Seguridad de aplicaciones en la nube: gestión de la identidad digital

PID_00286166

Ignasi Oliva Corrales
Jordi Guijarro Olivares

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Ignasi Oliva Corrales

Director de innovación en *blockchain* y tecnologías DLT en i2CAT (http://www.i2cat.net), el Centro de Investigación en Internet. Ingeniero técnico en informática de sistemas por la Facultad de Informática de Barcelona (FIB) y Máster en Tecnologías *Blockchain* por la Universidad Politécnica de Catalunya (UPC - BARCELONATECH). Experto en tecnologías blockchain, identidad y firma digital e innovación, ha participado en proyectos de innovación y transformación digital en el sector público y privado.

ignasi.oliva@i2cat.net

Jordi Guijarro Olivares

Director de innovación en ciberseguridad en i2CAT (http://www.i2cat.net), el Centro de Investigación en Internet. Ingeniero en Informática por la Universitat Oberta de Catalunya (UOC) y Máster en Gestión de las TIC por la Universidad Ramon Llull (URL). Experto en *cloud computing* y ciberseguridad, ha participado en proyectos de investigación e innovación de la comisión europea del programa Horizon 2020.

jordi.guijarro@i2cat.net

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Jorba Esteve

Primera edición: febrero 2022
© de esta edición, Fundació Universitat Oberta de Catalunya (FUOC)
Av. Tibidabo, 39-43, 08035 Barcelona
Autoría: Ignasi Oliva Corrales, Jordi Guijarro Olivares
Producción: FUOC
Todos los derechos reservados

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea este eléctrico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita del titular de los derechos.

Índice

1. Introducción a la identidad digital

Tal y como se recoge en el artículo 6 de la Declaración Universal de los Derechos Humanos y el artículo 16 del Pacto internacional de los Derechos Civiles y Políticos, toda persona tiene el **derecho a ser reconocida como persona** ante la ley.

Son diversos los instrumentos internacionales de los derechos humanos, como el artículo 7 de la Convención sobre los Derechos de los Niños y el 24.2 del Pacto Internacional de los Derechos Civiles y Políticos, que reconocen el derecho al registro de los nacimientos para poder **disponer de una identidad**.

Prueba de estos derechos se refleja en los objetivos del desarrollo sostenible (ODS), concretamente en el 16.9, de la Organización de las Naciones Unidas (ONU) que exige la **identidad legal para todas las personas**, objetivos que se quieren conseguir en 2030.

Figura 1. Los 17 objetivos del desarrollo sostenible

Fuente: ONU

La **identidad digital** según la norma ISO/IEC 24760-1 define la identidad como un conjunto de atributos, compuestas por características o propiedades, relacionados con una entidad, persona, organización, objeto o sistema.

El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos define la identidad digital como:

> «La identidad digital es la representación única de un subjeto involucrado en una transacción en línea. Una identidad digital siempre es única en el contexto de un servicio digital, pero no necesariamente identifica de manera única al subjeto en todos los contextos. En otras palabras, acceder a un servicio digital no significa que se conozca la identidad de la vida real del subjeto».
>
> NIST, «Identidad digital» (2017)

El concepto de identidad digital de las personas hace referencia a la representación unívoca de las personas a través de mecanismos electrónicos o telemáticos. La verificación de la relación entre la persona y la identidad digital en un determinado contexto se realiza mediante el **proceso de verificación o prueba de identidad**.

La **identidad de una persona** es el conjunto de condiciones necesarias y suficientes que permiten acreditar que es la misma persona en momentos diferentes a lo largo del tiempo.

La identidad no se restringe únicamente a las personas, también se aplica a animales u objetos.

1.1. Características que ha de cumplir la identidad

En el año 2005, Kim Cameron, arquitecto responsable de la identidad en Microsoft, publicó un artículo titulado «Las leyes de la identidad», un conjunto de hipótesis científicas para proporcionar una capa de identidad a través de internet y **proteger la confianza y fomentar la percepción de seguridad** entre los usuarios.

Estas siete leyes son un compendio de características que todo sistema de identidad digital ha de cumplir para ser un mecanismo fiable como sistema de identidad global y unificado para ser utilizado en internet:

1) Ley #1. Control y consentimiento del usuario: los sistemas de identidad solo han de revelar la información que identifique al usuario y siempre ha de contar con su consentimiento.

2) Ley #2. Divulgación mínima para un uso restringido: el sistema de identidad ha de revelar la mínima información necesaria para identificar a la persona y debe restringir al máximo su uso y propósito.

3) Ley #3. Justificación de las partes: los sistemas de identidad han de ser diseñados de tal manera que la información revelada esté delimitada a las partes que interactúan, es decir, que el usuario ha de saber con quién comparte la información de identificación y su uso, y la otra parte ha de utilizarla para el uso y motivos expuestos al usuario.

4) Ley #4. Identidad dirigida: los sistemas de identidad han de proporcionar identificadores omnidireccionales para entidades públicas que les permitan revelar su identidad de manera genérica y universal, a la vez que proporcionan identificadores unidireccionales para entidades privadas que han de permitirles establecer una relación de identidad de duración corta con carácter privado y restringido, de manera que se comparta la mínima información posible.

5) Ley #5. Pluralismo de operadores y tecnologías: un sistema de identidad universal ha de garantizar el funcionamiento independientemente de cualquier tecnología que la soporte y ha de permitir gestionar las múltiples funciones y los atributos de identidad que gestionen otros posibles proveedores de identidad.

6) Ley #6. Integración humana: el metasistema de identidad debe incorporar al usuario (persona) como un componente fundamental dentro del sistema distribuido de identidades existentes, y así garantizar la interacción a través de los canales de comunicación con el sistema de identidad (máquina) de manera que se facilite la comprensión e interacción y garantizando la seguridad y fiabilidad, y que a su vez se proporcionen mecanismos de protección contra posibles ataques contra la identidad del usuario.

7) Ley #7. Experiencia coherente en todos los contextos: el metasistema de identidad ha de garantizar a los usuarios una experiencia simple y coherente, y también ha de permitir diferenciar las múltiples opciones de identidad según sean los contextos a través de los diferentes operadores y tecnologías.

1.2. Problemáticas actuales de la identidad digital

La red de internet fue creada sin proporcionar una capa nativa de gestión de la identidad; consecuentemente, no es posible garantizar la identidad de los usuarios. Esta limitación ha influido en el nivel de confianza, seguridad, privacidad y veracidad de la información respecto a la identidad digital de los usuarios, lo que ha dado origen a la creación de un conjunto incontrolable de identidades o perfiles digitales que no están bajo el control del usuario y a múltiples sistemas de gestión de identidades que deben utilizarse.

Figura 2. «En Internet, nadie sabe que eres un perro», primer meme respecto al anonimato en internet

Fuente: dibujo realizado por Peter Steiner, publicado por *The New Yorker* el 5 de julio de 1993.

El principal problema de la identidad digital es la falta de control y el desconocimiento del número de identidades digitales que posee un usuario, así como el desconocimiento absoluto del uso que se realiza de sus datos, lo que ha dado origen a un problema aún mayor: la **vulneración del derecho a la privacidad del usuario**.

Cuando se utiliza un sistema de identidad digital se reproducen las siguientes problemáticas:

1) Inexistencia de un único estándar, interoperabilidad y portabilidad. Existen múltiples estándares que son utilizados por las organizaciones para ofrecer una identidad digital, lo que dificulta la interoperabilidad y portabilidad de la identidad digital e incrementa la problemática de la gestión de las identidades digitales.

2) Múltiples identidades. La falta de estandardización de la identidad digital obliga a las organizaciones a generar nuevas identidades con el único propósito de gestionar el acceso a los servicios que se les ofrecen a los usuarios. De este modo se contribuye a generar nuevas identidades de manera infinita.

3) Calidad en la representatividad de la identidad. La identidad digital de una persona es la agrupación de atributos que permite diferenciarse unívocamente de otras identidades; por tanto, es condición necesaria que los atributos

que la definen sean una referencia veraz y fiel de la persona. A menudo, estos conjuntos de atributos son inexactos y obsoletos, debido a que la identidad digital evoluciona y cambia con el paso del tiempo.

4) Inconsistencias de atributos. Las diferentes identidades digitales que posee una persona se caracterizan por una falta de consistencia y calidad de los atributos. En los mismos contextos de utilización de la identidad de una misma persona, no siempre los atributos son los mismos o tienen informados los mismos valores.

5) Falta de control de la identidad del usuario. El usuario no tiene el control de sus identidades digitales, desconoce cuáles son los valores de los atributos que la definen.

6) Origen de nuevos riesgos: ciberataques y fraude a la identidad. El aumento de la navegación y el consumo de servicios en internet generan trazas de información y comportamientos que se asocian a los usuarios. La explotación y comercialización de esta información ha generado una nueva industria que obtiene grandes dividendos comercializando estos datos.

El aumento de ciberataques a empresas para robar información y datos de los usuarios ha puesto de manifiesto las limitaciones de las políticas de seguridad de las empresas.

De igual manera, el usuario también es objetivo de ciberataques y víctima de potenciales fraudes, el más común es la **suplantación de la identidad**, conocido como ***phishing***, provocado por la sustracción de los datos que permite acceder a servicios y recursos digitales.

7) Pérdida de la privacidad. La privacidad en un entorno digital hace referencia al derecho que tienen los usuarios a proteger sus datos personales y disponer de la capacidad de decidir cuáles son los datos personales visibles o que han de estar visibles para el resto de los usuarios o empresas.

Se debe garantizar que el acceso a los datos de usuarios por terceras partes solo se realice mediante el consentimiento explícito del usuario.

8) Incremento de la desconfianza. Ante estas problemáticas, el usuario se enfrenta a una situación de indefensión e inseguridad, que se ve incrementada a medida que dan a conocer nuevos episodios de ciberataques a empresas, robos de datos y suplantación de identidades a usuarios, y que, sumado al desconocimiento del usuario sobre cómo debe autoprotegerse, incrementa su nivel de desconfianza al utilizar nuevos servicios a través de internet.

2. Arquitecturas y sistemas de gestión de la identidad digital en la nube

Cuando hablamos de «**la nube**» nos referimos a los servidores a los que se accede a través de internet, así como a las aplicaciones y datos existentes en estos servidores.

NIST define la computación en la nube como:

> «La computación en la nube es un modelo para permitir un acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo o interacción del proveedor de servicio».

La definición de **ISO/IEC** de la nube es:

> «Paradigma para permitir el acceso de red a un conjunto de recursos compartidos, escalables y elásticos, físicos o virtuales con aprovisionamiento de autoservicio y administración bajo demanda».

