

Innovación en arquitecturas de identidad digital para garantizar la privacidad en internet

Candidatura de Gataca al Premio de Emprendimiento en
protección de Datos Personales “Ángela Ruiz Robles”

Entidad: Gataca Labs S.L.

Fecha: 14 Octubre 2024

Contacto: hello@gataca.io

Página Web: <https://gataca.io/>

Índice de Contenidos

Introducción	2
Desafíos actuales y solución	2
Solución propuesta por Gataca	5
Propuesta de valor única	7
Funcionamiento	8
Casos de uso	9
Beneficios de la identidad descentralizada	10
Penetración de mercado	11
Tecnología e innovación del proyecto	12
Contexto regulatorio actual	13
Impacto social en la protección de datos	14
Gataca y los Objetivos de Desarrollo Sostenible	15
Equipo y referencias	16
Conclusión	18

Introducción

La identidad es un pilar fundamental para el funcionamiento de cualquier sociedad y economía. Sin embargo, a medida que las sociedades y mercados se hacen más grandes y complejos, también lo hacen los desafíos relacionados con la identidad.

En el mundo físico, hemos desarrollado diversos mecanismos para afrontar este reto, generalmente basados en algún tipo de “prueba” o documento que certifique nuestra identidad, como los pasaportes o las licencias de conducir.

Para que una economía digital funcione de manera eficaz, necesitamos implementar pruebas o credenciales similares en el entorno digital. A lo largo de los años, han surgido diferentes soluciones, desde simples copias digitales de documentos físicos hasta formas más sofisticadas de identificación, como los certificados digitales, las firmas electrónicas y el uso de criptografía de clave pública/privada. Estas tecnologías permiten identificar de manera única los datos digitales y “probar” la propiedad de los mismos.

El concepto de identidad digital, sin embargo, es complejo y sigue siendo objeto de debate. Por ejemplo, el [Instituto Nacional de Estándares y Tecnología \(NIST\)](#) la define como “la representación única de un sujeto 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 sujeto en todos los contextos.” No obstante, existen otras definiciones que varían según el ámbito y la perspectiva.

En Gataca, ampliamos esta noción para incluir la aplicación de la identidad digital al mundo físico. Definimos la identidad digital como un conjunto de atributos que permite a un ente (persona física, jurídica, animal u objeto) identificarse de manera electrónica frente a un tercero. Aunque el formato de identificación es electrónico, el contexto en el que se utiliza no tiene que serlo necesariamente.

No obstante, a pesar de la utilidad que ofrece la identidad digital, persisten problemas cada vez más graves relacionados con su funcionamiento actual. La mayoría de estos problemas no están vinculados directamente a la tecnología, sino a la gobernanza y el control de los datos.

En la era digital, la inmensa cantidad de datos generados y compartidos ha generado enormes desafíos en cuanto a la privacidad y protección de la información personal. Los modelos tradicionales de gestión de identidad, basados en sistemas centralizados y controlados por grandes organizaciones, han mostrado ser vulnerables a violaciones de datos, fraudes y abusos.

Este contexto ha impulsado la búsqueda de soluciones innovadoras que devuelvan el control de la identidad digital a los propios usuarios. Entre estas soluciones, la identidad digital descentralizada emerge como una de las propuestas más prometedoras.

Desafíos actuales y solución

En la actualidad, la gestión de la identidad digital enfrenta múltiples desafíos, muchos de los cuales tienen implicaciones directas en la privacidad, seguridad y control de los datos personales. A medida que la sociedad se ha digitalizado, la forma en que las personas acceden a servicios, interactúan en línea y realizan transacciones se ha vuelto cada vez más dependiente de la identidad digital.

Sin embargo, el modelo predominante para la gestión de estas identidades sigue siendo altamente centralizado, lo que ha generado una serie de problemas y necesidades críticas que deben ser abordadas.



Figura 1: Evolución Identidad Digital

Identidad digital centralizada

La identidad digital centralizada es la arquitectura de autenticación original en Internet adoptada masivamente con la introducción de la [World Wide Web](#) (WWW).

La mayor parte de servicios digitales responden todavía a esta arquitectura, en la que el usuario tiene que crear una cuenta de usuario (una identidad) para el contexto o servicio digital al que quiere acceder y es el proveedor del servicio el encargado de validar y gestionar múltiples identidades en sus bases de datos.

Cuando una persona se registra, por ejemplo, en una red social los datos personales que proporciona (nombre completo, fecha de nacimiento, dirección, domicilio, etc.) quedan bajo el control de esa plataforma, que puede utilizarlos, almacenarlos y compartirlos según sus propios intereses. En muchos casos, los usuarios no tienen visibilidad ni control sobre lo que sucede con sus datos una vez que los han proporcionado, perdiendo soberanía sobre su identidad.

Estos modelos no sólo son un inconveniente para los usuarios, sino también en muchos casos para las organizaciones. Las entidades públicas y privadas concentran millones de registros e información sensible de los usuarios en sus bases de datos, lo que las convierte en un blanco atractivo para los ciberataques. En los últimos años, se han producido numerosos casos de violaciones de datos masivas, donde información personal y sensible de millones de usuarios ha sido comprometida. Estas brechas no solo exponen datos financieros o de contacto, sino que también pueden incluir información crítica, como datos legales, credenciales de acceso, historiales médicos y más. Ejemplos como los ciberataques a empresas como Yahoo!, Equifax o Facebook han demostrado la magnitud del daño que pueden causar estas brechas.

En consecuencia, estas organizaciones deben invertir millones de euros en sistemas de seguridad, cumplimiento del [Reglamento General de Protección de Datos](#) y procesos de autenticación muy complejos para combatir los ciberataques y el fraude de identidad.

Además, cada servicio o plataforma utiliza su propio sistema de identidad, lo que dificulta la portabilidad de los datos personales y el acceso sin interrupciones, lo que en un mundo cada vez más digital hace que sea ineficiente y muy inconveniente para el usuario. Los usuarios necesitan crear y recordar una multitud de credenciales para acceder a diversos servicios en línea, lo que a menudo resulta en prácticas inseguras, como el uso de contraseñas repetidas o débiles.

Identidad digital federada

A principios de la década de 2010 las grandes empresas tecnológicas plantearon un modelo de identidad federado, en el que estas empresas se convertían en un proveedor de identidad intermediario ofreciendo un servicio de inicio de sesión único a los usuarios y una bolsa de usuarios autenticados a terceras empresas para acelerar los procesos de registro.

