan los derechos de acceso de un usuario, los tokens de acceso y los tokens de dispositivo pierden su validez.

Adobe ofrece políticas administrativas opcionales que limitan aún más la vida útil de los tokens de acceso al requerir una autenticación más frecuente, lo que puede ser útil para ciertas aplicaciones de Adobe Experience Cloud. Sin embargo, Adobe no recomienda utilizar estas políticas a menos que una empresa tenga requisitos de seguridad específicos.

Datos de identidad

¿Qué datos recopilamos y por qué lo hacemos?

Adobe recopila datos de identidad que garantizan que cada usuario final tenga un ID único para verificarlos a efectos de derechos de licencia y permitir la protección con contraseña de esos derechos, así como del contenido generado y almacenado por el usuario. Para los datos de identidad, Adobe recopila:

- **Nombre de usuario y dominio**: Un identificador del usuario, normalmente una dirección de correo electrónico primaria y válida en formato usuario@dominio. Para los tipos de Business ID y Enterprise ID, es necesario el nombre de usuario completo para iniciar sesión en las aplicaciones y los servicios en la nube de Adobe. Algunas empresas emplean nombres de usuario que no coinciden con sus direcciones de correo electrónico (por ejemplo, nombre de pila frente a usuario@dominio), sin embargo, esto lo controla la empresa. En el caso de los tipos de identidad de Federated ID, es necesario el correo electrónico completo o solo la parte del @dominio para pasar el control al proveedor de identidad adecuado.
- **UID (solo Federated ID)**: Un identificador único asociado al usuario (normalmente la dirección de correo electrónico); Adobe utiliza el UID como clave del proveedor de identidad para buscar al usuario final en Adobe IMS.
- **Contraseña (solo Business ID y Enterprise ID)**: Las contraseñas se codifican de acuerdo con las prácticas recomendadas del sector antes de almacenarlas. Adobe nunca conserva ninguna copia de la contraseña de un usuario en un formato que pueda ser descifrado en una contraseña de texto plano del usuario.
- **Fecha de nacimiento (solo Adobe ID)**: Necesario para cumplir con la Ley de Protección de la Privacidad de Menores de los Estados Unidos (COPPA), el Reglamento General de Protección de Datos (RGPD), y la verificación de la edad para el acceso al sitio web.
- **Código de país**: Los códigos de país ISO Alfa-2 e ISO Alfa-3 del usuario se recogen cuando se crea el perfil de identidad. Por lo general, Adobe utiliza el código de país para determinar la ubicación regional de almacenamiento de activos para el contenido generado por el usuario. Las ubicaciones del Enterprise ID y del Federated ID las define la organización.

- **Nombre y apellido**: Se recopilan cuando se crea el perfil de identidad. Para los tipos de identidad Enterprise ID y Federated ID, los campos UID, Código de país, Nombre y apellido los puede configurar el administrador de TI al crear las cuentas de usuario. Los administradores también pueden determinar la cantidad de información del usuario que se incluye en esos campos.

¿Dónde almacenamos tus datos de identidad?

Independientemente de la ubicación geográfica del cliente, todos los datos de identidad se almacenan en proveedores de infraestructura en la nube multirregional y con equilibrio de carga, con centros de datos situados en Norteamérica (Oregón y Virginia), Europa (Irlanda) y APAC (Singapur). Los datos de identidad se replican en todos los centros de datos por motivos de fiabilidad.

¿Cómo protegemos tus datos de identidad?

Todos los datos de identidad están protegidos en reposo mediante la codificación AES de 256, de conformidad con el Marco de Cumplimiento Común de Adobe (CCF), y cumplen nuestras políticas internas de codificación y almacenamiento de datos confidenciales.

¿Cuánto tiempo almacenamos los datos de identidad?