La nube es un entorno que se caracteriza por:

- Su constante evolución tecnológica.
- Su infraestructura distribuida.
- Su complejidad en su gestión tecnológica.
- Su obligación de cumplir con los marcos legales y regulaciones existentes.
- Sus múltiples proveedores, que proporcionan modelos de servicios y soluciones propias.
- Su exposición a ciberataques.

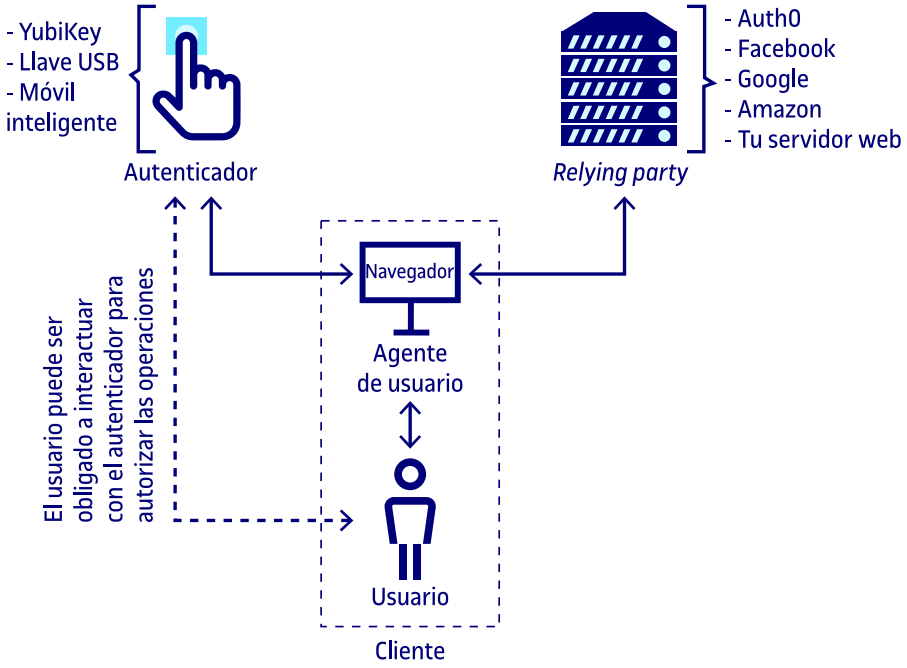
La identidad digital se utiliza como mecanismo para garantizar que únicamente aquellos usuarios que tienen **autorización** pueden acceder a los recursos y servicios que tienen asignados, así como la seguridad del uso de las aplicaciones y el perímetro de acceso a la red, proteger el acceso, la consulta y el procesamiento de datos, y proporcionar seguridad en la gestión, administración y uso de la nube.

Inicialmente eran las propias organizaciones las encargadas de proporcionar el **servicio de identificación y verificación** de la identidad digital a sus usuarios, solo de esta manera era posible acceder y utilizarlos. Únicamente cuando el usuario creaba sus credenciales de identidad digital en el servicio específico este tenía acceso.

Hoy en día, a pesar de disponer de mecanismos de autenticación más robustos, como pueden ser los certificados digitales o *tokens* de hardware, entre otros, el mecanismo más utilizado para autenticarse en un servicio en internet es el de **nombre de usuario y contraseña**.

En la siguiente imagen se describe el **flujo de autenticación** para acceder a un servicio web.

Figura 3. Flujo de autenticación de sitio web



El criptógrafo Christopher Allen publicó en el año 2016 un artículo en su blog titulado «Camino a la identidad digital autosoberana», donde presenta cuál ha sido la evolución de la identidad digital, desde las identidades centralizadas hasta las identidades federadas, pasando por las identidades centradas en el usuario y finalmente introduciendo el concepto de las identidades autosoberanas.

2.1. Modelos de identidades digitales

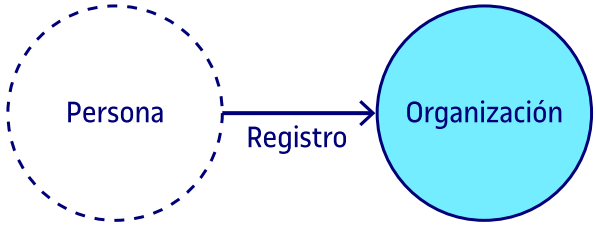
Con la aparición de internet, los modelos de identidad digital han evolucionado con los años. Esta evolución se agrupa en **cuatro grandes etapas**: la primera de estas es conocida como **identidad centralizada**; posteriormente surge la **identidad federada**, que evoluciona a un concepto de **identidad centrada en el usuario**, y, finalmente, se encuentra la que es conocida como **identidad autosoberana**.

1) Modelo de identidad centralizada

Internet proporcionó una nueva manera de compartir información. Es en este preciso momento cuando surge la necesidad de gestionar el acceso a esta información, y la solución se implementa mediante el mecanismo que permite identificar a los usuarios y seleccionar los contenidos y la información autorizados.

Para implementar esta funcionalidad, se crea el sistema de **cuentas centralizadas** gestionadas por el mismo proveedor de servicio. Es el propio proveedor de servicios el responsable de proporcionar un **servicio de registro**; para ello, proporcionará una cuenta de usuario personalizada y protegida por el binomio nombre de usuario y contraseña.

Figura 4



La gestión centralizada de la identidad tiene numerosos inconvenientes o limitaciones:

- Vulnerabilidades de seguridad. Por ejemplo, la mayoría de los usuarios reutiliza las contraseñas.

- Problemas de usabilidad, al ser necesario crear y manejar un gran número de cuentas, cada una con su propio nombre de usuario y contraseña.

- Limitaciones de la capacidad de la identidad digital, como consecuencia de la creación de múltiples cuentas en diferentes sitios web.

Los usuarios almacenan una pequeña parte de su identidad digital en las bases de datos de estos sitios web y proveedores de servicios. De esta manera, la identidad digital del usuario **queda fragmentada y aislada en numerosas bases de datos** diferentes (silos de datos) que son controladas por tantos terceros como cuentas de usuario ha creado el usuario.

2) Modelo de identidad federada

Uno de los principales problemas de la identidad centralizada es la necesidad y obligación que tienen los usuarios de crear tantas cuentas de usuario como accesos a servicios en línea quieren consumir.

La evolución natural lleva a dar respuesta a esta problemática proporcionando un **único proceso de autenticación** para acceder a los diferentes servicios y que es ofrecido bajo un mismo ecosistema en línea.

Figura 5

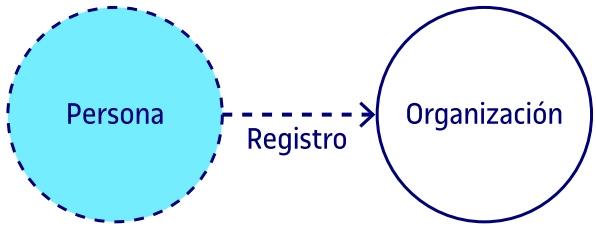
El modelo de identidad federada no solo permite que los usuarios utilicen sus credenciales en los diferentes servicios disponibles en un mismo ecosistema en línea, sino que permite utilizar servicios de otros ecosistemas en línea sin la necesidad de volver a autenticarse.

La gestión de la identidad es **responsabilidad de las diferentes organizaciones** que comparten los datos de registro, credenciales, identificadores y autorizaciones de los usuarios.

3) Modelo de identidad centrada en el usuario

En el año 2005, la comunidad IIW (*The Internet Identity Workshop*) comenzó a trabajar en este nuevo modelo, donde el **usuario es el centro** en todo el proceso de identidad.

Figura 6



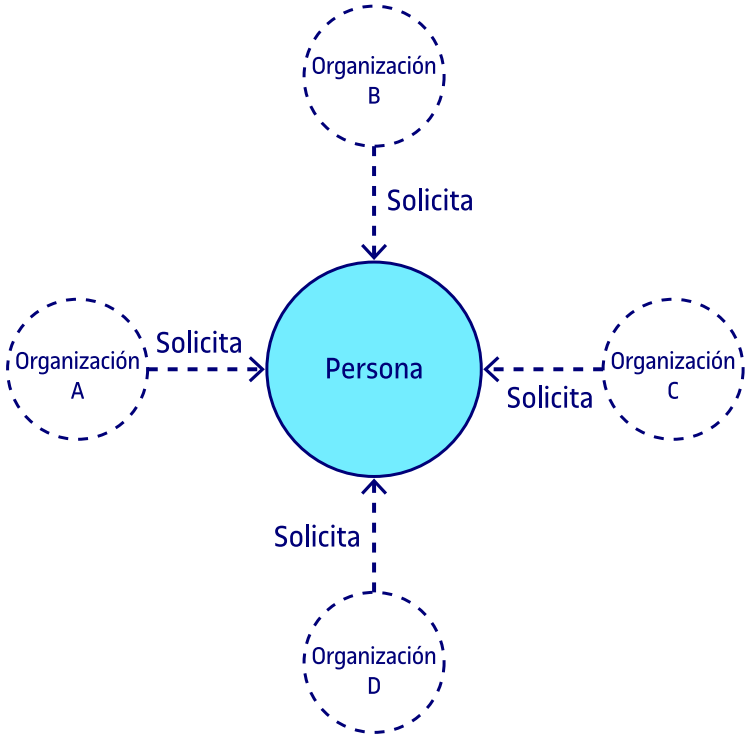
Su objetivo es proporcionar al usuario una mejora de la usabilidad para gestionar su identidad independientemente de la tecnología o plataforma de servicios, y de esta manera facilitar **interoperabilidad** y **portabilidad** a la identidad digital.

4) Modelo de identidad autosoberana (SSI)

En un modelo de identidad autosoberana (SSI, *self-sovereign identity*) son las personas las que controlan y gestionan su identidad digital. Con este modelo se produce un **cambio de paradigma** respecto a la manera de cómo se debe gestionar y administrar la identidad digital y pasa por retornar el control de la identidad digital a su propietario, es decir, al individuo.

El modelo de identidad soberana parte del modelo de identidad centrada en el usuario, al cual le concede todo el control y le proporciona plena autonomía, trasladando la gobernanza de la identidad a manos del usuario.

Figura 7



2.2. Gestión de la identidad digital y control de acceso

Existen dos conceptos que a menudo son confundidos: estos son la **autenticación** y la **autorización**. La autenticación es la práctica de seguridad que permite confirmar que alguien es quien dice ser, mientras que la autorización es el proceso de determinar el nivel de acceso que tiene asignado un usuario.

Para realizar una correcta gestión de la identidad digital y el acceso a los recursos es fundamental la existencia de una **relación de confianza y delegación de responsabilidades entre las organizaciones** que proporcionan servicios y sus usuarios.