Los proveedores actuales más conocidos son los ofrecidos por Google, Facebook y Twitter. Para lograr adopción masiva fue necesaria la definición del estándar [OpenID Connect](#) (OIDC), una capa de identidad sobre el protocolo OAuth 2.0, que permite a los proveedores de servicio verificar la identidad del usuario basándose en la autenticación realizada por un Servidor de Autorización provisto por un tercero (proveedor de identidad), así como obtener información de perfil básica sobre el usuario.

Por un lado, este modelo puede mejorar drásticamente la experiencia del usuario al permitirle registrarse al instante a través de sus cuentas de servicios establecidas, pero por otro, agrava los riesgos de privacidad y seguridad al centralizar aún más los datos de los usuarios en sus bases de datos.

Con los modelos federados, los usuarios delegan la gestión de su identidad en las grandes tecnológicas, que reciben el poder de gestionar nuestro acceso a servicios de terceros (es decir, Google gestiona tu acceso a Spotify), al tiempo que acumulan cada vez más información sobre nuestro perfil de consumidor (ahora Google tiene acceso a tus datos y comportamiento en Spotify).

Además, aunque la federación proporciona una cierta apariencia de portabilidad, el poder reside al completo en el proveedor de la identidad. De hecho, las implicaciones para un usuario si su cuenta federada es eliminada o comprometida son mucho mayores si esa cuenta es la clave para otros servicios de terceros, por lo que esta solución todavía no aporta un nivel de control y seguridad necesarios.

Por otro lado, de los tres niveles de seguridad en función del grado de fiabilidad (nivel de garantía bajo, sustancial y alto) diferenciados en el reglamento [eIDAS](#) de identificación electrónica en Europa, el protocolo OIDC únicamente contempla el nivel bajo, por lo que no es válido para acceder a servicios en industrias reguladas; es decir, aquellas que requieren niveles de garantía sustancial o alto, como son servicios de gobiernos, servicios financieros, educativos, del sector salud, seguros, etc.

Identidad digital descentralizada o Identidad Auto-Soberana (SSI)

La irrupción a comienzos del siglo XXI de las tecnologías descentralizadas basadas en registros distribuidos y, en particular, en cadenas de bloques o Blockchain constituyó un verdadero cambio de paradigma.

Las posibilidades que ofrecía ese nuevo contexto tecnológico abrían las puertas a un escenario en el que los tradicionales enfoques organizativos y computacionales centralizados se mostraban obsoletos, dando paso a una nueva arquitectura de identidad digital con una nueva coyuntura de descentralización y desintermediación.

La identidad descentralizada, auto-soberana o SSI por sus siglas en inglés (Self-Sovereign Identity) tiene como objetivo dar al usuario una alternativa a las identidades digitales convencionales. El concepto de identidad descentralizada es una arquitectura de identificación ciudadana que invierte el rol de los actores en la gestión de la identidad. En este modelo los usuarios son quienes gestionan su propia base de datos de credenciales de identidad, controlando en todo momento con quién comparte acceso a su contenido.

La identidad descentralizada cuenta con el desarrollo tecnológico necesario para ser la capa de identidad que falta en Internet y es especialmente relevante en el contexto de la protección de datos personales, ya que aborda algunos de los problemas más críticos del sistema actual:

1. **Privacidad y control de los datos:** Con la identidad descentralizada, los individuos tienen control sobre qué información comparten, con quién, y durante cuánto tiempo, lo que fortalece la privacidad y minimiza la exposición de datos sensibles.
2. **Soberanía del usuario:** La legislación de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa, pone un énfasis significativo en el derecho de las personas a controlar su propia información personal. La identidad digital descentralizada está alineada con estos principios, ya que facilita el cumplimiento normativo al permitir a los usuarios gestionar, actualizar y eliminar su información personal sin tener que depender de terceros.
3. **Seguridad:** Las identidades descentralizadas se basan en tecnologías de criptografía avanzada, lo que refuerza significativamente la seguridad de los datos. En lugar de tener un único punto de fallo, como ocurre con las bases de datos centralizadas, se utiliza el almacenamiento distribuido, lo que reduce el riesgo de ataques y robos masivos de información.
4. **Experiencia de usuario:** La identidad digital descentralizada mejora significativamente la experiencia del usuario al eliminar la necesidad de contraseñas tradicionales, reemplazándolas con métodos de autenticación más seguros, como la biometría del teléfono. Los usuarios pueden gestionar todas sus credenciales desde su cartera de identidad digital, lo que simplifica el acceso a diversas plataformas con un solo conjunto de credenciales reutilizables. Esto no solo facilita el inicio de sesión en múltiples servicios sin tener que recordar diferentes contraseñas, sino que también promueve la portabilidad.

Gataca Labs S.L fue una de las empresas pioneras en apostar por esta tecnología. Originada como un proyecto de investigación en el Massachusetts Institute of Technology (MIT) en 2018, Gataca propuso un marco de autenticación descentralizado que redefine los roles convencionales dentro de la gestión de identidades y desarrolló una solución de identidad descentralizada para facilitar la emisión, verificación y gestión de credenciales digitales de una manera segura y privada.

Solución propuesta por Gataca

Desde su creación, Gataca ha proporcionado una solución integral de identidad descentralizada con dos productos: Gataca Studio y Gataca Wallet.

Gataca Studio

[Gataca Studio](#) es una plataforma *cloud* para organizaciones que permite la emisión, verificación y gestión de credenciales verificables desde un sencillo panel de control.

Las credenciales verificables son un tipo de credencial digital diseñada para ser altamente segura y fácilmente verificable mediante criptografía avanzada, y que garantiza la privacidad habilitando métodos como la divulgación mínima.

Gataca Studio proporciona funciones de emisión de credenciales por parte de autoridades oficiales y herramientas de autenticación de inicio de sesión único para proveedores de servicios, que pueden integrarse fácilmente a través de APIs abiertas.

Los verificadores pueden aprovechar Gataca Studio para configurar de forma flexible los procesos de verificación (qué credenciales deben ser compartidas por el usuario utilizando una cartera de identidad digital o ID Wallet) y proporcionar todos los mecanismos necesarios para verificar la autenticidad de las credenciales recibidas.