El contenido se replica y se hace una copia de seguridad en cada centro de datos, en otros centros de datos de la región y en centros de datos interregionales para equilibrar la carga y la redundancia. Las copias de seguridad del centro de datos para los datos de identidad se realizan a diario y se almacenan durante siete (7) días. Adobe también cumple con la legistlación aplicable sobre transferencias de datos transfronterizas.

El usuario final crea, es propietario y controla las cuentas de Adobe ID. En consecuencia, el usuario individual controla el ciclo de vida de la cuenta, aparte de la política de retención indicada en la norma Consumer Personal Information Retention Standard (CPIR) mantener que los tipos de identidad de Adobe ID y Business ID que superen los cuatro (4) años de inactividad no se conserven y se eliminen. Adobe desactiva las cuentas de Adobe ID y elimina la información personal, la contraseña cifrada y los datos de pago asociados a ella a petición del usuario individual o tras 48 meses consecutivos de inactividad.

Tanto para los tipos de identidad de Enterprise ID como de Federated ID, el calendario de eliminación de cuentas lo determina el cliente de la empresa y puede controlarse dentro de la Adobe Admin Console. Cuando una empresa ya no desea tener un Enterprise ID o Federated ID específico asociado a la cuenta de la empresa, un administrador autorizado puede eliminarlo dentro de la Adobe Admin Console. Puedes consultar más detalles en la página de usuario de la Adobe Admin Console en Adobe HelpX.

¿Cómo gestionamos el registro?

Adobe registra las siguientes acciones del usuario:

- Cuando un usuario activa su aplicación o servicio de Adobe
- Cuando un usuario inicia sesión en una aplicación o servicio de Adobe
- Cuando un usuario abre una aplicación de Adobe en su escritorio o dispositivo móvil
- Cuando un usuario utiliza el almacenamiento o los servicios en la nube

Los datos de registro recogidos pueden incluir el ID de usuario, la dirección de correo electrónico y la dirección IP del usuario, así como datos de seguimiento de eventos. Adobe también puede registrar datos analíticos relacionados con el uso de la aplicación y los servicios. Los usuarios pueden cancelar la recopilación de análisis en cualquier momento.

¿Quién puede acceder a tus datos de identidad?

Solo el personal autorizado de Adobe tiene acceso a los datos de identidad y únicamente en función de las necesidades y con los mínimos privilegios, de acuerdo con la certificación ISO 27001 de Adobe. Los datos registrados por Adobe IMS se consideran "más privilegiados" (según la Norma de clasificación y gestión de datos de Adobe) y solo puede acceder a ellos un número aún más restringido de personal de Adobe.

Resumen del programa de seguridad de Adobe

El programa de seguridad integrada de Adobe se compone de cinco (5) centros de excelencia, que reproducen y perfeccionan constantemente los métodos de detección y prevención de riesgos haciendo uso de las tecnologías emergentes y más recientes, como la automatización, la inteligencia artificial y el aprendizaje automático.

Figura 5: Los cinco centros de excelencia en seguridad

Los centros de excelencia del programa de seguridad de Adobe son los siguientes:

- **Seguridad de las aplicaciones**: se centra en la seguridad de nuestros códigos de producto, lleva a cabo investigaciones sobre amenazas e implementa programas de recompensas por errores ("bug bounty").
- **Seguridad operativa**: contribuye a controlar y proteger nuestros sistemas, redes y sistemas de producción en la nube.
- **Seguridad empresarial**: está enfocado en proteger los accesos y la autenticación en el entorno empresarial de Adobe.
- **Cumplimiento normativo**: supervisa nuestro modelo de control de la seguridad, los programas de auditoría y de cumplimiento normativo, y los análisis de riesgos; y
- **Respuesta ante incidentes**: incluye nuestro centro de operaciones de seguridad y respuesta ante amenazas, disponible las 24 horas del día, los 7 días de la semana.

Como parte de nuestro compromiso con la seguridad de nuestros productos y servicios, los centros de excelencia informan a la oficina del director de seguridad de Adobe, quien coordina todos los esfuerzos de seguridad actuales y desarrolla la visión de la evolución de la seguridad en Adobe.