A los sistemas de gestión de identidades y acceso se les conoce como IAM (*Identity and Access Manager*) y son los responsables de verificar las identidades de los usuarios y encargados de controlar sus privilegios para determinar lo que puede hacer.

Gartner define **IAM** como: «La disciplina de seguridad que permite a las personas adecuadas acceder a los recursos adecuados en el momento adecuado por las razones adecuadas».

En los últimos años, proteger la identidad ha sido una prioridad al convertirse en el principal foco de todo ciberataque, con importantes afectaciones y consecuencias en la gestión de identidades y accesos a servicios.

Los servicios IAM garantizan que únicamente los **usuarios autorizados** puedan acceder a determinados recursos. Conceptualmente, el IAM es muy sencillo: un usuario acredita su identidad y se le permite el acceso a un recurso al que tiene derecho.

Sin embargo, en la práctica, hay varios factores que añaden complejidad a este proceso:

- La existencia de un elevado número de usuarios.
- La existencia de múltiples formatos para representar la identidad digital.
- Los usuarios pueden tener numerosas identidades digitales.
- El aumento del número de dispositivos y aplicaciones donde los usuarios deben autenticarse.
- La complejidad en la gestión de las distintas identidades digitales sobre cuáles son los derechos y las autorizaciones sobre los recursos disponibles.

Por medio de la gestión de identidades y acceso (IAM) se proporciona un mecanismo que permite **conocer quién es el usuario** (identidad digital) y **qué permisos tiene** para acceder al sistema (acceso a recursos). También es conocido como gestión de identidad (IdM).

La identidad de un individuo se verifica mediante una **prueba de identidad** a través de los atributos proporcionados a un tercero, de manera que podrá verificar la identidad del individuo. Es importante tener presente que la verificación de una identidad no implica tener acceso a todos los recursos y servicios disponibles del sistema donde se ha autenticado.

En el contexto de IAM, aparece la figura de los **proveedores de identidad**, conocidos con las siglas **IdP**, que son los responsables de gestionar el proceso de inicio de una sesión y se responsabilizan de almacenar y gestionar las identidades digitales de los usuarios.

Según el estándar de identificación digital NIST, el proceso de identificación digital incluye dos componentes y un tercero opcional:

1) Primer componente: verificación e inscripción de identidades. La prueba de identidad responde a la pregunta: «¿Quién eres?». Hace referencia al procedimiento por el cual un proveedor de servicios de identidad (IDSP) recopila, valida y verifica la información de una persona.

2) Segundo componente: autenticación y gestión del ciclo de vida de la identidad. La prueba de identidad responde a la pregunta: «¿Sois la persona identificada/verificada?».

Mediante este segundo componente se establece que la persona que desea acceder a un servicio es la misma persona previamente acreditada por un proveedor de identidades (IdP), y a su vez posee y tiene bajo su control las credenciales de identificación.

Para ayudar a la autenticación de la persona se utilizan **tres factores de autenticación**, que permiten confirmar su identidad utilizando:

- **Una cosa que el usuario conoce:** contraseña, pin, código, pregunta-respuesta u otro secreto.

- **Una cosa que solo el usuario posee:** un certificado, una tarjeta, *token* de seguridad, móvil, monedero digital, etc.

- **Una cosa que el usuario es:** huella digital, comportamiento, datos biométricos etc.

3) Tercer componente: mecanismos de portabilidad e interoperabilidad (opcional). Es necesario definir y adoptar estándares para representar la identidad digital; sin estos, la interoperabilidad y la portabilidad de la identidad digital es difícil de conseguir, y complica la gestión de las identidades digitales de los usuarios.

La manera sobre cómo acceder a los recursos en la nube a través de la identidad digital obliga a plantearse **cómo administrar las identidades**, una decisión que debe ser compartida entre proveedores y usuarios de la nube. En este contexto, la gestión de la identidad y el control de acceso se complican debido a que son diversas las organizaciones que tienen esta responsabilidad.

Las organizaciones para gestionar las identidades digitales deben considerar los siguientes puntos:

- **Evaluar la seguridad actual y la madurez de la identidad digital.** Identificar las debilidades de seguridad, definir una arquitectura y una hoja de ruta según la estrategia corporativa.

- **Entender quién tiene acceso a qué.** Conocer y comprender los procesos de control de acceso a los recursos de la organización.

- **Utilizar estándares de identidad abiertos.**

- **Incorporar autenticación multifactor** (MFA).

- **Proteger los canales de acceso a los recursos de la nube.**

- **Gestionar el ciclo de vida de las políticas e identidad digital.**

- **Establecer procesos de acceso de confianza cero**, donde la confianza se verifica y establece continuamente para cada dispositivo, usuario, computación, dispositivo de red y solicitud.

Un sistema de gestión de identidades consta de los siguientes **componentes** básicos:

- Repositorio de identidad.
- Herramientas para la gestión del ciclo de vida de acceso.
- Sistema de regulación y cumplimiento de accesos.
- Sistema de auditoría e informes.
- Mecanismos de autenticación multifactor (MFA).

2.3. Arquitecturas para gestionar la identidad en la nube

Las **implementaciones** (*Identity and Access Manager*) en la nube suelen implementar algunas de las siguientes arquitecturas:

a) Cuentas en la nube: consiste en replicar o sincronizar las cuentas de los usuarios en el entorno de la nube.

b) Federación de identidades: la gestión de identidades de manera federada es una configuración que se realiza entre dos o más dominios de confianza para permitir que los usuarios de estos dominios accedan a aplicaciones y servicios utilizando la misma identidad digital.

Existen dos posibles arquitecturas, la primera y menos utilizada consiste en que los sistemas de gestión de las identidades de las organizaciones se conectan directamente con los proveedores de servicio en la nube.

La segunda y más implementada es la conocida como ***Hub and spoke***, que consiste en que los sistemas de gestión de las identidades de las organizaciones se conectan a un proveedor único de identidades centralizado para toda la federación, que actúa como un proveedor de identidades para los proveedores de servicio en la nube.

c) IDMaaS: identidad como servicio. La identidad como servicio (IDaaS ofrece capacidades y servicios para la gestión y administración de identidades y accesos (IAM) que son implementados en la nube como SaaS (software como servicio administrado) por un proveedor externo de confianza.

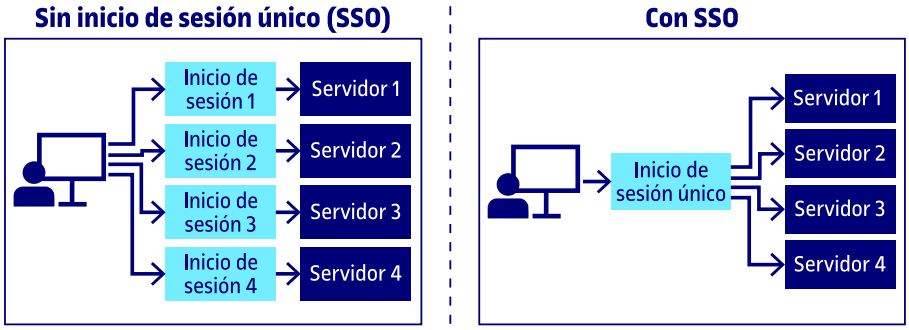
3. Inicio de sesión único (SSO) y despliegue en un proveedor de identidad (IdP)

El **inicio de sesión único** (*single sign-on*, SSO) es un procedimiento de autenticación que habilita a un usuario para acceder a varios sistemas con un solo proceso de identificación.

El inicio de sesión único (SSO) centraliza en un único punto el inicio de sesión para el acceso a diversas aplicaciones, de esta manera el usuario solo debe proporcionar sus credenciales de inicio de sesión una sola vez y en un solo punto de verificación para acceder a los diferentes servicios y aplicaciones en la nube. El uso de SSO permite mejorar la experiencia del usuario y proporciona mayor seguridad.

Mediante el inicio de sesión único, los usuarios solo necesitan de una identidad para acceder a los diferentes sistemas de una misma organización.

Figura 8. Inicio de sesión único



Fuente: blog auth0

Las **ventajas** que nos ofrece un SSO son las siguientes:

- **Contraseñas más seguras:** los usuarios solo tienen que usar una única contraseña, de esta manera se facilita que la contraseña sea más segura.
- **Eliminación de la «fatiga de contraseñas»:** se produce cuando los usuarios reutilizan la misma contraseña en varios servicios.
- **Mejora la aplicación de la política de contraseñas:** solo es necesario proporcionar un único lugar donde introducir la contraseña.
- **Autenticación multifactorial (MFA) en un único punto.**

- **Creación de un único punto para cumplir el reingreso de la contraseña.**

- **Gestión de credenciales internas en un entorno controlado.**

- **Reducción del tiempo de los procesos de recuperación o restablecimiento de contraseñas.**

En un proceso de autenticación de SSO, las partes que participan son tres: primero el **sujeto**, que es el usuario que desea acceder a un servicio o aplicación; el segundo, el **proveedor de identidades (IdP)**, que es el servicio responsable de confirmar la identidad del usuario, y, finalmente, el **proveedor de servicio**, plataforma o conjunto de servicios o aplicaciones que se le ofrece al usuario.

Un servicio SSO no tiene por qué recordar o saber quién es el usuario, ya que no almacena las identidades de los usuarios. Mayoritariamente, los servicios SSO funcionan comprobando las credenciales del usuario con un servicio de proveedor de identidades (IdP) para verificar su identidad.

Los IdP son una parte esencial del proceso de inicio de sesión SSO. Los proveedores de SSO verifican la identidad del usuario con el IdP cuando los usuarios inician la sesión. Una vez realizado este proceso, el SSO puede verificar la identidad del usuario con cualquier aplicación en la nube a la que esté conectado.

3.1. Funcionamiento de un inicio de sesión único (SSO)

El SSO proporciona un servicio a los usuarios para que estos proporcionen sus credenciales de identidad y que, de esta manera, el usuario no tenga que iniciar la sesión directamente en la aplicación o servicio en internet.

Una vez que el usuario ha introducido sus credenciales de identidad, el servicio SSO procede a verificar las credenciales proporcionadas contra el **servidor de autenticación** de la empresa que ofrece el servicio o al proveedor de identidades.

Una vez verificadas las credenciales proporcionas por el usuario, el servicio SSO crea un ***token* de autenticación**, que es gestionado por el navegador del usuario o por los servidores del servicio SSO, que le permite acreditar que el usuario ha sido verificado correctamente.

A partir de este momento, todo servicio o aplicación a la que desee acceder el usuario verificará con el servicio SSO si el usuario ha sido verificado.

En caso afirmativo, el servicio SSO proporcionará el *token* de autenticación del usuario a la aplicación; así, el usuario podrá acceder al servicio o aplicación deseada. De esta manera, los usuarios no necesitan confirmar su identidad en cada uno de los servicios a los que desea acceder.

