Un pantallazo sobre el Ciclo de Vida de la Identidad Digital (v2)

Por Andrew Cameron y Olaf Grewe

Tabla de contenidos

Resumen

Una identidad digital atraviesa varias etapas a lo largo de su existencia: desde su creación, pasando por modificaciones en respuesta a diferentes eventos, hasta su desactivación o eliminación. Este artículo aborda los diferentes tipos de identidad digital que deben ser gestionados, además de las diferentes etapas de esta, describiendo su ciclo de vida de principio a fin, dentro o a lo largo de múltiples sistemas. La intención de este artículo es abarcar los ciclos de vida que pueden aplicarse en la mayoría de los casos de uso de B2B (“negocio a negocio”, por sus siglas en inglés), B2C (“empresas a consumidores”, por sus siglas en inglés) y B2E (“empresas a empleados”, por sus siglas en inglés).

Introducción a la identidad digital

Para el propósito de este artículo, la identidad digital se define como la combinación de un identificador único con los atributos relevantes que identifican exclusivamente a una entidad. Dependiendo de la complejidad del entorno en el cual es usada la identidad digital, su ciclo de vida -desde su concepción hasta su cierre- puede ser bastante más complicado que simplemente crear, leer, actualizar y borrar (CRUD, por sus siglas en inglés).[1]

Las fases del ciclo de vida varían dependiendo del tipo de identidad (humana como Fuerza laboral o Cliente, y no-humana como un Sistema o Dispositivo). La IAM ("Administración de Identidades y Accesos", por sus siglas en inglés) de empresa es un conjunto establecido de procedimientos que determina los procedimientos y capacidades de gobernanza necesarios para garantizar que solo las personas indicadas (a través de sus cuentas) tengan acceso únicamente a las aplicaciones requeridas (recursos). La IAM de cliente tiene un conjunto de requerimientos completamente diferente que representa valor a un negocio, ya que por su naturaleza se define por las interacciones con un cliente. Una interacción deficiente con un cliente puede tener efectos negativos en una empresa. Por estas razones, los diferentes tipos de identidad requerirán sistemas y procedimientos separados para darles soporte:

Tipo de Identidad	Descripción
Fuerza laboral	Una identidad de Fuerza Laboral es creada para funcionar dentro del contexto de una empresa, incluyendo Negocio-a-Negocio (B2B) y/o Negocio-a-Empleado (B2E). Algunos ejemplos de estos tipos de identidad son empleados, proveedores, contratistas u otras identidades humanas que dan soporte a la fuerza laboral corporativa.
Cliente	El tipo de identidad de cliente suele funcionar fuera del marco empresarial, habilitando negocios digitales entre el dueño de la identidad de cliente y la empresa. Suele haber múltiples canales de acceso (web, móvil, dispositivo del Internet de las cosas [IoT, por sus siglas en inglés]) para administrar un conjunto más grande de datos de identidad (atributo de identidad) necesario para facilitar la interacción.

[1] "Crear, leer, actualizar, borrar" ldapwiki.com, página modificada por última vez el 19 de marzo de 2020, https://ldapwiki.com/wiki/Create%20Read%20Update%20Delete.

Dispositivo o Sistema	Los Dispositivos de identidad son comúnmente utilizados para proveer información y representación en una red digital. Las Identidades de Sistema son usadas para autenticar servicios (por ej., aplicaciones o procesos basados en servidores) ante una red.

Terminología

- Identidad digital –la combinación de un único identificador con atributos relevantes que identifican exclusivamente una entidad.
- Creación basada en el trayecto del usuario – El proceso mediante el cual se guía al cliente a través de una serie de interacciones previas a establecer una identidad digital. Por ejemplo, capturar de un cliente la mínima y básica información para habilitar la creación de una identidad.
- Atributos - Pares clave/valores relevantes para la identidad digital (nombre de usuario, primer nombre, apellido, etc.).
- Interorganizacional (Federación): Una organización depende de la identidad digital de otra organización y de los procesos de administración del ciclo de vida.
- Intra-organizacional (Inicio de Sesión Único): Una identidad digital central, como una cuenta en un directorio, es asociada como autoridad por sistemas de bajada de datos con el propósito de autenticar.