La organización de seguridad de Adobe

La organización de seguridad de Adobe, basada en una plataforma de toma de decisiones transparente, responsable y fundamentada, aúna la amplia variedad de servicios de seguridad en un modelo de control de la seguridad. El director de seguridad de Adobe colabora con los directores de informática y privacidad para garantizar la coordinación en la estrategia y las operaciones de seguridad.

Además de los centros de excelencia descritos anteriormente, Adobe incluye miembros de los equipos de asuntos legales, privacidad, marketing y RR. PP. en la organización de seguridad para garantizar la transparencia y responsabilidad en todas las decisiones relacionadas con la seguridad.

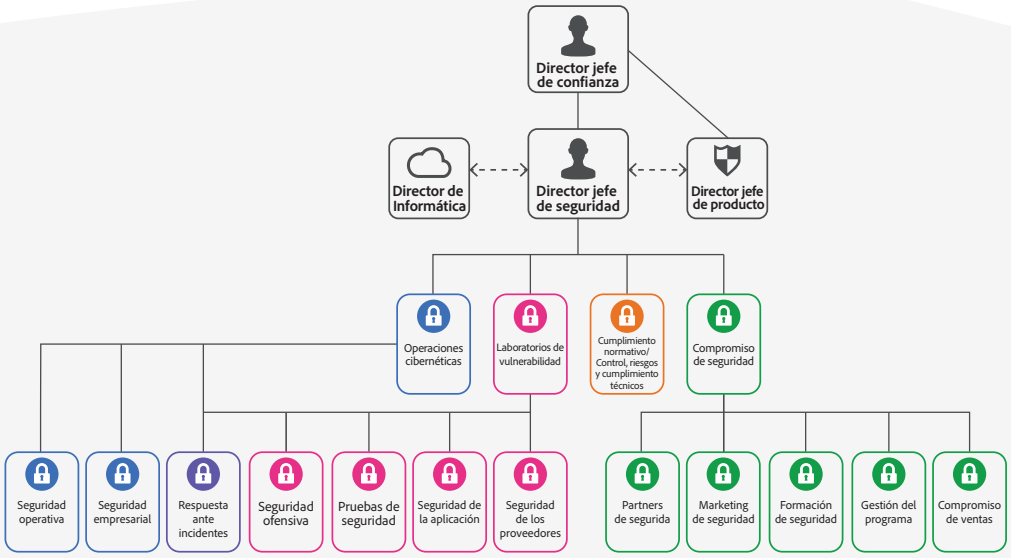


Figura 6: La organización de seguridad de Adobe

Como parte de nuestra cultura de seguridad integral en la empresa, todos los empleados de Adobe deben llevar a cabo nuestra formación de concienciación e información sobre seguridad, que debe realizarse y volverse a certificar cada año. Esto permite garantizar la contribución de cada empleado a la protección de los activos corporativos de Adobe, así como de los datos de nuestros clientes y empleados. En el momento de la contratación, se inscribe de manera automática a nuestros empleados técnicos, incluidos los equipos de ingeniería y operaciones técnicas, en un programa de formación exhaustivo "al estilo de las artes marciales" adaptado a cada función.

La cultura de seguridad y los programas de formación de Adobe se describen con más detalle en el documento técnico sobre la cultura de seguridad de Adobe.

Ciclo de vida seguro de los productos de Adobe

El ciclo de vida seguro de los productos de Adobe (SPLC), que está integrado en varias fases del ciclo de vida de los productos, desde su diseño y desarrollo hasta la garantía de calidad, prueba e implementación, es la base de toda la seguridad de Adobe. El SPLC de Adobe (un conjunto riguroso de varios cientos de actividades de seguridad específicas que abarcan herramientas, procesos y prácticas de desarrollo de software) define procesos claros y repetibles para ayudar a nuestros equipos de desarrollo a integrar la seguridad en nuestros productos y servicios, así como a evolucionar continuamente para incorporar las prácticas recomendadas más recientes del sector.