En caso negativo, si no ha iniciado una sesión, el servicio solicitará que lo realice a través del servicio SSO.

SSO permite a los usuarios que se autentiquen en múltiples aplicaciones y servicios a la vez. De esta manera el usuario solo debe iniciar una sesión en una sola pantalla de inicio de sesión para después utilizar varias aplicaciones.

Los *tokens* de autenticación tienen sus propios estándares, el principal estándar de *token* de autenticación es SAML (*Security Assertion Markup Language*).

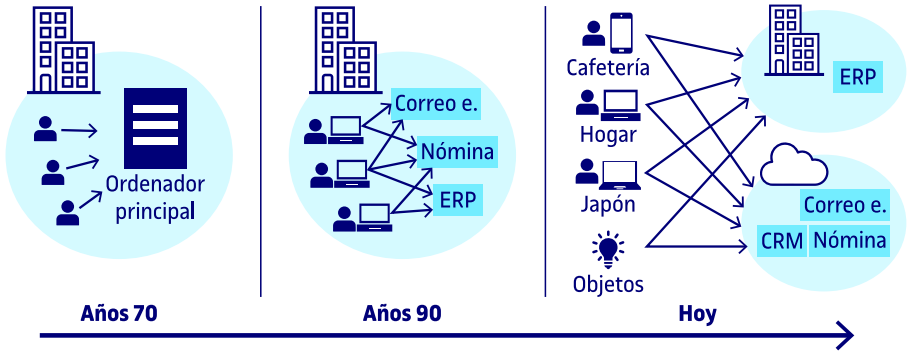
El SSO es un tipo de **gestión de identidades federadas**. El SSO se produce cuando un usuario inicia sesión en un cliente y a continuación inicia sesión en otros clientes de forma automática, independientemente de las diferentes plataformas, tecnologías o dominios.

El SSO está basado en **estándares abiertos** como *Security Assertion Markup Language* (SAML) y *OpenID Connect* (OIDC), para federar la identidad y dar acceso a servicios y aplicaciones de proveedores de servicios.

4. Federaciones de identidad

La red de internet fue creada sin proporcionar una capa nativa para la gestión de la identidad, por lo que no era posible garantizar la identidad de los usuarios.

Figura 9. Evolución de la identidad digital



Fuente: Identity as a Service (IDaaS) For Dummies, Auth0 Special Edition

Esta limitación ha provocado la creación de un **conjunto incontrolable de identidades** o perfiles digitales a los usuarios, que no están bajo su control, a la vez que ha generado numerosos sistemas de gestión de identidades.

La manera de acceder a los recursos en la nube a través de la identidad digital obliga a plantearse cómo administrar las identidades, una decisión que debe ser compartida entre proveedores y usuarios de la nube. En este contexto, la gestión de la identidad y del control de acceso se complica debido a que son diversas las organizaciones que tienen esta responsabilidad.

La federación de identidades es la principal herramienta para gestionar este problema, creando relaciones de confianza. La idea central es permitir que los individuos utilicen las mismas credenciales para acceder a servicios en diferentes dominios.

La **gestión de identidad federada** es un modelo que se puede realizar entre dos o más dominios de confianza para permitir que los usuarios de esos dominios accedan a aplicaciones y servicios utilizando la misma identidad digital.

Según la publicación de NIST (800-63C), la **federación de identidades** es un proceso que permite la transmisión de información de identidad y autenticación mediante un conjunto de sistemas en la red.

La federación de identidades permite que diferentes dominios definan y acuerden un **protocolo** para que las afirmaciones de una identidad digital puedan utilizarse entre estas, a la vez que posibilita la implementación de un servicio SSO.

Para hacerlo posible, los recursos ubicados en los diferentes dominios deben estar integrados de manera transparente para el usuario, para lo que será necesario implementar un sistema de confianza entre las partes, para que estas puedan relacionarse.

4.1. Funcionamiento básico de la federación de identidad

Las políticas de gestión de las identidades no permiten acceder a las *cookies* o cualquier otra información almacenada en el ordenador del usuario, a no ser que sea el propio creador de la información quien acceda. Por tanto, cuando un usuario navega entre aplicaciones que requieren autenticación, y estas no están dentro del mismo dominio de confianza, no pueden consultar los datos de autenticación del usuario.

Ante esta situación es necesario definir un mecanismo que permita **transferir información** (credenciales de identidad) entre dominios de manera segura. Para garantizar esta funcionalidad, surge la figura del proveedor de identidades.

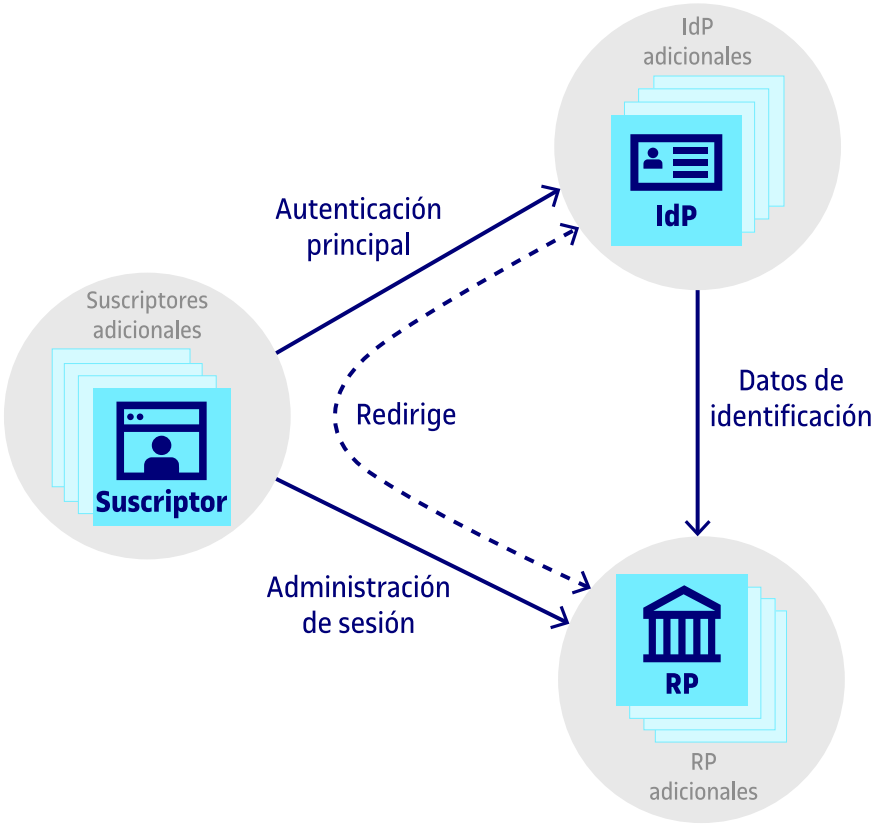
En un modelo de identidad federada identificamos **tres componentes**:

- **Usuario** que reclama acceso al recurso, conocido como **suscriptor**.
- Verificador o proveedor de servicios de credenciales, conocido como **proveedor de identidad** (IdP).
- **Proveedor de recursos** o parte que confía (RP).

La tecnología de federación de identidades se usa generalmente cuando el RP y el IdP no son la misma entidad o no están bajo una administración común.

El siguiente esquema nos permite describir de manera genérica el proceso que se requiere para acceder a los servicios o aplicaciones que ofrece un **proveedor de servicios** (RP) a través del modelo de federación de identidades.

Figura 10



Fuente: NIST, Special Publication 800-63C

1) Primer paso: el suscriptor debe autenticarse ante el IdP. El **suscriptor** no se autentica directamente en el **RP**. El protocolo de federación define un mecanismo para que un **IdP** proceda ante una solicitud de identificación de un suscriptor por parte de un RP.

2) Segundo paso: el IdP verifica las credenciales del suscriptor y se procede a generar una afirmación. El **IdP** es responsable de autenticar al **suscriptor**.

Las afirmaciones son declaraciones de un **IdP a un RP** que contienen información sobre un **suscriptor**.

Una afirmación normalmente incluye un identificador para el suscriptor, lo que permite la asociación del suscriptor con sus interacciones previas con el RP.

Las afirmaciones pueden incluir, además, valores de atributo o referencias de atributo que caracterizan más al suscriptor y respaldan la decisión de autorización en el RP.

3) Tercer paso: una vez verificadas satisfactoriamente las credenciales por el **IdP**, confirma al **RP** la identidad del suscriptor para que le proporcione acceso al recurso.

El RP usa la información en la aserción para identificar al suscriptor y tomar decisiones de autorización sobre su acceso a los recursos controlados por el RP.

Este proceso permite al suscriptor obtener servicios de múltiples RP sin la necesidad de tener o mantener credenciales separadas en cada uno. También puede ser utilizado para admitir el inicio de sesión único (SSO).

Lecturas recomendadas

Para conocer con detalle los mecanismos de autenticación entre el suscriptor y el IdP, se puede consultar la publicación del NISTSP 800-63B.

Para conocer con detalle los procedimientos para transmitir atributos entre el suscriptor y el IdP, se puede consultar la publicación del NIST SP 800-63A.

La gestión de identidades federadas es un método para transferir datos de autenticación sin vulnerar la política del mismo origen, generalmente utilizando un servidor de autorización externo.

4.2. Modelos de la federación de identidad

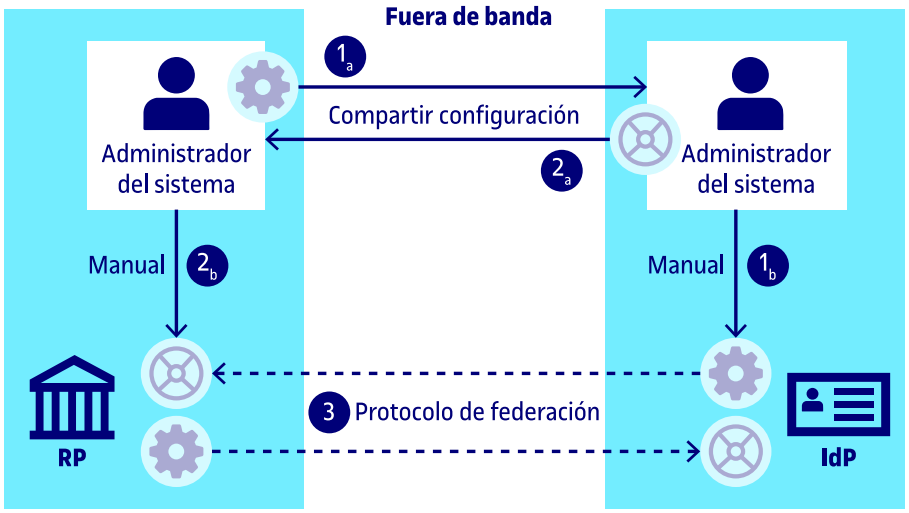
A continuación, mostramos el detalle genérico y cuáles son los requisitos de los modelos de federación existentes.