Ciclos de vida de la identidad

Para cada fase "de creación" del ciclo de vida, una identidad digital es creada como un identificador único en un sistema de registro. Puede ser creada como parte de un proceso del negocio (fuerza laboral o identidad de dispositivo) o transparentemente como parte del trayecto del usuario (identidad de cliente).

A lo largo de su ciclo de vida, una identidad digital habilita transacciones digitales a través de todas las cuentas asignadas y de los derechos otorgados a dichas cuentas. Si bien en este documento se describe el ciclo de vida como un *continuum*, el lector debe saber que:

- En la mayoría de las organizaciones, el ciclo de vida de la identidad digital puede estar distribuido a través de varias soluciones técnicas.
- Algunos pasos del ciclo de vida (por ej., autenticar, usar) ocurrirán más frecuentemente que otros (por ej., unificar, borrar).

Identidad de la fuerza laboral

El ciclo de vida de la identidad de fuerza laboral se aborda a través de tres procesos de negocio principales: incorporación, traslado o baja. El proceso de **incorporación** cubre todas las fases del ciclo de vida que facilitan la creación de recursos (identidades, cuentas, membresías de grupos, etc.) que habilitan la identificación y el acceso en un entorno empresarial. El proceso de **traslado** permite cambios o actualizaciones en el estado de la

identidad que aún está vinculada al entorno empresarial y toma en cuenta los procedimientos de atestación necesarios para verificar los permisos de acceso y derechos. El proceso de **baja** cubre la serie de pasos que deben realizarse cuando se elimina el acceso de una identidad al entorno empresarial.

La Figura 1 describe las fases IAM de la fuerza laboral en el procedimiento:

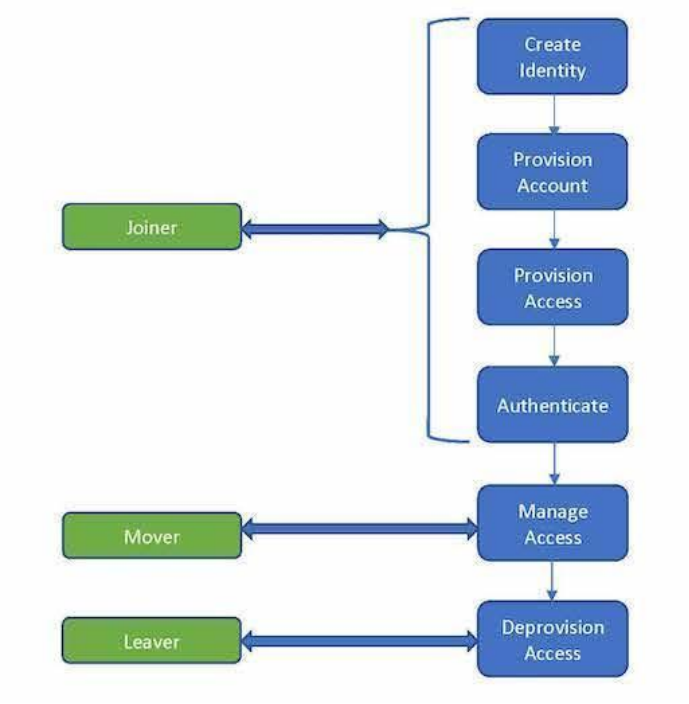


Figura 1 – Procedimientos centrales de IAM

El siguiente recuadro describe las fases que dan soporte al ciclo de vida de la identidad de fuerza laboral:

