

Estrategia de Identidad Digital



SECRETARÍA

gob digital



Colaboradores Estrategia de Identidad Digital

El Ministerio de Hacienda, a través de la Secretaría de Gobierno Digital, en conjunto con el Ministerio de Justicia y Derechos Humanos, con el respaldo técnico de la OCDE, agradece la colaboración de las siguientes instituciones, expertas y expertos en el proceso de elaboración de esta Estrategia.

- Servicio de Registro Civil e Identificación
- Coordinación Nacional de Ciberseguridad
- Secretaría de Modernización
- Laboratorio de Gobierno
- Coordinaciones Microeconómica y de Mercado de Capitales del Ministerio de Hacienda
- Ministerio de Economía, Fomento y Turismo
- Servicio de Impuestos Internos
- Asesores del Senado
- Asociación de Retail Financiero
- Universidad de Chile
- Chile Telcos
- Asociación de Bancos e Instituciones Financieras de Chile
- Subsecretaría de Telecomunicaciones
- Comisión para el Mercado Financiero
- Asociación Chilena de Empresas de Tecnología de Información
- Chilettec
- Fundación País Digital
- ONG Derechos Digitales
- Universidad Técnica Federico Santa María.

1. Introducción



1.1 Alcance

Este documento propone un marco estratégico para el establecimiento de un nuevo sistema de **identidad digital para las personas naturales** que actúen por sí y, eventualmente, aquellas que actúen en representación de otra persona natural o jurídica. La identidad digital también abarca objetos y sistemas, por lo que el modelo propuesto, si bien no los incluye directamente, tiene el potencial de ser extendido, de manera gradual, a estos otros componentes.



1.2 Relevancia

En un mundo cada vez más digitalizado, es esencial disponer de sistemas e instrumentos robustos de identidad digital que permitan a las personas acceder de manera rápida, segura y confiable a los servicios públicos y privados disponibles en línea. En este contexto, la identidad digital se ha convertido en una herramienta clave para garantizar que la ciudadanía pueda ejercer sus derechos en entornos digitales y en un factor fundamental de la competitividad de nuestra economía digital.

La identidad digital es un habilitante clave para el ejercicio de los derechos de las personas. La identidad, en general, es un derecho humano, reconocido expresamente por la Convención sobre los Derechos del Niño (UNICEF, 1989). En esta línea, de acuerdo con los Objetivos de Desarrollo Sostenible, en particular el ODS 16 sobre paz, justicia e instituciones sólidas, se espera “de aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos” (Naciones Unidas, 2023). A medida que las interacciones entre las personas y las instituciones se trasladan al ámbito digital, resulta evidente que la identidad jurídica debe estar también reconocida y operativa en estos entornos digitales. Contar con una identidad digital robusta hoy en día es fundamental para la inclusión digital, en cuanto permite recibir servicios básicos como atención médica y beneficios sociales, acceder a capital y servicios financieros, e incluso votar, cruzar fronteras o poseer bienes, entre otras actividades (BID, 2017; CEPAL, 2021).

Desde una perspectiva económica, **la identidad digital puede desempeñar un papel clave en el aumento de la productividad y el crecimiento.** En la Unión Europea, se estima que la implementación de billeteras de identidad digital podrían generar un valor añadido a la economía de 1.268 millones de euros en un período de 10 años (European Commission, 2021). En 2020, los pagos digitales se consolidaron como el principal método de compra en la región, lo que contribuyó a un aumento del 18% en el comercio electrónico (WEF, 2022). En el Reino Unido, el actual desarrollo de un nuevo sistema de identidad digital espera generar beneficios de alrededor de 800 millones de