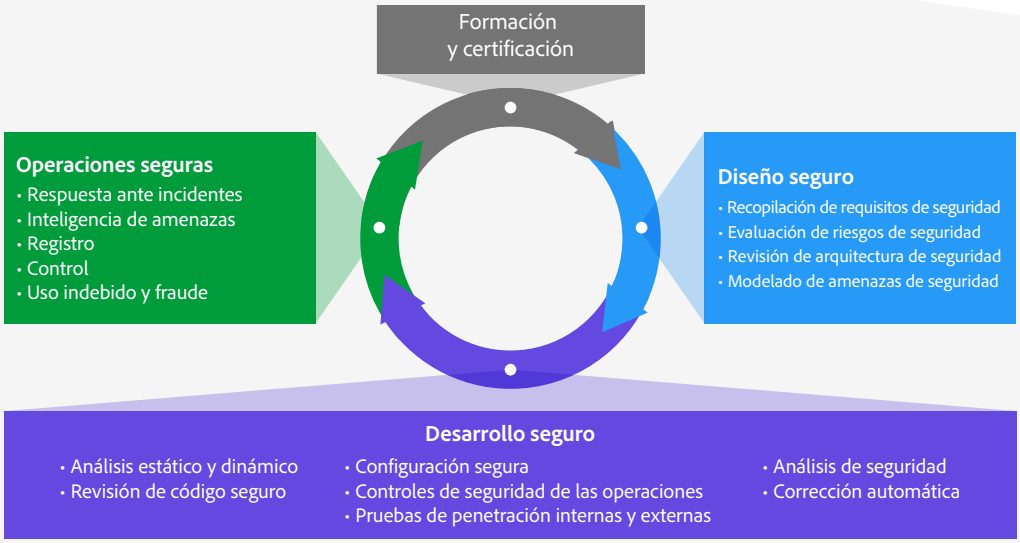


Figura 7: Ciclo de vida seguro de los productos de Adobe

Adobe tiene publicado un estándar de ciclo de vida seguro de los productos que puedes revisar previa solicitud. Puedes obtener más información sobre los componentes del SPLC de Adobe en el Resumen sobre la seguridad de las aplicaciones de Adobe.

Seguridad de las aplicaciones de Adobe

En Adobe, el desarrollo de las aplicaciones con una "seguridad de serie" parte de la Pila de seguridad de las aplicaciones de Adobe. Esta pila combina procesos claros y repetirles basados en una investigación y una experiencia consolidadas con la automatización, que permiten garantizar la aplicación coherente de los controles de seguridad; por lo que contribuye a la mejora de la eficiencia del desarrollo y la minimización del riesgo de que se cometan errores de seguridad. Mediante el uso de bloques de codificación seguros, probados y preaprobados, que eliminan la necesidad de codificar desde cero los patrones y bloques más utilizados, los desarrolladores pueden centrarse en su área de especialización con la tranquilidad de saber que su código es seguro. La Pila de seguridad de las aplicaciones de Adobe, junto con las pruebas, las herramientas especializadas y las supervisión, ayuda a los desarrolladores de software a crear un código seguro de serie.