Gataca Wallet

[Gataca Wallet](#) es una cartera de identidad digital. Se trata de una aplicación móvil gratuita que permite a los usuarios almacenar y compartir credenciales verificables para autenticarse fácilmente en servicios digitales.

Estas credenciales (documento de identidad, carnet de conducir, diploma, tarjeta de empleado y mucho más), se digitalizan siguiendo estándares abiertos, se firman criptográficamente por las autoridades para garantizar su autenticidad y se protegen con biometría y un cifrado robusto para que solo los usuarios puedan compartir información específica cuando sea necesario y decidir quién accede a sus datos.

Gataca Wallet está disponible en las tiendas de aplicaciones de [iOS](#) y [Android](#).

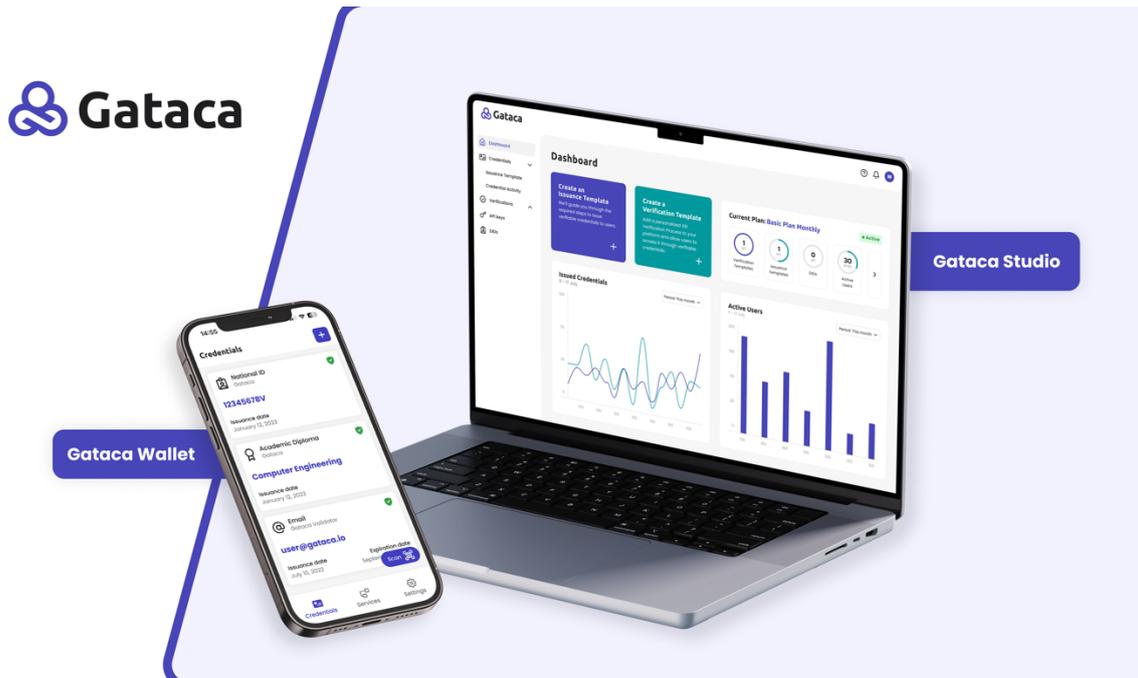


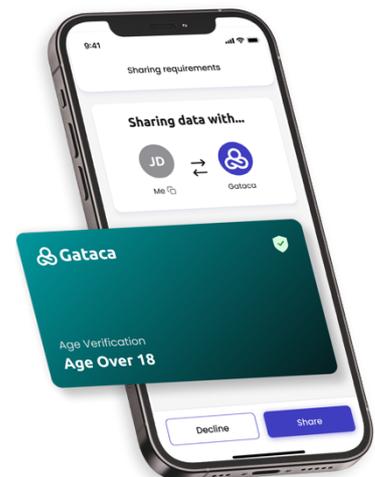
Figura 2: Soluciones de Gataca

Gataca Vouch

De forma complementaria a sus dos productos principales, Gataca ha lanzado en septiembre de 2024 [Gataca Vouch](#), un nuevo sistema de verificación de edad con el que los usuarios pueden confirmar que son mayores de edad sin revelar ninguna información personal usando la Gataca Wallet.

Vouch está diseñado para sitios que requieren verificación de edad, como plataformas de entretenimiento para adultos, citas, juegos online, redes sociales y comercio electrónico con restricciones de edad.

El producto garantiza el anonimato total y minimiza el impacto en el tráfico de las plataformas a diferencia de los métodos tradicionales que pueden ser poco fiables, comprometer la privacidad o dificultar la experiencia del usuario.



Propuesta de valor única

La ventaja competitiva de Gataca se sustenta en la madurez y flexibilidad de nuestro producto y en nuestro posicionamiento como pioneros del mercado, especialmente en Europa.

Somos la primera solución *full-stack* lista para el mercado que es completamente agnóstica a la infraestructura, permitiendo la integración con diversas redes blockchain, incluyendo redes EBSI, Ethereum e Hyperledger Fabric, bases de datos e Infraestructuras de Clave Pública (PKI). Este elemento innovador posicionó a Gataca como un referente mundial.

Además, la arquitectura de Gataca es modular y permite la integración con múltiples marcos de confianza, protocolos de intercambio de credenciales verificables, modelos de datos de credenciales verificables y métodos criptográficos, lo que permite la interoperabilidad del usuario final entre las diferentes implementaciones.

Por otro lado, el siguiente gráfico muestra cómo Gataca Vouch se diferencia de los métodos tradicionales de verificación de la edad, como la autodeclaración, la estimación facial de la edad y la verificación de documentos de identidad.

	Self-declaration	Facial Age Estimation	ID Document Proofing	Vouch
Reliability Age is verified with certainty	✗	✗	✓	✓
Safety Protects minors from harming content	✗	✗	✓	✓
Privacy Protects adults' anonymity/personal data	✓	✗	✗	✓
Unlinkability Does not allow tracking users across services	✓	✓	✗	✓
Usability Allows easy & ultra-fast age verification process	✓	✗	✗	✓

Figura 3: Comparación métodos de verificación de edad

También somos la única startup de identidad descentralizada con certificación ISO, concretamente con la certificación [ISO/IEC 27001:2022](#). Esta norma mundialmente reconocida para los Sistemas de Gestión de Seguridad de la Información (SGSI) subraya nuestro compromiso inquebrantable con la aplicación de las mejores prácticas y la mejora continua de nuestro programa de seguridad basado en riesgos.