1) Registro manual

El proveedor de identidades (IdP) y el proveedor de servicios (RP) proporcionan manualmente información de configuración sobre las partes con las que esperan interoperar. Este proceso es implementado mediante tres pasos:

- **Primer paso:** el administrador del sistema del RP comparte los atributos del RP con el administrador del sistema del IdP, para asociarlos con el RP.
- **Segundo paso:** el administrador del sistema del IdP comparte los atributos del IdP con el administrador del sistema del RP, para asociarlos con el IdP.
- **Tercer paso:** finalmente, el IdP y el RP se comunican mediante el protocolo de federación.

Figura 11



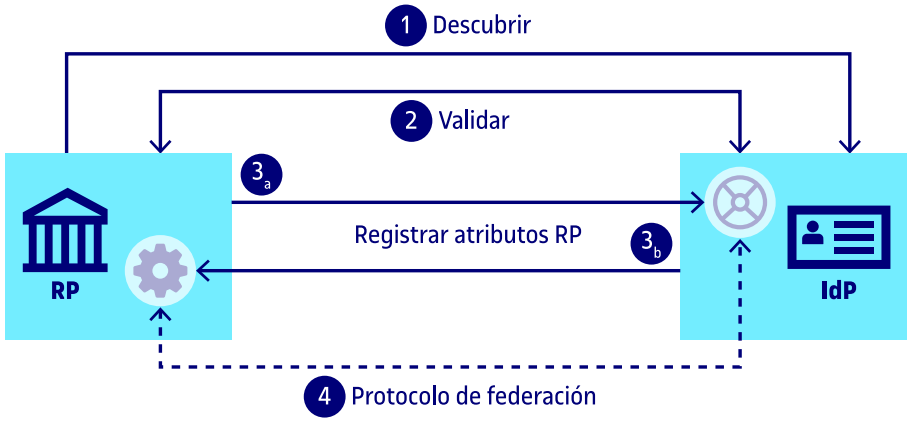
Fuente: NIST, Special Publication 800-63C

2) Registro dinámico

Las relaciones entre los miembros de la federación se pueden establecer en la misma transacción de comunicación. La información de configuración está disponible para establecer la comunicación entre el IdP y el RP. Este proceso es implementado mediante cuatro pasos:

- **Primer paso:** el RP va a una ubicación conocida del IdP para encontrar los metadatos del IdP.
- **Segundo paso:** el RP y el IdP se verifican respectivamente.
- **Tercer paso:** se registran los atributos del RP. El RP envía sus atributos al IdP y el IdP asocia esos atributos con el RP.
- **Cuarto paso:** el IdP y el RP se comunican mediante el protocolo de federación.

Figura 12

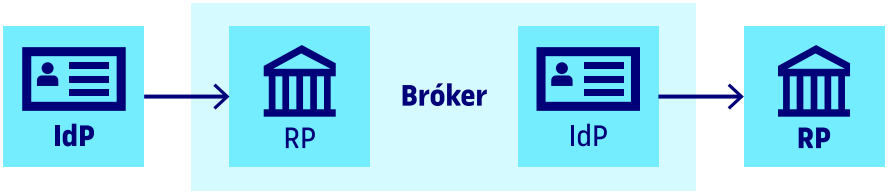


Fuente: NIST, Special Publication 800-63C

3) Federación representada

En este modelo, la comunicación entre el IdP y el RP se realiza mediante la figura de un intermediario que actúa como un bróker de identidades.

Figura 13



Fuente: NIST, Special Publication 800-63C

Un **corredor de identidad** (*identity broker*) es un servicio que intermedia para que conecten diversos proveedores de servicios (RP) con diferentes proveedores de identidad (IdP).

Como servicio intermediario, el corredor de identidad es responsable de crear una relación de confianza con un proveedor de identidad externo para utilizar sus identidades y acceder a los servicios internos expuestos por los proveedores de servicios.

4) Autoridades de federación

Las autoridades de la federación se responsabilizan de la gobernanza de la federación ayudando en la toma de decisiones y verificando los requerimientos de seguridad e integridad establecidos.

Sus **funciones** son:

- Examinar a todos los miembros de la federación para determinar si cumplen con los estándares de seguridad, identidad y privacidad establecidos.

- Verificar que los IdP cumplen con los requerimientos de la federación; solo así son autorizados a participar y operar en la federación. Esta información es utilizada por los RP para identificar cuáles son los IdP con los que pueden relacionarse.

- Ayudar en el proceso de configuración y conexión técnica entre los miembros (publicando datos de configuración para los IdP o emitiendo declaraciones de software para los RP).

El proceso para verificar a los miembros que pueden participar de la federación, sean IdP o RP, ha de satisfacer las siguientes condiciones:

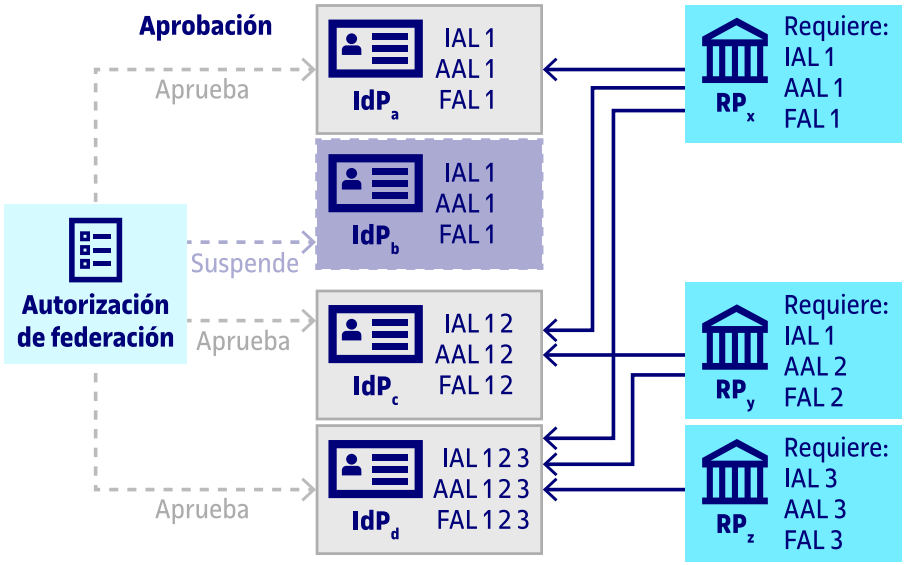
- Las afirmaciones generadas por los IdP deben cumplir con los estándares definidos.

- La información que se comparte entre un IdP y un RP en un proceso de autenticación es conocida como afirmación, y hace referencia al conjunto de valores o referencias de atributo que se realiza sobre un suscriptor autenticado.

- Los RP han de adherirse a los requerimientos del IdP sobre el manejo de datos de los atributos del suscriptor.

- Los sistemas RP e IdP utilizan perfiles aprobados de protocolos de federación.

Figura 14



Fuente: NIST, Special Publication 800-63C

5. Integración avanzada de un proveedor de identidad (IdP) y los protocolos OAuth, OpenID y SAMLv2

A continuación, enumeramos los **principales estándares** que permiten implementar una identidad digital para una federación de identidades:

a) OAuth: es un estándar de IETF para la autorización que se usa ampliamente para servicios web. Es utilizado para delegar el control de acceso/autorizaciones entre servicios.

OAuth está diseñado para funcionar a través de HTTP y actualmente está en la versión 2.0, que no es compatible con la versión 1.0.

OAuth 2 es un estándar de autorización que proporciona acceso seguro a los recursos del usuario final. Especifica un proceso que permite el acceso a los recursos de otros proveedores de servicio sin tener que compartir sus credenciales de identidad.

b) OpenID: es un estándar para la autenticación federada que es ampliamente compatible con los servicios web.

Basado en HTTP, con URL usadas para identificar el proveedor de identidad y el usuario/identidad.

La versión actual es OpenID Connect 1.0, una capa de identidad simple sobre el protocolo OAuth 2.0. Permite verificar la identidad del usuario final basándose en la autenticación realizada por un Servidor de Autorización, así como obtener información de perfil básica sobre el usuario final de una manera interoperable y similar a API-REST.

3) *Security Assertion Markup Language* (SAML) 2.0: es un estándar OASIS para la administración de identidades federadas que admite autenticación y autorización.

Utiliza XML para realizar afirmaciones entre un proveedor de identidad y un proveedor de servicios.

Las afirmaciones pueden contener declaraciones de autenticación, declaraciones de atributos y declaraciones de decisión de autorización.

5.1. Protocolo OAuth

Proporciona una *framework* de autorización que delega la autenticación del usuario al proveedor de identidad (IdP) y que autoriza a aplicaciones de terceros a acceder a la cuenta del usuario sin tener que proporcionar credenciales.

OAuth se diferencia de OpenID y SAML en que se utiliza exclusivamente para fines de autorización y no para fines de autenticación.

Auth0 permite estar conectado en todos los dominios, acceder a las cuentas del usuario en su sistema, establecer restricciones de acceso específicas entre los proveedores de identidad y mantener todos estos datos consistentes.

En los flujos OAuth 2.0 participan cuatro roles:

a) Usuario final: es el propietario del recurso. Posee los datos y tiene la capacidad de permitir que los clientes tengan acceso a esos datos o recursos.

b) Servidor de autorización o proveedor de identidad (IdP): es el responsable de garantizar la identidad del usuario, conceder y revocar el acceso a los recursos y emitir *tokens*.

El servidor de autorización es el responsable de gestionar las peticiones de autorización.

Verifica la identidad de los usuarios y emite una serie de *tokens* de acceso a la aplicación cliente.

c) Cliente OAuth: entidad que utiliza el recurso después de obtener la autorización del cliente.

El cliente de OAuth suele ser la parte con la que interactúa el usuario final y solicita tokens del servidor de autorización. El cliente debe contar con el permiso del propietario del recurso para acceder a este.

d) Servidor de recursos: entidad que aloja los recursos. Confía en el servidor de autorización para autenticar y autorizar al cliente de OAuth de forma segura.

En el siguiente esquema podemos observar cómo estos cuatro roles se relacionan entre sí:

- **Primer paso:** la aplicación solicita al usuario que se autentique.

- **Segundo paso:** el usuario es redirigido al servidor de autenticación para proceder a su identificación.

- **Tercer paso:** el usuario se autentica a través de su nombre de usuario y contraseña o cualquier otro mecanismo definido. *A posteriori* debe dar su consentimiento explícito a la aplicación conforme al uso que va a tener.