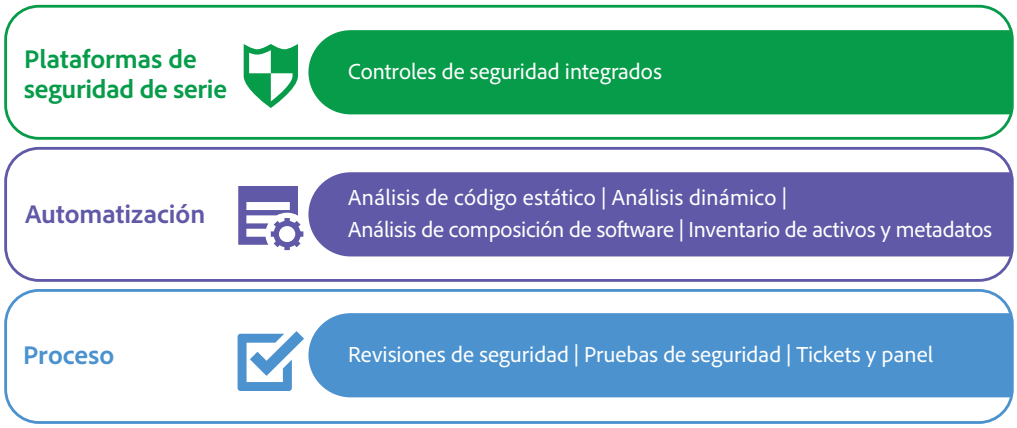


Figura 8: Pila de seguridad de las aplicaciones de Adobe

Adobe también tiene varios estándares publicados sobre la seguridad de las aplicaciones, incluidos los destinados a trabajos específicos para el uso de la infraestructura de la nube pública de Amazon Web Services (AWS) y Microsoft Azure. Puedes revisar estos estándares previa solicitud. El Información general sobre la seguridad de las aplicaciones de Adobe contiene información más detallada sobre las prácticas y procesos de seguridad de las aplicaciones de Adobe.

Seguridad operativa de Adobe

Para garantizar que todos los productos y servicios de Adobe se diseñaran desde su concepción teniendo en cuenta las prácticas recomendadas en materia de seguridad, el equipo de seguridad operativa creó la Pila de seguridad operativa de Adobe. Se trata de un conjunto consolidado de herramientas que ayudan a los ingenieros y desarrolladores de productos a mejorar su enfoque de seguridad y reducir los riesgos tanto para Adobe como para sus clientes. Además, contribuye a garantizar la conformidad con los marcos de cumplimiento, privacidad y otros marcos de control.

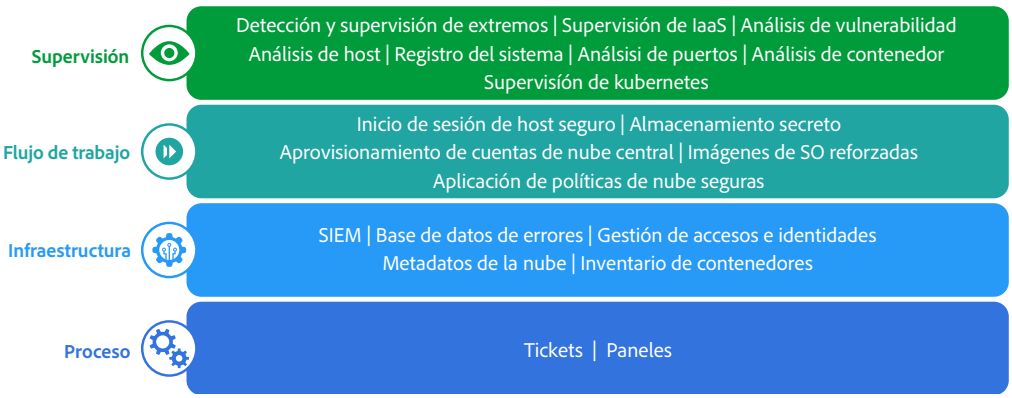


Figura 9: La Pila de seguridad operativa de Adobe

Adobe tiene publicados varios estándares sobre sus operaciones en la nube en curso que puedes consultar previa solicitud. Puedes encontrar una descripción detallada de la Pila de seguridad operativa de Adobe y de las herramientas específicas que se utilizan en Adobe en el Resumen sobre la Pila de seguridad operativa de Adobe.