Fase del ciclo de vida	Descripción

Crear una identidad	La creación de una identidad de fuerza laboral como parte de un proceso de negocio (empleados, proveedores, etc.) suele ir de la mano con la recolección de pruebas para establecer el conjunto mínimo de atributos que se asociará con el identificador. La creación de una identidad digital puede ser automatizada (por ej., sincronizada con un evento del sistema de recursos humanos), especialmente cuando las identidades digitales son generadas a escala por motivos varios como una fusión o una adquisición. Los procedimientos de inscripción de las entidades de fuerza laboral suelen involucrar a otras entidades humanas (como un gerente de línea o agente de administración autorizado) para validar la prueba provista. En países que carecen de un sistema de identidad nacional establecido (Estados Unidos, Reino Unido, Australia, etc.) es posible que se requieran varios documentos como prueba (licencia de conducir, pasaporte, factura de servicio, tarjeta de crédito/estado de cuenta) en lugar de un documento de identidad nacional.
Aprovisionar cuenta	La creación de cuentas en sistemas de empresa basadas en reglas de negocio y accesos requeridos a recursos.
Aprovisionar acceso	La creación de privilegios asociando cuentas de usuarios con objetos que habilitan el acceso a recursos corporativos en los sistemas requeridos. Los privilegios suelen estar representados por valores de atributos, membresías en grupos o por el alineamiento organizacional. Las reglas de negocio definirán el acceso a un recurso basándose en los privilegios empresariales.
Autenticar	Solicitar a una cuenta de usuario que valide una credencial antes de permitir el acceso a una red o a un recurso.
Administrar el acceso	Validar el acceso que se le ha otorgado a una cuenta y aprobar el acceso continuo a recursos corporativos. La certificación de acceso es un procedimiento que valida todos los accesos actuales y puede ser utilizado para eliminar un acceso que ya no es necesario. El procedimiento de atestación para verificar y otorgar acceso es un componente crucial y suele ser subestimado dentro de un sistema IAM maduro. Las identidades digitales suelen estar sujetas a actualizaciones, principalmente de sus atributos. A veces, incluso el identificador puede cambiar. Un ejemplo es la identidad digital donde el nombre de usuario es el mismo que el identificador (por ej., la dirección de correo electrónico). Un usuario puede querer cambiar su nombre de usuario por varios motivos como un cambio de nombre real en su vida o por un

	cambio de preferencias. Para profundizar en el tema, refiérase al artículo de Ian Glazer “Identificadores y nombres de usuario”.[2] Actualiza con frecuencia los casos de uso que describen las capacidades del flujo de trabajo que involucren requerimientos de aprobación, establecimiento o notificación. Estos controles son importantes para enfrentar los riesgos de usurpación de identidad. Dependiendo del valor de la identidad digital en la organización, las actualizaciones de las identidades digitales pueden estar sujetas a la demostración del tipo de inscripción.
Desaprovisionamiento de acceso	Eliminar el acceso a uno o todos los recursos corporativos. La necesidad de esta eliminación puede surgir como resultado de un proceso de baja o de una validación proveniente de una certificación de acceso. Cuando una identidad digital ya no es necesaria debería ser deshabilitada en el sistema de registro. Esta acción no implica solamente la deshabilitación o eliminación en un directorio central sino también dar de baja en los sistemas que mantienen registros asociados con esta identidad digital, así como en los repositorios de registro y auditoría. Únicamente cuando el identificador usado para esta identidad digital haya sido borrado de todos los sistemas, se puede considerar que la identidad digital fue genuinamente eliminada. Encuentre una discusión detallada sobre la importancia de la deshabilitación o eliminación de cuentas siguiendo los procedimientos actuales más adecuados en el artículo de Andrew Hindle “El Impacto del RGPD en la identidad y la gestión de acceso”.[3]

Identidad de cliente

Recientemente, la IAM de cliente ha evolucionado para dar soporte a los procesos que gobiernan la experiencia de usuario de los consumidores cuando interactúan con el negocio digital. Las soluciones de CIAM (“Identidad del Cliente y Gestión de Accesos”, por

[2] Glazer, Ian, “Identificadores y Nombres de Usuario,” Cuerpo de Conocimiento de IDPro, 31 de marzo de 2020, https://bok.idpro.org/article/id/16/.

[3] Hindle, Andrew, “Impacto del RGPD en la identidad y la gestión de acceso”, Cuerpo de Conocimiento del IDPro, 31 de marzo de 2020, https://bok.idpro.org/article/id/24/.

sus siglas en inglés) han sido desarrolladas para proveer a las compañías datos de valor agregado sobre recolectados de los clientes como resultado de las experiencias que los mismos han tenido con servicios y sitios web corporativos. Las experiencias de los clientes son descritas en su mayoría como parte del "trayecto del usuario" que representa las interacciones (autenticación, registro, actualización de perfil) que tiene el cliente al relacionarse con recursos digitales tales como sitios web, aplicaciones de móvil o interfaces IoT.