libras esterlinas anuales (Gobierno del Reino Unido, 2022). En Estonia, por su parte, ya sabemos que su sistema de identidad y firma digital le ha permitido a ese país ahorrar hasta un 2% del PIB anual (e-Estonia, 2019). En esta línea, según el informe Estudios Económicos de la OCDE: Chile 2025, Chile se clasifica como una economía de ingreso medio-alto (OCDE, 2025), la implementación de sistemas de identidad digital podría aportar entre un 3% y 13% sobre el PIB total para el año 2030, dependiendo del país y del nivel de adopción (McKinsey & Company, 2019). A nivel mundial, podrían invertirse unos 47,000 millones de dólares al año en tecnologías para proteger la privacidad y asegurar la autenticidad de datos (McKinsey & Company, 2022). Además, se ha estimado que la implementación de sistemas de identidad digital puede reducir los costos de gestión y verificación de identidad requeridos para acceder a servicios digitales hasta en un 50% (Banco Mundial, 2024).

En este contexto, los marcos legales y estratégicos de identidad digital de diversos países se han transformado en una herramienta clave para garantizar el ejercicio de derechos fundamentales, promover la inclusión digital y fortalecer la economía digital. En Chile, como veremos en la sección siguiente, se han logrado avances importantes, pero aún persisten desafíos significativos para consolidar un sistema que se alinee con las mejores prácticas internacionales y responda plenamente a las necesidades de la ciudadanía.

1.3 La identidad digital en Chile

Nuestro país ha alcanzado cierto nivel de madurez en materia de identidad digital gracias a iniciativas pioneras que han sentado bases relevantes para su desarrollo:

- Chile cuenta con un sistema de identidad análogo robusto, en base a un registro poblacional centralizado, a cargo del Servicio de Registro Civil e Identificación ("el Registro Civil"), institución que por ley, tiene la responsabilidad de establecer la identidad civil de las personas. Su infraestructura se sustenta en el Rol Único Nacional (RUN), un identificador único asignado a cada persona al nacer, lo que garantiza la unicidad y universalidad de la identidad de las personas.
- Desde 1995, el Servicio de Impuestos Internos ("SII") ha liderado un importante proceso de digitalización de los trámites tributarios, lo que ha obligado a la industria y, en general, a todos los contribuyentes a familiarizarse con la prestación de servicios públicos en línea (SII, 2003). En este contexto, el SII desarrolló la Clave Tributaria, un par RUT-clave que permite, en principio, acceder a todo tipo de servicios tributarios en línea.
- De manera más transversal, el año 2002 el país estableció por medio de la Ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, la equivalencia funcional de los documentos físicos y electrónicos y reguló de manera clara y precisa la entrega de servicios de certificación de firma electrónica avanzada, creando así un marco de confianza

para estos efectos, el que está compuesto por una Entidad Acreditadora (el Ministerio de Economía, Fomento y Turismo), las entidades acreditadas (las empresas prestadoras de servicios de certificación) y los usuarios y usuarias (quienes obtienen certificados de firma electrónica avanzada de dichas empresas), que pueden ser tanto públicos como privados.

- El principal activo del país en materia de identidad digital es la plataforma ClaveÚnica, desarrollada y operada por la Secretaría de Gobierno Digital (“SGD”). Este mecanismo de autenticación nació en 2010 como una Clave Internet, permitiendo inicialmente el acceso a trámites del Registro Civil. Sin embargo, a partir de 2011, su uso se amplió a otros órganos de la Administración del Estado, consolidándose como un servicio clave que cuenta con más de 15 millones de usuarios y usuarias (SGD, 2024) y facilita el acceso a aproximadamente 1.800 trámites en distintos organismos públicos. No obstante, el marco jurídico actual sólo permite que la Administración Pública y algunas entidades privadas, como las AFP y las prestadoras de servicios de certificación, puedan utilizar ClaveÚnica para autenticar a sus clientes.
- Chile, además, ha adquirido una serie de compromisos internacionales en la materia. En efecto, nuestro país es parte del Acuerdo de Asociación de Economía Digital (“DEPA”), que aborda la interoperabilidad entre identidades digitales. Asimismo, Chile suscribió un Acuerdo Marco Avanzado con la Unión Europea, el que promueve la cooperación en materia de identidad digital, y ha adoptado la Recomendación del Consejo de la OCDE sobre Gobernanza de la Identidad Digital, un estándar internacional respaldado por 38 países y reconocido por el G20 y el G7.