Por último, nuestra profunda implicación en desarrollos normativos y tecnológicos que han sido clave en el espacio de la identidad descentralizada nos diferencia de la competencia.

Funcionamiento

Para entender mejor el funcionamiento práctico de las carteras de identidad vamos a comparar el proceso tradicional de verificación de credenciales con el nuevo enfoque,

utilizando como ejemplo el sector educativo. No obstante, este ejemplo puede ser extrapolado a una gran variedad de casos de uso e industrias como veremos más adelante.

Proceso Tradicional

Imagina un escenario en el que Sara, una recién graduada, está solicitando un máster en otra institución. Para ello, debe proporcionar a la nueva universidad pruebas de su título de grado, expedientes académicos y otras certificaciones.

Sara contacta a la universidad donde cursó su grado para solicitar estos documentos, un proceso que puede tardar varias semanas y tiene un costo asociado.

Una vez que recibe los documentos, Sara los envía a la oficina de admisiones de la nueva universidad, que a su vez debe verificar su autenticidad contactando al registro académico de la universidad anterior.

Este proceso retrasa la solicitud de Sara, lo que genera frustración tanto para ella como para las administraciones de ambas universidades. No solo es un proceso lento y costoso, sino también propenso a errores y fraudes. Los documentos en papel pueden perderse, dañarse o ser falsificados.

Proceso con carteras de identidad digitales

Después de graduarse, Sara recibe por parte de su universidad su diploma y sus expedientes en formato digital directamente en su cartera de identidad (Gataca Wallet). Estas credenciales están firmadas criptográficamente.

Al solicitar su programa de máster, Sara puede compartir fácilmente su diploma y expedientes digitales. Escanea un código QR en el sitio web de la oficina de admisiones mediante su cartera de identidad y comparte la información solicitada con un solo clic.

La oficina de admisiones verifica la autenticidad de las credenciales en tiempo real utilizando una plataforma de verificación (Gataca Studio), que comprueba la firma criptográfica para confirmar la autenticidad de los datos y la legitimidad de la universidad emisora.

Sara conserva sus credenciales en su wallet de identidad. Puede verlas, gestionarlas y elegir cuándo compartirlas o revocar el acceso de un servicio a las mismas cuando ella lo desea.

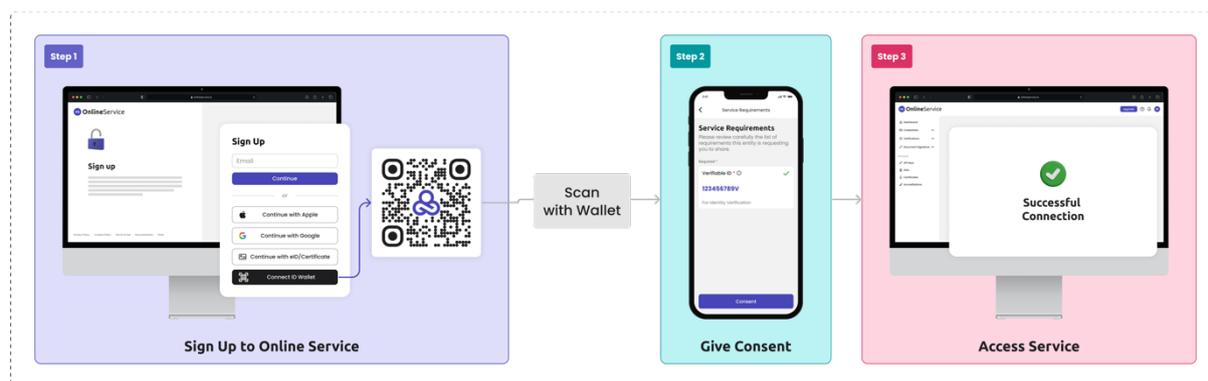


Figura 4: Proceso verificación de edad con carteras de identidad

Video explicativo: https://www.youtube.com/watch?v=O72UMJeVg_o

Proceso de verificación de edad con carteras de identidad digitales

Los usuarios escanean un código QR con su cartera de identidad antes de acceder a contenidos restringidos, comparten una credencial que confirma que son mayores de la edad requerida, y obtienen acceso instantáneo. No se comparte ninguna información personal, ni siquiera su edad exacta o fecha de nacimiento.

La credencial compartida es una credencial verificable de «Mayor de 18 años» (o la edad requerida) obtenida a través de la Gataca Wallet.

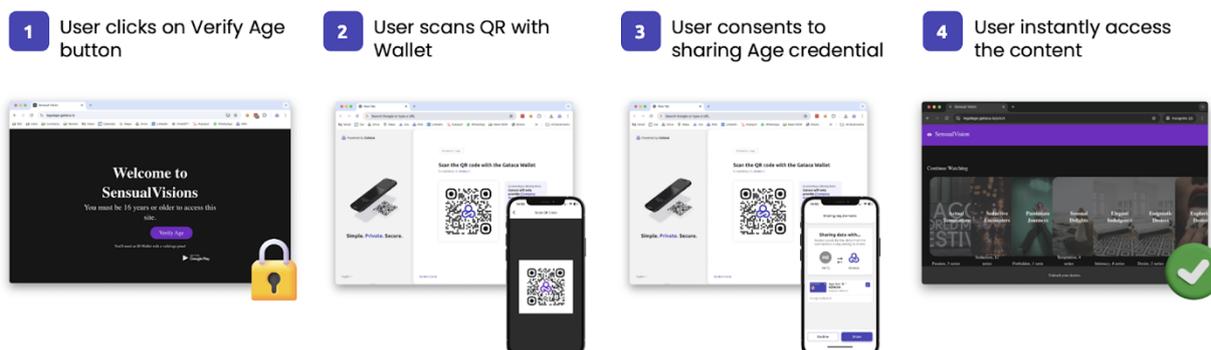


Figura 5: Verificación de edad con Gataca Vouch

Video explicativo: <https://www.youtube.com/watch?v=CFmN12cRIHs>

Casos de uso

La adopción de la identidad digital descentralizada ofrece soluciones a una amplia gama de sectores e industrias. A continuación se exploran algunos de los casos de uso más relevantes:

- **Onboarding de Clientes (KYC / KYB):** Permitir a los usuarios probar su identidad y proporcionar la información necesaria con un solo clic para cumplir con los requisitos de KYC (*Know Your Customer*) o KYB (*Know Your Business*) en los procesos de incorporación de nuevos clientes.
- **Autenticación de Usuarios:** La autenticación mediante la identidad digital descentralizada combina la simplicidad de un inicio de sesión único (Single Sign-On) con mecanismos de autenticación seguros, eliminando el uso de contraseñas.
- **Control de Acceso Físico:** Proveer acceso seguro a instalaciones físicas como oficinas, hoteles, eventos o aeropuertos al integrarse con dispositivos como cerraduras inteligentes o torniquetes.
- **Emisión de Credenciales Digitales:** Emitir certificados, diplomas, tickets o cualquier otro documento de identidad o datos personales.
- **Verificación de Edad:** Verificación fiable de la mayoría de edad para acceder a contenido restringido por edad en plataformas de entretenimiento, comercio electrónico, o redes sociales.
- **Firma de Contratos y Documentos Electrónicos:** Facilitar la firma de acuerdos legales, contratos y otros documentos importantes de manera segura y eficiente.

Beneficios de la identidad descentralizada

A. Para las Organizaciones

- **Mayor Seguridad**

Las carteras de identidad utilizan biometría, cifrado fuerte y almacenamiento distribuido para garantizar la máxima seguridad. Es importante destacar que la información personal nunca se almacena en la blockchain, lo que minimiza el riesgo de exposición.

- **Protección Contra Fraudes**

Las credenciales verificables están protegidas criptográficamente, lo que permite verificar automáticamente la autenticidad de los datos y asegura que no puedan ser alterados o falsificados. Esto garantiza que solo individuos verificados puedan acceder a los servicios de la organización.

- **Cumplimiento Legal**

Las carteras de identidad logran el cumplimiento de normativas de protección de datos y regulaciones de identificación electrónica (eID), incluyendo el RGPD y eIDAS en Europa, al otorgar a los usuarios un mayor control sobre sus datos.

- **Mejora de la Experiencia del Usuario**

Los usuarios pueden disfrutar de un acceso sin contraseñas a los servicios en línea simplemente escaneando un código QR con su cartera digital para compartir sus credenciales. Esto reduce las tasas de abandono en los procesos de registro y aumenta la retención de usuarios.

- **Reducción de Costos**

Las organizaciones pueden reducir los gastos operativos relacionados con la verificación de identidad, el cumplimiento normativo y el almacenamiento de datos, lo que hace que el sistema sea más rentable.

B. Para los Usuarios

- **Control de Datos**

Los individuos tienen un mayor control sobre sus datos. Pueden elegir qué información compartir y con quién. También pueden optar por revelar solo detalles específicos, como compartir solo su nombre y apellido sin revelar su dirección al compartir un documento de identificación nacional.

- **Portabilidad**

Las credenciales digitales permiten a las personas almacenar y llevar de manera segura sus credenciales en una aplicación en su teléfono, lo que les permite compartir su información en cualquier lugar y en cualquier momento.

- **Rapidez**

Los usuarios pueden compartir con un solo clic sus credenciales para la verificación de identidad y autenticación.

- **Reconocimiento Global**

Las credenciales verificables se adhieren a estándares internacionales, lo que garantiza que sean reconocidas y aceptadas a nivel global.

- **Mayor Protección**

Las credenciales verificables están fortificadas con seguridad criptográfica, lo que les permite a los usuarios confiar en que su información personal se mantiene segura.

Penetración de mercado

Las soluciones de Gataca ya están disponibles en el mercado y listas para que las organizaciones las implementen a gran escala.

Algunos de nuestros clientes ya han implementado las soluciones en sus sistemas y las tienen operativas. Sin embargo, la mayoría aún están en la fase de proyectos piloto en entornos

controlados. Esta fase es parte de una estrategia integral y escalonada, diseñada para asegurar una adopción gradual por parte de los usuarios.

A continuación, se destacan los principales sectores en los que Gataca está centrando su actividad comercial, así como los casos de éxito más relevantes obtenidos hasta el momento.

Mercado Objetivo

Según el último [estudio de mercado de Gartner](#), 500 millones de personas utilizarán credenciales verificables en 2026 y el mercado de la identidad descentralizada superará probablemente los 3.000 millones de dólares en 2031.

Gataca es una empresa B2B dirigida a organizaciones de los ámbitos público y privado. Nos centramos en empresas que pueden actuar como emisores y verificadores de credenciales de identidad y ofrecer esta forma de autenticación a sus ciudadanos, clientes o empleados:

- **Instituciones educativas:** Las universidades han comenzado a utilizar carteras de identidad para la gestión de credenciales académicas. Los estudiantes pueden recibir y compartir sus carnets de estudiante, diplomas, certificados, transcripciones de expedientes, etc. de manera digital, lo que agiliza los procesos administrativos y reduce el riesgo de fraude.
- **Servicios públicos:** Gobiernos locales y nacionales están explorando el uso de las carteras de identidad para simplificar el acceso a servicios públicos, como la obtención de licencias y la presentación de documentos para trámites administrativos.
- **Sector financiero:** Bancos y empresas de servicios financieros han implementado carteras de identidad para mejorar el proceso de onboarding (KYC). Estas soluciones permiten a los clientes verificar su identidad de manera rápida y segura, facilitando la apertura de cuentas y otros servicios.
- **Verificación de edad:** Las plataformas que ofrecen contenido, productos o servicios para adultos están adoptando carteras de identidad para implementar una verificación de edad eficaz. Estas garantizan el anonimato de los usuarios y al mismo tiempo proporcionan una experiencia de usuario sin fricciones.