- **Cuarto paso:** validada la identidad del usuario, y si el usuario ha dado su consentimiento, es redirigido a la aplicación. A continuación, se proporciona una *cookie* autorizando a la aplicación para acceder al recurso protegido.

- **Quinto paso:** la aplicación realiza una solicitud al servidor de autorización, con el permiso que el usuario le ha dado, acompañado de algunos datos que permiten identificar a la aplicación para verificar que es un usuario válido para acceder a los recursos. Si no se produce ningún error, el servidor de autorización proporcionará un *token* de acceso.

- **Sexto paso:** la aplicación utiliza este *token* de autenticación que le permite acceder a los recursos sin necesidad de volver a solicitar credenciales de identificación al usuario.

- **Séptimo paso:** se procede a guardar las *cookies* del dominio sobre el que se está accediendo.

Figura 15

Fuente: Blog auth0

Si el usuario desea acceder a una nueva aplicación en otro dominio, este recibe un *token* de autorización, y procederá a validar con el servidor de autenticación el *token* proporcionado, si es correcto permitirá su acceso.

5.2. OpenID Connect

OpenID Connect es un protocolo de autenticación interoperable basado en la familia de especificaciones OAuth 2. 0. Proporciona una capa de identidad adicional construida sobre OAuth 2 que especifica un proceso para verificar la identidad de un usuario asegurándose de que sea quien dice ser.

Al igual que en el protocolo OAuth, en OpenID Connect también son necesarios los mismos cuatro roles: **usuario final**, **servidor de autorización o proveedor de identidad (IdP)** y **cliente OAuth** y **servidor de recursos**.

OpenID Connect utiliza *tokens* web JSON (JWT) junto al protocolo OAuth 2. 0.

1) *Tokens* de autenticación (JWT)

Los *tokens* web JSON son un método RFC 7519 estándar de la industria de código abierto para representar reclamaciones de forma segura entre dos partes.

Los clientes reciben la identidad de los usuarios codificada en un *token* web JSON (JWT) seguro, el cual recibe el nombre de *token* de identificación.

2) Protocolo OAuth 2. 0

Los testimonios de identificaciones se obtienen mediante el protocolo OAuth 2. 0; de esta manera también se consigue disponer de un protocolo que permite la autenticación y la autorización.

La principal diferencia entre OpenID y OAuth es que OpenID es un protocolo de autenticación, mientras que OAuth es un *framework* de autorización.

Los *tokens* de identificación contienen un conjunto de afirmaciones sobre el usuario, como el nombre y el correo electrónico. Mientras que los *tokens* de acceso autorizan el acceso a los servidores de recursos con un alcance limitado, pero no contienen ningún dato sobre la identidad del usuario.

El flujo de autorización OpenID Connect es el siguiente:

- **Primer paso:** el usuario intenta iniciar una sesión con su aplicación cliente y es redirigido al proveedor OpenID, que realiza los siguientes pasos:
  - Autentica y autoriza al usuario para una instancia de aplicación en particular.

  - Codifica los detalles del usuario en un id_token (JWT) que contiene información del usuario y la firma.

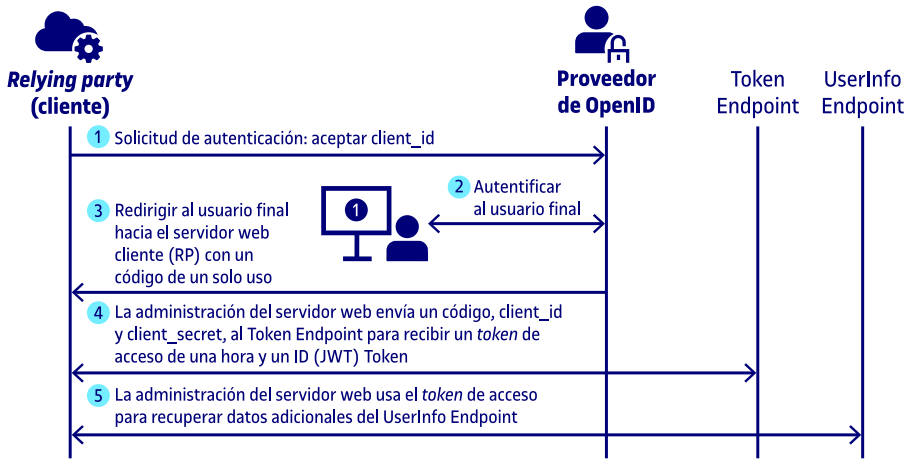
- **Segundo paso:** el proveedor de OpenID autentica y autoriza al usuario para una instancia de aplicación en particular.

- **Tercer paso:** devuelve un código de un solo uso al servidor web mediante un URI de redireccionamiento predefinido.

- **Cuarto paso:** el servidor web pasa el código, la identificación del cliente y el secreto del cliente al punto final del *token* del proveedor de OpenID, y el proveedor de OpenID valida el código y devuelve un *token* de acceso de una hora.

- **Quinto paso:** el servidor web utiliza el *token* de acceso para obtener más detalles sobre el usuario (si es necesario) y establece una sesión para este.

Figura 16. Flujo de autorización OpenID Connect



Fuente: onelogin

5.3. SAML (lenguaje de marcado de aserción de seguridad)

La versión actual de SAML es la 2.0, que fue ratificada como estándar OASIS (Organization for the Advancement of Structured Information Standards) en marzo de 2005.

SAML 2.0 es un protocolo basado en XML que utiliza *tokens* de seguridad que contienen aserciones para pasar información, tanto de autenticación como de autorización, sobre un usuario final entre un proveedor de identidad (IdP) y otro de servicios (RP). SAML 2.0 permite el inicio de sesión único entre dominios basado en la web (SSO).

OpenID Connect y SAML son protocolos de identidad para autenticar usuarios y proporcionar datos de identidad que permitan realizar el control de acceso a los recursos disponibles.

Una diferencia entre estos dos protocolos es el número de interacciones que son necesarias entre la aplicación y el proveedor de identidades.

SAML utiliza *tokens* SAML escritos en XML. La aplicación valida la propia firma y la autorización. OpenID Connect se basa en REST/JSON. Los proveedores de OpenID Connect emiten un *token* de acceso y un identificador. OpenID Connect permite que una aplicación obtenga la identidad sin realizar una consulta al proveedor de identidades.

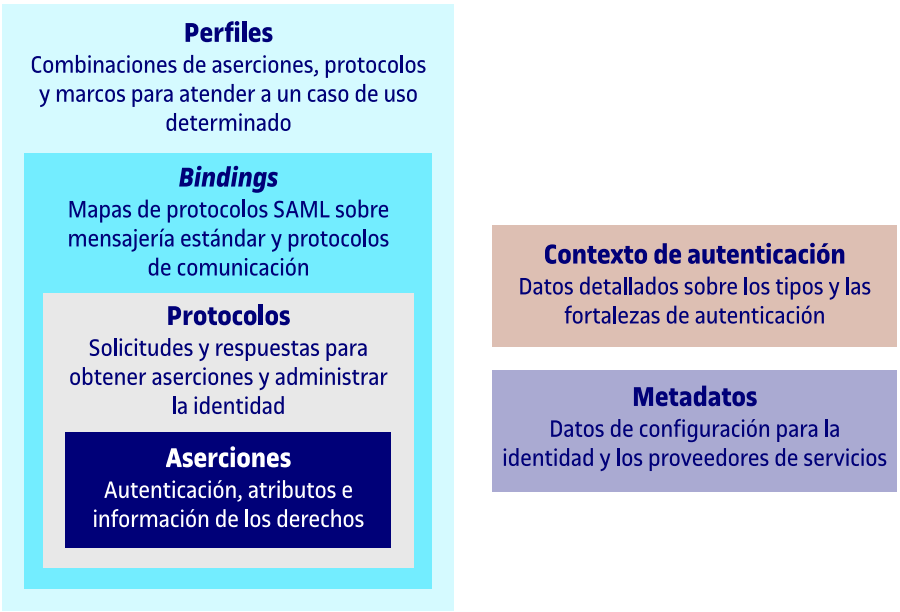
SAML consta de componentes básicos que permiten principalmente la transferencia de información de identidad, autenticación, atributos y autorización entre organizaciones autónomas que tienen una relación de confianza establecida.

La especificación principal de SAML define la estructura y el contenido tanto de las afirmaciones como de los mensajes de protocolo que se utilizan para transferir esta información.

Las afirmaciones de SAML llevan declaraciones sobre un usuario. La estructura y el contenido válidos de una aserción se definen mediante el esquema XML de aserción SAML. Los mensajes del protocolo SAML se utilizan para realizar las solicitudes definidas por SAML y devolver las respuestas adecuadas.

En el siguiente esquema se pueden ver los conceptos básicos SAML:

Figura 17. Conceptos básicos del SAML



Fuente: Security Assertion Markup Language (SAML) V2.0 Technical Overview

1) Protocolos: protocolos de solicitud/respuesta para interaccionar. Mediante estos, la aplicación puede solicitar o consultar una aserción, o bien solicitar a un usuario que se autentifique. Estos son los protocolos:

- *Authentication request protocol*
- *Assertion query and request protocol*
- *Single logout protocol*
- *Artifact resolution protocol*
- *Name identifier management protocol*
- *Name identifier mapping protocol*

2) *Bindings*: los enlaces detallan cómo realizar la transferencia de los mensajes del protocolo SAML mediante los protocolos de transporte subyacentes.

3) Perfiles: definen cómo las aserciones, los protocolos y los enlaces SAML se combinan y restringen para proporcionar una mayor interoperabilidad en escenarios de uso particulares.

4) Aserciones: una aserción SAML es el mensaje que le dice a un proveedor de servicios que un usuario ha iniciado sesión. Las aserciones SAML contienen toda la información necesaria para que un proveedor de servicios confirme la identidad del usuario, incluida la fuente de la aserción, la hora en la que se emitió y las condiciones que hacen válida la afirmación.

Documento XML creado por el proveedor de identidad (IdP) que envía al proveedor de servicios (RP), y que puede contener una o más declaraciones.

5) Metadatos: definen la forma de expresar y compartir información de configuración entre partes de SAML.

6) Contexto de autenticación SAML: se utiliza en la declaración de autenticación de una aserción para transportar esta información.

En el siguiente esquema se describe cuál es flujo para un inicio de sesión único (SSO) cuando un usuario accede a una aplicación y esta requiere identificar al usuario.

Figura 18. Flujo para un inicio de sesión único (SSO) cuando un usuario accede a una aplicación y esta requiere identificar al usuario

Fuente: Overview of SAML

- **Primer paso:** el usuario intenta acceder a un recurso en el proveedor de servicios, pero aún no se ha autenticado en el SP.