El siguiente diagrama describe las fases del ciclo de vida de CIAM:

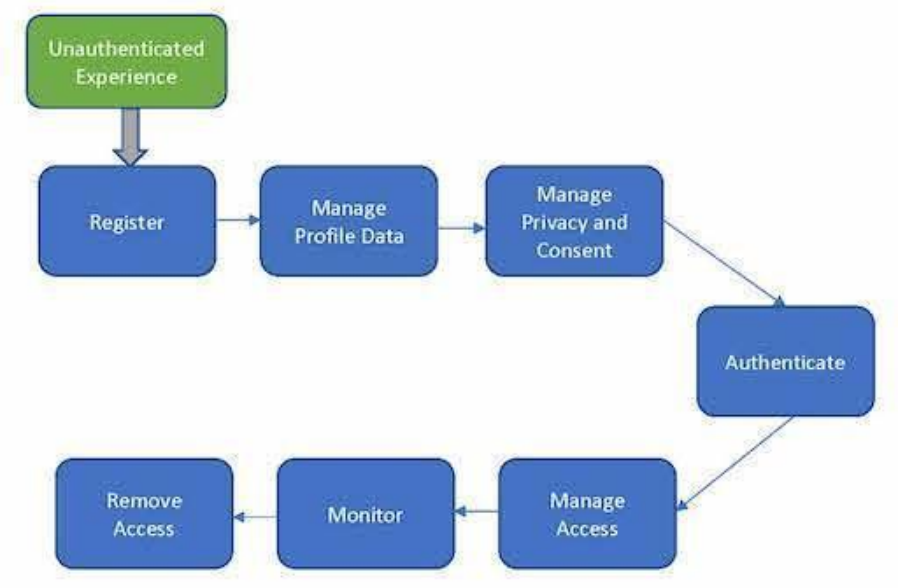


Figura 2 – El Ciclo de vida de la identidad de cliente

El siguiente recuadro describe las fases que dan soporte al ciclo de vida de la identidad de cliente:

Fase del ciclo de vida	Descripción
Registro	La primera parte del viaje de usuario es la creación de una identidad de cliente a través de un proceso de registro. Típicamente, el registro ocurre cuando se requiere de una identidad digital para habilitar una experiencia determinada. Como parte del trayecto, se recopila información del usuario, al que se le permite consentir el uso que se dará a la información recolectada. El registro suele ser una interacción única con el usuario que concluye con la confirmación del cumplimiento del motivo del flujo (por ej. "Su cuenta ha sido creada"). Las interacciones de registro también pueden ser transparentes para el usuario si han sido habilitadas a través de una identidad federada como iniciar sesión con una cuenta de red social (por ej. "Para registrarse ingrese con su cuenta de Facebook"). El registro no requiere atributos obligatorios más allá de los pasos de vinculación en el trayecto del usuario hacia el identificador. Dependiendo de la naturaleza de la transacción digital, las identidades de clientes pueden requerir garantías sobre varios atributos. En este punto es clave recopilar los atributos usados para establecer la propiedad (o la recuperación) de una identidad digital, ya sea a través de medios humanos o no-humanos.
Administrar datos del perfil	Cada cliente tiene un perfil y administrar los datos de este involucra una experiencia de usuario que permite al cliente actualizar sus datos a través de los recursos corporativos (sitios web o aplicaciones de móvil). Esta fase se aplica principalmente a las identidades digitales basadas en el trayecto del usuario. Para que los servicios digitales puedan continuar el trayecto del usuario, es necesario enriquecer las identidades digitales con atributos que sean específicos con la forma en la que el usuario accede al servicio. Dos técnicas comunes para esto son las cookies o las huellas digitales de dispositivos - encuentre un ejemplo de las últimas en el sitio de EFF Panopticlick-.[4]
Administrar la privacidad y el consentimiento	El ciclo de vida del cliente debe incluir un procedimiento que informe y habilite al cliente al cumplimiento de sus derechos en lo que refiere al conocimiento y consentimiento de lo que puede suceder con su información.
Autenticar	Como parte del flujo de trabajo y previo al acceso a cualquier servicio de cliente, el cliente debe validar su credencial.