Casos de éxito

- **[UNA Europa](#):** Alianza de 11 universidades de distintos países europeos (500.000 estudiantes). Gataca proporcionó la tecnología para la implementación de credenciales académicas verificables, permitiendo el reconocimiento automático de diplomas y créditos académicos transfronterizos en el programa Erasmus.
- **[FNMT \(Fábrica Nacional de Moneda y Timbre\)](#):** Contrato para la integración de nuestra tecnología con el sistema de backend del gobierno y la proporción de una cartera de identidad digital de marca blanca para generar y almacenar credenciales verificables para el acceso seguro a servicios digitales en tres universidades españolas.
- **[INCM \(Imprensa Nacional Casa da Moeda\)](#):** Gataca ha sido seleccionada por la Casa de la Moneda portuguesa como socio tecnológico para un proyecto de identidad digital que utiliza credenciales verificables para una autenticación sencilla y segura en varios servicios digitales, junto con Universidade Lusófona.
- **[Bankinter](#):** Prueba de concepto para el caso de uso de customer onboarding en instituciones financieras en preparación para el cumplimiento de eIDAS.
- **[ERUA \(European Reform University Alliance\)](#):** Proyecto para facilitar la inscripción y el acceso a talleres y cursos a los miembros de la alianza que integren tecnologías de identidad descentralizada en consonancia con las iniciativas EBSI y eIDAS 2.0.

- [IDEMIA y Gobierno Holandés](#): Como parte del Programa de Adopción Temprana de EBSI, eligieron a Gataca como proveedor tecnológico para un caso piloto de uso de eID Nacional y Diploma Académico.

Tecnología e innovación del proyecto

Hasta la fecha, ningún sistema de identidad ha sido capaz de resolver la disyuntiva entre privacidad, seguridad y experiencia del usuario.

La identidad descentralizada permite combinar por primera vez la sencillez y rapidez de las tecnologías de inicio de sesión único con la criptografía avanzada y las tecnologías distribuidas para una seguridad de extremo a extremo, donde la privacidad también está en el centro del diseño.

Esto se consigue mediante tecnologías disruptivas como son las credenciales verificables, identificadores descentralizados (DID) y, opcionalmente, tecnologías distribuidas (DLT), de la mano del uso de carteras de identidad digitales.

Las credenciales verificables son un tipo de credencial digital diseñada para ser altamente segura y fácilmente verificable mediante criptografía avanzada, y que garantiza la privacidad habilitando métodos como la divulgación mínima.

Esta tecnología asegura que las credenciales no puedan ser alteradas o falsificadas y permite a las organizaciones verificar automáticamente su autenticidad sin depender únicamente de la confianza en el emisor. Es importante señalar que el término «credenciales verificables» se adhiere explícitamente al modelo de datos de credenciales verificables del W3C.

Por otro lado, los identificadores descentralizados (DID) ayudan a los usuarios a representar quiénes son en cualquier contexto sin tener que remitirse a registros de identidad centralizados para los atributos de identidad. Más concretamente, un DID es un identificador único global que no requiere una autoridad centralizada para su generación o registro y es único a nivel mundial y para todos los contextos, independientemente de dónde se vaya a utilizar (a diferencia de un nombre de usuario que sólo se utiliza para el servicio en cuestión).

Gataca fue una de las primeras empresas del mundo en lanzar una plataforma integral de identidad descentralizada.

Originada como un proyecto de investigación en el Massachusetts Institute of Technology y tras participar en el programa de aceleración MIT Delta V, se trasladó su sede operativa desde Boston a Madrid, constituyendo oficialmente la empresa en España en 2019, demostrando desde entonces su carácter innovador.

Esfuerzos como el grupo de trabajo [UX4SSI](#), que define especificaciones técnicas y mejores prácticas para la UX en la identidad descentralizada, o la especificación del Acuerdo de Datos (Data Agreement), dirigida por Gataca, subrayan nuestra dedicación a continuar mejorando.

Otro ejemplo de innovación es el reciente lanzamiento de Gataca Vouch, un nuevo sistema de verificación de edad con el que los usuarios pueden confirmar que son mayores de edad con solo un clic desde su móvil, sin revelar ninguna información personal. Esto es posible usando carteras de identidad digitales.

Desde Gataca, vimos la urgente necesidad de encontrar una solución que ofreciera una protección sólida a los menores de edad y, al mismo tiempo, privacidad absoluta y facilidad de uso para los usuarios adultos ya que en la actualidad no hay ningún método que garantice privacidad, seguridad y experiencia de usuario.

Nuestro equipo supera constantemente los límites, adopta la experimentación y aprende tanto de los éxitos como de los fracasos.

Contexto regulatorio actual

Las iniciativas de identidad digital descentralizada están siendo adoptadas a nivel mundial en mayor o menor medida. Sin embargo, es en Europa donde la regulación eIDAS 2.0 ([Reglamento \(EU\) 2024/1183](#)) impulsará una adopción masiva.

El objetivo es que, para 2030, más del 80% de la población europea disponga de una cartera digital que les permita verificar su identidad y autenticarse al acceder a servicios en línea.

La nueva normativa, que entró en vigor en mayo de 2024, establece que todos los Estados Miembros deben implementar al menos una [Cartera de Identidad Digital Europea](#) en los próximos 24 meses, basada en estándares técnicos comunes. La Gataca Wallet está alineada con estas especificaciones.

Es importante destacar que el alcance de la Cartera de Identidad Digital Europea (EUDI Wallet) no se limita solo al sector público. Los proveedores de servicios privados, como los sectores de transporte, energía, banca, finanzas, seguridad social, salud, telecomunicaciones y educación, que están obligados a utilizar autenticación robusta para la identificación en línea, también deberán aceptar las carteras de identidad como un método de autenticación. Esto significa que la autenticación con tecnología de identidad descentralizada se convertirá en cosa del día a día en los próximos meses.

En este contexto, Gataca se destaca por sus contribuciones clave a la definición de las especificaciones. Su CTO, Samuel Gómez, ha sido uno de los expertos técnicos contratados por la Comisión Europea para dar forma al marco regulatorio recientemente aprobado. Además, Gataca ha sido pionera en debates comunitarios, como la propuesta de privacidad W3C sobre divulgación selectiva, y ha realizado contribuciones significativas, como la iniciativa de la Interfaz Universal Verificable.

Gataca también participa activamente en proyectos de identidad descentralizada, como los pilotos a gran escala eIDAS, en los que forma parte del consorcio [DC4EU](#), compuesto por 80 organizaciones de 22 países. Este consorcio está centrado en el uso de la EUDI Wallet en casos de identidad, seguridad social y educación. Además, Gataca lidera el consorcio [VECTOR](#), cuyo objetivo es avanzar el uso de credenciales verificables y los registros de confianza habilitados por la EBSI en casos de uso transfronterizo.