- **Segundo paso:** la aplicación identifica el origen del usuario y redirige al usuario al proveedor de identidad (IdP), para iniciar el proceso de autenticación, en el caso de que no tenga sesión activa.

- **Tercer paso:** se establece una sesión con el proveedor de identidad (IdP).

- **Cuarto paso:** el proveedor de identidad autentica al usuario, creando una aserción SAML de respuesta de autenticación en forma de un documento XML que contiene el nombre de usuario o la dirección de correo electrónico del usuario; lo firma con un certificado X.509 y envía esta información al proveedor de servicios.

- **Quinto paso:** el proveedor de servicios (RP) recibe la aserción SAML y valida la firma utilizando la clave pública, para garantizar que la aserción SAML sea su IdP de confianza y que ninguno de los valores de la aserción ha sido modificado.

- **Sexto paso:** se establece la identidad del usuario y se le proporciona acceso a la aplicación.

6. Identidad autosoberana

Las principales limitaciones que tiene la identidad digital es la **falta de confianza de los usuarios** para gestionar su identidad y la imposibilidad de preservarla. Actualmente, los modelos de identidad digital acaban siendo bien un modelo centralizado, bien un modelo federado que mantiene el control de los atributos de las identidades de los usuarios.

El hecho de que el usuario no tenga el control de su identidad contribuye a la inconsistencia de atributos, que conlleva un cuestionamiento de la certeza de su identidad ante servicios de autenticación de terceros. La **percepción de indefensión del usuario** se incrementa con el desconocimiento del uso que se lleva a cabo y con quién se comparte su identidad.

Los usuarios están supeditados a la disponibilidad del servicio que ofrecen las empresas. Es decir, en el caso de que el servicio no esté activo o la empresa proveedora del servicio desaparezca, se produce una pérdida de los atributos y las credenciales de la identidad de los usuarios del servicio.

Las empresas proporcionan estos servicios con un **propósito económico**, sus intereses consisten en recopilar y almacenar datos de potenciales usuarios de sus servicios. La comercialización y explotación de estos datos conlleva procesos de manipulación y tratamiento, que en la mayoría de los casos compromete la privacidad de los usuarios.

Controlan la identidad digital de sus usuarios, los datos recogidos son almacenados y custodiados en servidores centralizados, y se convierten en potenciales objetivos para sufrir un ciberataque. En esta situación **los usuarios están indefensos ante cualquier ciberataque**, no tienen capacidad de reacción o protección, y se ven indefensos al desconocer cuándo y cuáles han sido sus datos substraídos.

Para superar y resolver estas limitaciones y problemáticas, aparece el modelo de identidad autosoberana, un modelo que **pone al usuario en el centro de la gestión de su identidad empoderándolo**, a la vez que le otorga toda propiedad y control sobre los datos y atributos que componen su identidad digital.

6.1. ¿Qué es la identidad autosoberana?

La identidad autosoberana (SSI, *self-sovereign identity*) defiende la soberanía del individuo respecto a cualquier autoridad para gestionar su identidad.

Un sistema de **identidad autosoberana** proporciona a los usuarios la capacidad de almacenar, gestionar y controlar los datos de su identidad con total autonomía, así como los mecanismos para que de manera autónoma pueda seleccionar cuáles han de ser los datos que desea proporcionar para acreditar su identidad sin la necesidad de un tercero que la certifique.

La identidad autosoberana es un modelo basado en la descentralización de la identidad, no requiere de un tercero para emitir y gestionar la identidad del usuario. Por ello es necesario proporcionar una infraestructura descentralizada que dé seguridad y confianza al usuario.

Esta infraestructura se sustenta en **tres pilares**: el uso de **credenciales verificables**, **identificadores únicos** y la **tecnología *blockchain***, sin requerir la participación de proveedores de servicios de identidad.

La seguridad es proporcionada mediante la utilización de las credenciales verificables (VC), que se sirven de técnicas criptográficas, permiten verificar la información de un usuario, que es representado mediante un identificador único descentralizado (DID).

Según W3C, «las credenciales verificables representan declaraciones hechas por un emisor de una manera a prueba de manipulaciones y respetando la privacidad».

La **tecnología *blockchain*** proporciona una infraestructura descentralizada que otorga al usuario la capacidad de gestionar y controlar su identidad digital.

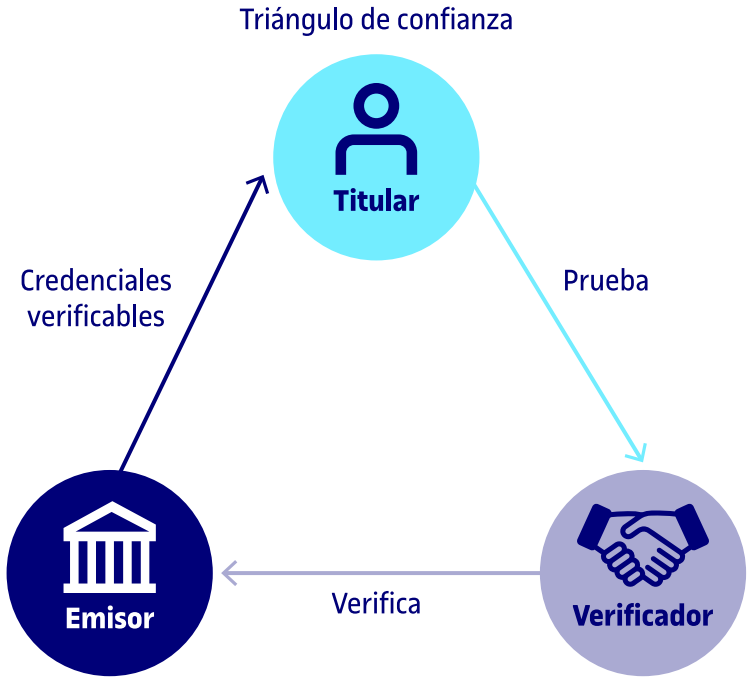
La gestión y utilización de las credenciales verificables necesita de tres actores: emisor, titular y verificador. Su interacción o flujo de intercambio es conocido como el triángulo de confianza:

- **Emisor de credenciales:** es la persona, organización u organismo que emite una credencial verificable a un titular acreditando una determinada información o conjunto de datos.

- **Titular de las credenciales:** persona, organización u organismo propietario de la credencial verificable emitida. Está bajo su control y la gestión es responsabilidad exclusiva del titular.

- **Verificador de credenciales:** persona, organización u organismo que solicita a un tercero presentar una credencial, con capacidad para verificarla y comprobar su veracidad.

Figura 19. Flujo de intercambio en el triángulo de confianza



Fuente: Adaptada de «Self-sovereign identity in the context of data protection and privacy»

6.2. Principios rectores de la identidad autosoberana

Christopher Allen, en su artículo «El camino hacia la identidad autosoberana», recuerda que toda identidad autosoberana (SSI) debe cumplir con unos principios rectores que permitan definirla de manera más precisa.

1) Existencia: los usuarios han de tener una existencia independiente. La identidad autosoberana, como principio, hace referencia al «YO» que existe como ser humano.

2) Control: los usuarios han de controlar sus identidades. No existe ningún organismo u organización que actúe como autoridad superior al usuario.

El control de la identidad del usuario se garantiza mediante la utilización de técnicas criptográficas que garantizan la validez de la identidad y permite verificar las credenciales.

Todo usuario ha de ser capaz de gestionar su identidad; esto incluye la capacidad de modificarla o actualizarla, así como de decidir cuáles deben ser los datos que desea mostrar.

3) Acceso: los usuarios deben poder acceder a sus datos. El usuario ha de poder recuperar las credenciales y datos que hacen referencia a su identidad. En todo momento, el usuario ha de ser consciente y debe estar informado de cuáles son los datos que definen o participan de su identidad.

Acceso

Que el usuario tenga acceso a los datos que definen su identidad no implica necesariamente la capacidad de modificar, alterar o eliminar esos datos atendiendo únicamente a intereses personales.

4) Transparencia: los sistemas y algoritmos han de ser transparentes. Los sistemas responsables de administrar y proporcionar el servicio de identidad han de ser accesibles para que toda persona interesada pueda conocer su funcionamiento.

Los algoritmos utilizados por los sistemas de identidad han de ser de código abierto y lo más independientes posible en la arquitectura que los soporta.

5) Persistencia: las identidades han de ser longevas. Las identidades tienen que estar vigentes y perdurar a lo largo del tiempo, o por el contrario hasta que el usuario así lo desee.

El usuario ha de disponer de una identidad siempre que lo desee, y esta debe ser dinámica y adaptarse a la identidad del titular a lo largo de los años.

6) Portabilidad: la información y los servicios de la identidad han de ser transportables. La identidad no puede estar en custodia, gestión o control por un tercero, sea un proveedor de servicios de identidad autorizado, empresa u otra organización. El cese o desaparición de la actividad supone automáticamente la desaparición de la identidad del usuario.

Para garantizar al usuario tener el control y la existencia de su identidad, es necesario asegurar su portabilidad, y que pueda ser trasladada a otros sistemas.

7) Interoperabilidad: las identidades han de maximizar su uso. La identidad debe estar disponible de manera global y ser utilizada en cualquier entorno sin pérdida del control por parte del titular.

Para asegurar una máxima disponibilidad de la identidad, es necesario garantizar su longevidad, usabilidad y autonomía en cualquier contexto.

8) Consentimiento: los usuarios han de dar el consentimiento al uso de su identidad. Todo intercambio de datos que se produzca debe ser realizado después del consentimiento explícito del titular.

9) Minimización: es necesario minimizar la difusión/divulgación de las afirmaciones. En todo proceso en el que exista un intercambio o compartición de datos, solo se han de revelar aquellos mínimos datos y necesarios para satisfacer el propósito específico del proceso. El proceso deberá garantizar la privacidad del titular.

10) Protección: los derechos del usuario se deben proteger. La autenticación de las identidades se han llevar a cabo mediante algoritmos independientes del sistema de identidad. Los algoritmos tendrán que ser resilientes y resistentes a cualquier tipo de censura, y ejecutarse de manera descentralizada.

6.3. Componentes de un sistema de identidad digital autosoberana

Un sistema de identidad digital autosoberana está compuesto por **tres componentes básicos** fundamentales:

1) Cartera digital (*wallet*)

Una cartera digital o *wallet* es una herramienta, software o hardware, que ha sido diseñada para que el usuario pueda almacenar y gestionar de manera segura sus credenciales de identidad. Estas credenciales son un conjunto de afirmaciones que siguen un modelo de datos estructurados y estandarizados que definen la identidad del titular.