[4] "Panopticlick 3.0," Fundación *Electronic Frontier*, vista el 13 de abril de 2020, https://panopticlick.eff.org/.

Administrar el acceso	El ciclo de vida del cliente requiere gestionar el acceso a los servicios de negocios basados en interacciones con clientes. El usuario puede también elegir proveer atributos adicionales. Típicamente, el servicio permite al cliente crear un nombre de usuario y contraseña para iniciar sesión una vez que su sesión actual expire. En esta etapa, un servicio puede combinar varios identificadores creados por diferentes dispositivos (móvil, escritorio, laptop, etc.). En esta etapa, la identidad digital es considerada como seudónimo ya que no hay garantías sobre los atributos provistos por el usuario.
Monitoreo	Una vez completadas las fases iniciales, el ciclo de vida del cliente pasa a la fase de monitoreo donde el proceso de minar/recolectar datos sobre el usuario y sus experiencias dan soporte a una variedad de negocios, y ocurren requerimientos del consumidor. Desde un punto de vista de seguridad, el monitoreo de datos puede ser usado para notificar al cliente sobre la filtración de credenciales u otros datos. El negocio también puede beneficiarse al hacer uso del historial de la actividad del cliente mediante un servicio de analítica.
Eliminar acceso	La eliminación de acceso de un cliente suele darse como resultado de una solicitud de este o por inactividad.

Identidad de dispositivo o sistema

La identidad de dispositivo o sistema es un área en desarrollo en un contexto donde los dispositivos poseen crecientes niveles de capacidad tecnológica, lo cual incrementa la necesidad de identificarlos y administrarlos mediante un ciclo de vida. Por ejemplo, los automóviles tienen decenas de sistemas internos que requieren capacidades de administración sofisticadas sobre la vida de la identidad del vehículo. En el extremo opuesto, algunos monitores simples pueden conectarse a una red y proveer únicamente un valor de temperatura o alguna otra información básica. Cualquiera sea el caso, todos los dispositivos necesitan fases específicas de ciclo de vida para ser administrados en función de sus capacidades.

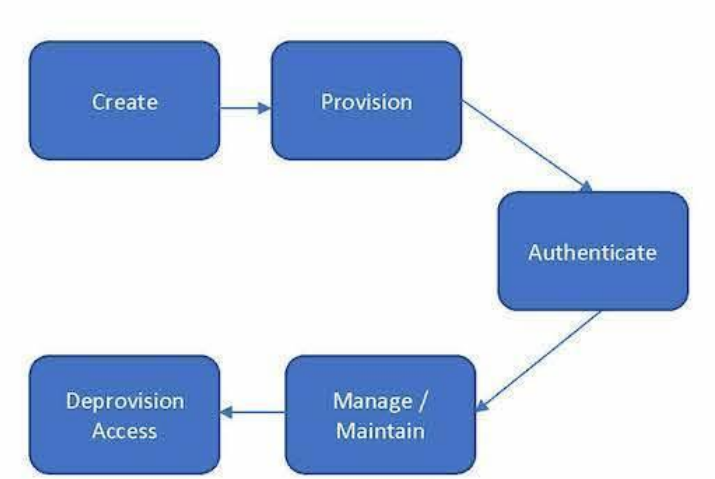


Figura 3 – El ciclo de vida de una identidad de dispositivo

El siguiente recuadro describe las fases de un modelo simple que da soporte al ciclo de vida de la identidad de dispositivo:

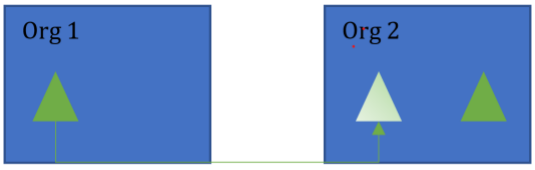
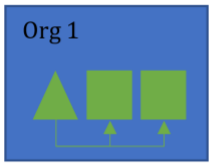
Fase del ciclo de vida	Descripción
Crear	La primera fase en el ciclo de vida del dispositivo o sistema es iniciar el procedimiento de creación del identificador que se asignará al dispositivo o sistema.
Provisionar	Cuando el identificador es asignado, comienza el procedimiento de habilitar el dispositivo o sistema para que sea reconocido, monitoreado y administrado. El aprovisionamiento del dispositivo se hace utilizando algún tipo de certificado o infraestructura PKI para garantizar que únicamente los dispositivos conocidos puedan interactuar con los recursos corporativos.
Autenticar	La autenticación del dispositivo o sistema se hace usando una infraestructura PKI que garantiza que el dispositivo conectado es conocido y tiene permiso para interactuar con la red.
Administrar / Mantener	Una vez completadas las fases iniciales, el dispositivo o sistema debe ser monitoreado para determinar si el mismo necesita alguna acción de mantenimiento. Siguiendo una práctica adecuada de seguridad TI, las credenciales (contraseñas) asociadas a identidades no-humanas deben ser cambiadas regularmente para asegurar la protección contra los ataques de fuerza bruta basados en contraseñas.
Desaprovisionamiento de acceso	Cuando el dispositivo o sistema ya no está en uso (determinar esto puede requerir procedimientos diferentes a los de las identidades de la

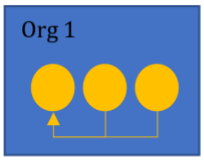
	fuerza laboral o de las identidades digitales de clientes), se debe eliminar el acceso del dispositivo o sistema del sistema de registro, deshabilitando así cualquier acceso a la red corporativa.

Otras relaciones de identidad digital

Algunas transacciones digitales requieren una organización para establecer relaciones entre emisores de identidad digital, también conocidos como proveedores de identidad. Estas relaciones pueden darse con socios externos (por ej. una relación B2B) o dentro de varias aplicaciones de empresa (por ej. un entorno de inicio de sesión único). Las identidades digitales pueden también estar relacionadas con otras identidades dentro de una organización para establecer una autoridad delegada o para administrar requerimientos de control dual. En todos estos casos, las relaciones suelen ser administradas ya sea como atributos de la identidad digital (por ej. identificadores para los servicios permitidos) o como puntos de datos separados en un directorio central (por ej. la membresía de un grupo LDAP ["Protocolo Ligero de Acceso a Directorios", por sus siglas en inglés]).

Algunos tipos comunes de relaciones son:

Interorganizacional (Federación)	 Inter-organizational Una organización depende de la identidad digital y de los procedimientos de administración del ciclo de vida de otra organización.
Intra-organizacional (Inicio de Sesión Único)	 Intra-organizational Una identidad digital central, como una cuenta en un directorio, es asociada como autoridad por sistemas de bajada de datos con el propósito de autenticar.

Inter-entidad (Delegación)	 Inter-entity La delegación implica asignar un subconjunto de autoridad de una identidad que se encuentra dentro de un dominio de negocio a una identidad que reside dentro de otro dominio de negocio. En este ejemplo, el dominio de negocio se refiere a los límites definidos que existen dentro de una entidad, lo cual habilita el cumplimiento de políticas. Algunos ejemplos de dominios de negocio son: una compañía, una organización (dentro de una compañía) o incluso un equipo de trabajo (dentro de una organización). La autoridad se otorga ya sea de forma explícita o basándose en reglas de negocio (políticas) definidas en el nivel de dominio.
Intra-entidad	 Intra-entity Ya sean requisitos impulsados por los usuarios o por fuera de la organización, una relación es establecida entre varias identidades digitales para identificar a un humano único o a una entidad no-humana como el propietario/la propietaria.

Conclusión

La complejidad del ciclo de vida de la identidad digital se hace evidente con el transcurso de los años y a medida que se incorporan más funcionalidades a los sistemas. Por lo tanto, se recomienda abordar los requisitos del ciclo de vida con una visión a largo plazo y asegurar que las capacidades de administración del usuario sean expandibles.

Agradecimientos

El autor agradece a Ian Glazer por articular la progresión de una identidad del anonimato al seudonimato y lo conocido. A Dean Saxe que contribuyó a la clasificación de relaciones. A John Lehtinen y Heather Flanagan que me motivaron y sufrieron conmigo mientras redactaba los primeros borradores de este artículo.

Registro de cambios

Fecha	Cambio
28-02-2022	Actualizada la definición de identidad digital; esclarecido el uso del término ‘ciclo de vida’; diagramas actualizados, descripción de delegación actualizada.
30-10-2020	V1 publicada