Además, también en Europa, la [Ley de Servicios Digitales \(DSA\)](#), vigente desde febrero de este año, obliga a todas las plataformas accesibles por menores a implementar medidas efectivas y seguras de verificación de edad que garanticen la privacidad. En este ámbito, la solución Gataca Vouch proporciona una verificación de edad fiable y privada.

Por último, es fundamental mencionar el [Reglamento General de Protección de Datos \(GDPR\)](#). Aunque los usuarios tienen derechos sobre sus datos personales, como el derecho al olvido, a la portabilidad y al acceso, a menudo les resulta difícil ejercer estos derechos cuando sus datos están bajo el control de grandes plataformas. Las soluciones de identidad descentralizada de Gataca permiten a los usuarios tener un mayor control sobre su información personal, cumpliendo plenamente con las normativas de protección de datos a nivel global.

Impacto social en la protección de datos

Disponer de una identidad es un derecho fundamental para todas las personas y tiene importantes implicaciones sobre la libertad individual de cada una.

En un mundo digital donde los servicios se gestionan en línea, la identidad digital cobra cada vez más importancia. En particular, la identidad descentralizada representa un cambio en la forma en que gestionamos y protegemos nuestra información personal en el mundo digital, el cual no solo tiene implicaciones tecnológicas, sino que también tiene un profundo impacto

social en la protección de datos y la garantía de los derechos y libertades de las personas. Gataca enmarca su misión y visión en este contexto.

La identidad digital descentralizada coloca el control de la información personal en manos del individuo. Esto significa que las personas pueden decidir qué datos compartir y con quién, lo que les otorga una mayor autonomía sobre su identidad. Este empoderamiento es especialmente crucial para grupos vulnerables que a menudo son objeto de abuso o explotación. Por ejemplo, las víctimas de violencia de género pueden beneficiarse de la capacidad de ocultar su identidad real y compartir solo la información necesaria para acceder a servicios de apoyo sin temor a represalias.

La descentralización de la identidad digital también mejora significativamente la protección de datos. En los sistemas tradicionales, la información personal a menudo se almacena en servidores centralizados, lo que los convierte en objetivos atractivos para los hackers. La identidad descentralizada distribuye y encripta la información, reduciendo el riesgo de violaciones de datos. Esto no solo protege la privacidad de los usuarios, sino que también aumenta la confianza en las interacciones digitales, permitiendo a las personas participar en la economía digital sin miedo a la exposición de su información sensible.

Además, a través de las tecnologías de la información y la comunicación se está produciendo la conocida como 4ª revolución y no son los países desarrollados los únicos que se están beneficiando de ello. Los países más pobres del mundo ven sus vidas radicalmente mejoradas gracias a estos avances tecnológicos, y en algunos casos, incluso son los primeros en adoptarlos y beneficiarse de ellos.

En cuanto a iniciativas relacionadas con la igualdad, Gataca se enorgullece de contar con un equipo paritario, algo poco común en empresas tecnológicas, siendo una de las pocas empresas en el sector de la ciberseguridad con una mujer a la cabeza.

Irene Hernández, CEO de Gataca, participa regularmente en foros para divulgar su historia e impulsar el emprendimiento en mujeres, comprometida con que las mujeres tengan las mismas oportunidades y que las nuevas generaciones tengan ejemplos con los que referenciarse.

De hecho, Irene ha sido reconocida por su liderazgo, incluyendo el premio “Top 300 mujeres fundadoras en Europa” otorgado por el European Young Innovators Forum, el Premio Emprendedora 2021 de Womenalia y su mención en la lista de las 500 españolas más influyentes en 2023 por el periódico El Mundo.

Gataca y los Objetivos de Desarrollo Sostenible

El derecho a una identidad reconocida es fundamental y se consolidó en 2015 con los Objetivos de Desarrollo Sostenible (ODS), específicamente en el objetivo 16.9, que propone proporcionar acceso a una identidad jurídica para todos.

Tener una identidad es esencial para acceder a derechos y servicios básicos como subsidios sociales, atención médica, educación, derecho a voto, cuentas bancarias y movilidad internacional.

Diferentes estudios ponen de manifiesto el papel que las nuevas tecnologías pueden tener en la consecución de los Objetivos de Desarrollo Sostenible. La revolución que se está llevando a cabo actualmente tiene el potencial de dar lugar a grandes mejoras en la calidad de vida de la ciudadanía, de las cuales los países de bajos ingresos no tienen por qué quedar excluidos.

Según las cifras más recientes de registro de nacimientos de UNICEF, unos 2 mil millones de personas, incluidos 650 millones de niños menores de 16 años, no han recibido certificados de nacimiento. Estimaciones recientes también sugieren que más de 1.100 millones de personas tendrían dificultades para demostrar quiénes son o validar su identidad. Los

sistemas de identificación, y más concretamente la identidad descentralizada, ofrecen la oportunidad de regularizar la situación de estas personas que hoy carecen de pruebas efectivas de su identidad.

Gataca propone, mediante su tecnología, el acceso a servicios transfronterizos mediante una identidad global descentralizada, favoreciendo la igualdad de todos los habitantes, imposibilitando cualquier tipo de discriminación social, racial o de género.

Además, un sistema de identificación inclusivo es un paso importante hacia la igualdad de género y la participación sin trabas de las mujeres en la vida económica y social en línea con el objetivo 5 de los ODS, asegurándose acceso a productos y servicios que requieren prueba de identidad y dándoles mayor control sobre los recursos económicos.



Figura 6: Agenda 2030

También, aunque ciertamente no es suficiente por sí solo, un sistema de identificación que proporcione una prueba de la edad puede desempeñar un papel fundamental en la “eliminación del trabajo y la explotación infantil”, que es parte fundamental del objetivo 8 de los ODS.

Alineado con nuestra solución Gataca Vouch, también puede ayudar a proteger a los menores de contenido inapropiado mediante un sistema de identificación que verifique la edad.

Equipo y referencias

El equipo de Gataca, formado actualmente por 14 profesionales, tiene experiencia en diversos campos, como identidad digital, blockchain, diseño UX/UI, ciberseguridad, gestión empresarial, ventas, marketing y finanzas, y trabaja con el objetivo común de lograr una Internet más segura, privada y eficiente.