Las carteras digitales utilizan técnicas criptográficas de par de llaves (PK - Clave pública y SK - Clave privada). Las claves públicas se utilizan para intercambiar información, mientras que la clave privada está vinculada al usuario. Es utilizada para compartir afirmaciones o credenciales verificables.

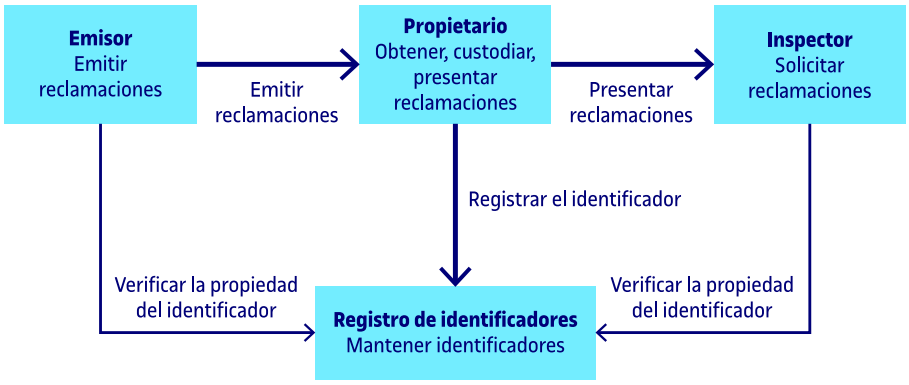
2) Credenciales verificables

Una credencial verificable es un conjunto de afirmaciones y metadatos que se pueden verificar criptográficamente. Hacen referencia al conjunto de una o más afirmaciones (edad, correo electrónico, titulación académica, certificado de nacimiento, etc.) creadas por otra persona o entidad. Son el equivalente electrónico de las credenciales físicas, como pueden ser: el carné de conducir, los títulos universitarios, el pasaporte, el documento de identidad, etc.

Almacenadas en la cartera digital (*wallet*) del titular, son un estándar de la World Wide Web Consortium (W3C), que permite representar las credenciales físicas como credenciales digitales.

Contienen un conjunto de afirmaciones formuladas por el **emisor** al **titular** de la credencial verificable. Esta estará bajo el control del titular, y será el único responsable de su gestión. El **verificador** puede utilizar la credencial verificable para obtener pruebas criptográficas sobre las afirmaciones y su titular, y proceder a su verificación.

Figura 20. Credenciales verificables Data Model 1. 0



Fuente: <https://www.w3.org/TR/vc-data-model/>

En la figura puede observarse el fujo de emisión, la presentación y la verificación de una credencial verificables.

Sus principales características son:

- La difusión de las credenciales es más restrictiva, al poder seleccionar la información o datos que deben compartirse.
- Son más seguras, al utilizar criptografía.
- Mejora la usabilidad y la eficiencia de los procesos de creación, emisión, gestión y control, al poder automatizarse.
- Su uso está condicionado por el consentimiento explícito del titular.

3) Identificadores descentralizados (DID)

Un identificador descentralizado (DID) es un nuevo tipo de identificador único persistente a nivel mundial que no requiere de autoridad de registro centralizada.

Los identificadores descentralizados permiten a sus propietarios demostrar que están bajo su control gracias al uso de pruebas criptográficas, como por ejemplo las firmas digitales.

Los identificadores descentralizados (DID) son un estándar de la World Wide Web Consortium (W3C). Los DID proporcionan un formato común para un identificador único global que es una abstracción de cualquier par de llaves.

Sirven como identificador único para los usuarios, pudiendo tener múltiples DID, e incluyen una mínima información y funcionalidades para garantizar que son resistentes, persistentes e interoperables.

Los identificadores descentralizados se caracterizan por:

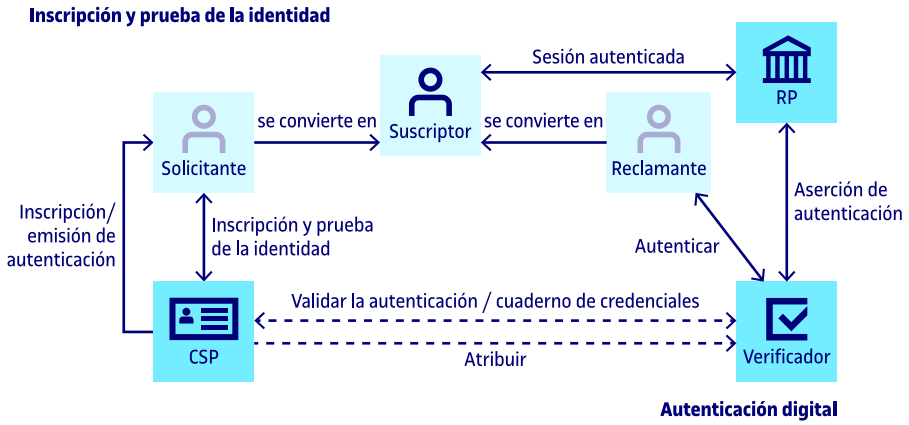
- Estar protegidos mediante una clave privada. Solo el propietario de la llave privada puede demostrar que es propietario y que está bajo su control.
- Admite múltiples claves.
- Permite satisfacer uno de los principios rectores de la identidad digital, la persistencia de la identidad.
- Permite añadir, eliminar o cambiar el par de claves que la controlan.
- Proporciona interoperabilidad entre diferentes sistemas de identidad.
- Controla lo que se conoce como documento DID, que contiene metadatos, *endpoints* u otra información relacionada sobre el DID.

Los DID deben satisfacer las siguientes propiedades:

- **Permanente:** el identificador no ha de cambiar nunca, independientemente de cuál sea su uso, el sistema de identidad o los proveedores de servicios.
- **Resoluble:** el identificador ha de ser capaz de recuperar la clave pública del titular de la identidad.
- **Verificable criptográficamente:** el titular de la identidad ha de poder demostrar que tiene el control de la clave privada asociada al identificador.
- **Descentraliza:** ha de utilizar redes distribuidas como es la cadena de bloques.

Los siguientes modelos de identidad: centralizados, federados y centrados en el usuario, se caracterizan por que el intercambio de credenciales está controlado por el emisor o proveedor de servicios de identidad. Igualmente, tanto la asignación de atributos como el proceso de verificación de la identidad del titular de la credencial siempre han de pasar por el proveedor del sistema de identidad, tal y como se puede observar en la figura siguiente.

Figura 21. Proceso de intercambio de credenciales para los modelos de identidad centralizados, federados y centrados en el usuario

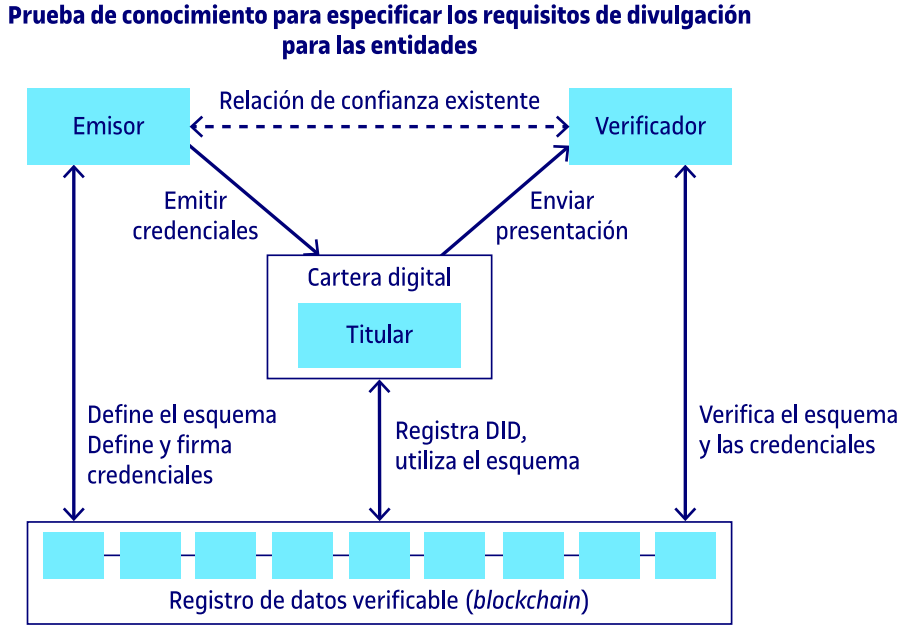


Fuente: NIST Special Publication 800-63-3

Este esquema representa el proceso de intercambio de credenciales para los modelos de identidad: centralizados, federados y centrados en el usuario, y que contrasta con el modelo de identidad autosoberana que ahora se explica.

En la figura siguiente se visualizan los procedimientos y las relaciones que son necesarias establecer en la operativa de un sistema de identidad autosoberana.

Figura 22. Procedimientos y relaciones necesarios en la operativa de un sistema de identidad autosoberana



Fuente: Integrity of Self-Sovereign Identity Solutions

Primero es necesario que exista el conocido **triángulo de confianza** formado por tres actores del sistema: emisor, titular y verificador.

En la parte central, se puede ver representada la **cartera digital** (*wallet*) del titular, que cumplirá con su objetivo de almacenar el conjunto de datos o credenciales que definen o describen la identidad del titular.

También es necesario que exista una **relación de confianza** entre el emisor de una credencial y el verificador. Sin olvidar la capa proporcionada por la cadena de bloques, implementada con **tecnología *blockchain***, que actúa como un único e inmutable registro de datos verificados.

La identidad autosoberana comienza a construirse mediante el **identificador descentralizado** (DID), que otorga la verificabilidad del proceso de identificación de una persona, sin que esta deba revelar ningún dato o información de carácter personal.

El usuario propietario actúa como **titular** (*holder*) de su cartera digital (*wallet*), de manera que es capaz de gestionar autónomamente sus DID y credenciales sin requerir presencia o autorización ante cualquier autoridad centraliza.

La propiedad de un DID, como la propiedad de identidad asociada a un DID, puede ser verificada mediante **pruebas criptográficas** ancladas en la *blockchain*.

Los emisores de credenciales verificables utilizan los DID para identificar el propietario de la credencial emitida, y que solo sus propietarios pueden utilizarlas.

El titular de las credenciales podrá utilizar los datos de las credenciales para acreditar características de su identidad mediante la creación de una prueba verificable. Estas pruebas son un conjunto de datos que se proporcionan a un tercero, que actúa como verificador.

Los **verificadores** actúan como solicitantes de identidades, y son los titulares los responsables de proporcionar el mínimo de datos necesarios para cumplir con el objeto de la verificación requerida por el verificador. El titular tendrá que presentar una prueba, creada a partir del conjunto de datos que están contenidos en una o más credenciales verificables en posesión y bajo el control exclusivo del titular. Este conjunto de datos puede ser verificado criptográficamente.