Seguridad empresarial de Adobe

Además de proteger nuestros productos y servicios, así como nuestras operaciones de alojamiento en la nube, en Adobe utilizamos una serie de controles de seguridad internos para garantizar la seguridad de nuestros sistemas y redes, nuestras ubicaciones físicas corporativas, y los datos de nuestros empleados y clientes.

Puedes consultar más información sobre nuestros controles de seguridad empresarial los estándares que hemos desarrollado para estos controles en el Resumen sobre seguridad empresarial de Adobe.

Cumplimiento normativo de Adobe

Todos nuestros productos y servicios se adhieren al marco Common Controls Framework (CCF) de Adobe, un conjunto de actividades de seguridad y controles de cumplimiento normativo que se implementan dentro de nuestros equipos de operaciones de productos, así como en varias partes de nuestros equipos de aplicaciones e infraestructura. En la medida de lo posible, Adobe aprovecha innovadores procesos de automatización para alertar a los equipos de posibles casos de incumplimiento normativo, además de para garantizar una mitigación y un reajuste rápidos.

Los productos y servicios de Adobe cumplen los estándares legales aplicables o pueden utilizarse de una forma que permite a los clientes cumplir las obligaciones legales relacionadas con el uso de proveedores de servicio. Los clientes mantienen el control de sus documentos, datos y flujos de trabajo, y pueden elegir la forma que estimen oportuna de cumplir con las normativas locales y regionales, como el Reglamento General de Protección de Datos (RGPD) de la UE.

Asimismo, Adobe cuenta con una formación en cumplimiento normativo y estándares relacionados disponibles para su revisión previa solicitud. Para obtener más información sobre el CCF de Adobe y las certificaciones principales, consulta la lista de normativas de cumplimiento, estándares y certificaciones de cumplimiento normativo de Adobe.

Respuesta ante incidentes

En Adobe, nos esforzamos por garantizar que nuestra gestión de riesgos y vulnerabilidades, respuesta ante incidentes, mitigación y proceso de resolución sean ágiles y precisos. Monitorizamos continuamente el panorama de las amenazas, compartimos conocimientos con expertos en seguridad de todo el mundo, resolvemos incidentes de forma rápida cuando ocurren, y devolvemos esta información a nuestros equipos de desarrollo para lograr los niveles más altos de seguridad en todos los productos y servicios de Adobe.

También mantenemos estándares internos para la gestión de vulnerabilidades y la respuesta ante incidentes, que puedes revisar previa solicitud.

Puedes encontrar más información acerca del proceso de notificación y respuesta ante incidentes de Adobe en el Resumen de respuesta ante incidentes de Adobe.

Continuidad empresarial y recuperación frente a desastres

El programa Continuidad empresarial y recuperación frente a desastres de Adobe (BCDR, por sus siglas en inglés) se compone del Plan de continuidad empresarial (BCP) y Planes de recuperación frente a desastres (DR) específicos de productos, que contribuyen a garantizar la disponibilidad y entrega continuas de los productos y servicios de Adobe. Nuestro programa BCDR, que cuenta con la certificación ISO 22301, mejora nuestra capacidad de responder ante el impacto de las interrupciones imprevistas, mitigarlo y recuperarnos de él. Puedes obtener más información sobre el programa BCDR de Adobe en el Resumen sobre el programa de continuidad empresarial y recuperación frente a desastres de Adobe.

Conclusión

El enfoque proactivo con respecto a la seguridad y los estrictos procedimientos descritos en este documento contribuyen a proteger la seguridad de las soluciones de Adobe, así como tus datos confidenciales. En Adobe, nos tomamos muy en serio la seguridad de tu experiencia digital, por lo que monitorizamos continuamente la evolución del panorama de amenazas a fin de adelantarnos a las actividades malintencionadas y garantizar la seguridad de los datos de nuestros clientes.

Para obtener más información sobre la seguridad de Adobe, ve al Centro de confianza de Adobe.

Adobe

12/22