Lo que nos distingue no es sólo nuestra experiencia, sino también nuestros logros y experiencia colectiva. Con formación en las mejores instituciones académicas y décadas de experiencia combinada en consultoría para grandes empresas, aportamos a nuestros proyectos un profundo conocimiento y perspicacia.

Estamos reconocidos como líderes en el campo de la identidad autónoma en Europa, con el apoyo de asesores con sólidas redes tanto en el sector público como en el privado.



Figura 7: Equipo de Gataca

Equipo fundador

- **Irene Hernández** (<https://www.linkedin.com/in/irenehernandez/>)

Irene Hernández es una emprendedora, investigadora y conferenciante, actualmente CEO de Gataca.

Cuenta con más de 15 años de experiencia asesorando a empresas multinacionales sobre estrategias de TI y ha llevado a cabo una amplia investigación sobre arquitecturas descentralizadas para sistemas de financiación de identidad y energía en el MIT, lo que le ha valido el reconocimiento como líder de pensamiento en ciberseguridad y tecnologías blockchain.

Ha sido reconocida con el premio «Top 300 Women Founders in Europe» y seleccionada por Forbes como una de las «21 líderes del cambio».

Irene tiene estudios en Ingeniería de Telecomunicaciones y Aeronáutica y un MBA en el MIT Sloan, logrando la beca del Decano del MIT en reconocimiento a sus destacados logros académicos y potencial profesional.

- **Samuel Gómez** (<https://www.linkedin.com/in/samuelgoes/>)

Samuel Gómez, cofundador y CTO, es un desarrollador líder de blockchain con más de 15 años de experiencia en la creación de sistemas para soluciones empresariales. Antes de Gataca, fue líder de blockchain en Grant Thornton y Jefe de Tecnología en BQ.

Samuel también ha sido experto en la materia para la Comisión Europea, ayudando a dar forma al marco para la identidad autosoberana en la región que se ha aprobado recientemente como parte del reglamento eIDAS 2.0.

Además, comparte su experiencia como profesor de tecnologías de libro mayor distribuido (DLT) en la Universidad Complutense de Madrid.

- **José San Juan** (<https://www.linkedin.com/in/jsanjup/>)

José San Juan, CISO y cofundador de Gataca, es un experto en ciberseguridad con 10 años de experiencia en desarrollo de software.

Antes de Gataca, dirigió iniciativas de ciberseguridad e ingeniería en BBVA. En el espacio de la identidad descentralizada, dirigió la iniciativa de interoperabilidad global *Verifier Universal Interface*, siendo reconocido como líder de interoperabilidad en el sector.

Posee una doble titulación en Ingeniería por la Universidad Politécnica de Madrid, así como otro máster en Ciberseguridad por la Universidad Internacional de Valencia.

Experiencia

El equipo de Gataca ha participado activamente en iniciativas de identidad descentralizada tanto regionales como internacionales, demostrando nuestro compromiso innovador con el avance de este campo.

- Contribuciones a la comunidad de identidad descentralizada:
 - Samuel Gómez, CTO de Gataca, fue contratado como uno de los tres expertos de dominio para asesorar a la [Comisión Europea](#) en la definición de las especificaciones técnicas iniciales para ESSIF (European Self-Sovereign Identity Framework) en EBSI.
 - Gataca fue contribuyente a la propuesta de privacidad del W3C sobre divulgación selectiva -[Engineering Privacy for Verified Credentials](#)
 - Líder del grupo de trabajo [Verifier Universal Interface](#) (VUI) Interoperability con 12 entidades involucradas para construir un conjunto de APIs estándar que permitan la interoperabilidad entre carteras de identidad y componentes verificadores. Gataca donó la VUI a la Fundación de Identidad Descentralizada (DIF) para su posterior desarrollo y adopción.
- Gataca también colabora con importantes entidades en torno al debate sobre la identidad descentralizada:
 - Participante en el [consorcio DC4EU](#) para la ejecución de eIDAS Large Scale Pilots, que se centra en el uso de la cartera de identidad digital de la UE para tres casos de uso específicos: Identidad, Seguridad Social y Educación.
 - Líder técnico en el [consorcio VECTOR](#) para avanzar en el [marco EBSI/ESSIF](#).
 - Invitado a representar a Europa en [conversaciones bilaterales con Canadá y África](#).
 - Participación en tres proyectos del programa EBSI Early Adopter como proveedor de tecnología.
 - Miembro colaborador de la [Decentralized Identity Foundation](#).
 - Miembro de [NGI Essif-Lab](#).
- Otros trabajos publicados sobre identidad descentralizada:
 - Bibliotecas básicas de la [Interfaz Universal de Verificación \(VUI\)](#).
 - Publicación de investigación sobre [Zero Knowledge Proof y otros mecanismos de divulgación selectiva](#).
 - Artículo de reflexión sobre [marcos de confianza](#).
 - Post de liderazgo intelectual sobre [métodos DID](#).
 - Post de liderazgo intelectual sobre la [integración de SSI con soluciones de Identity Proofing](#).

Conclusión

La identidad digital descentralizada es una solución innovadora y necesaria en un mundo cada vez más digitalizado, donde la protección de los datos personales y la privacidad se han vuelto esenciales. Gataca ha logrado posicionarse como un líder en este campo, desarrollando tecnologías que no solo cumplen con las regulaciones más estrictas, como elIDAS 2.0 y el RGPD, sino que también mejoran significativamente la seguridad y la experiencia de los usuarios. Al proporcionar control sobre su propia información, nuestras soluciones permiten proteger los derechos y libertades fundamentales de las personas.

Nuestra candidatura para el **Premio de Emprendimiento en protección de Datos Personales “Ángela Ruiz Robles”** refleja nuestro compromiso con la innovación, la privacidad y la seguridad. Las soluciones de Gataca no solo son técnicamente avanzadas, sino que también tienen un impacto social positivo al mejorar la protección de los datos y garantizar que los derechos individuales se respeten en cada interacción digital. Además, nuestra participación en proyectos europeos de gran escala y la colaboración con gobiernos y entidades privadas refuerza la viabilidad y el alcance de nuestra propuesta.

Creemos que nuestra tecnología, nuestra visión y nuestro impacto alinean perfectamente con los objetivos del premio, y estamos seguros de que Gataca puede ser un referente clave en la construcción de un futuro más seguro, transparente y respetuoso con los derechos de los usuarios.