1.4 Desafíos particulares de la identidad digital en Chile

En primer lugar, en Chile, se registra un **aumento en los casos reportados de fraude asociados a la identidad digital**. Los datos hablan por sí solos: la mitad de los chilenos y chilenas ha sufrido algún intento de fraude con pagos electrónicos (Universidad Gabriela Mistral & Black & White, 2023); el 29% de los adultos mayores afirmó haber sido víctima de un fraude digital en lo que iba del año, según datos recopilados hasta julio de 2024 (ClaroVTR & Critería, 2024); y, en 2023 se reportaron 21 mil casos de troyanos bancarios en Chile (Kasperky, 2023). Así entonces, el *phishing* se ha consolidado como una de las amenazas cibernéticas presentes en Chile. Los estafadores utilizan correos electrónicos, mensajes de texto y redes sociales para engañar a las víctimas y obtener información confidencial, como datos bancarios o contraseñas. Las cifras criminales son coherentes con este escenario. El delito de suplantación de identidad ha aumentado entre un 30% y un 45% (PDI, 2022a). Asimismo, según la Policía de Investigaciones de Chile, en 2022, el 58% de las estafas reportadas se cometieron a través de Internet (PDI, 2022b).

En segundo lugar, **el marco regulatorio sobre identidad digital es débil y limitado.**

Aunque se han logrado avances, tanto en el sector público como en el sector privado, las soluciones de identidad digital (sean requeridos ya sea para identificar, autenticar, autorizar, consentir, firmar electrónicamente u otro fin) no están respaldadas por una regulación suficientemente sólida que garantice una identidad digital segura y confiable para toda la ciudadanía. Por el contrario, la escasa regulación vigente está muy fraccionada. A nivel de ley, por ejemplo, sólo se ha regulado la prestación de servicios de certificación de firma electrónica avanzada, una herramienta que, inserta en un sistema de identidad digital más amplio, podría ser mucho más potenciada. A nivel administrativo, sólo se ha regulado el uso de ClaveÚnica en los órganos de la Administración del Estado, el Poder Judicial y las administradoras de fondos de pensiones (AFP) y cesantía (AFC III). Sin embargo, no existen habilitantes legales que permitan expandir de manera general, segura y confiable el uso de ClaveÚnica en el sector privado. Estos vacíos regulatorios han (i) dificultado la estandarización de sistemas de autenticación y la protección efectiva de los derechos de los usuarios, desincentivando el establecimiento de un sistema público-privado de identidad digital que aproveche la infraestructura pública digital ofrecida por ClaveÚnica e (ii) impedido la consolidación de una identidad digital “jurídica” u “oficial”, que permita acceder a toda clase de servicios públicos y privados, como la que actualmente existe en el mundo análogo, con la cédula de identidad emitida por Registro Civil.

En tercer lugar, **la gobernanza de la identidad digital en Chile está muy fragmentada.**

El Registro Civil establece y registra la identidad civil de las personas y gestiona los documentos oficiales de identidad; la SGD desarrolla y opera las plataformas ClaveÚnica, CasillaÚnica y FirmaGob; el Ministerio de Economía acredita, inspecciona y regula el mercado de la firma electrónica avanzada; el SII opera la Clave Tributaria; y diversos órganos sectoriales, como la Comisión para el Mercado Financiero, la Superintendencia de Pensiones, la Subsecretaría de Previsión Social y el Poder Judicial, han dictado normas administrativas relacionadas con autenticación de personas naturales. Con todo, no existe una institución claramente responsable de liderar y coordinar el ejercicio de estas competencias ni mucho menos un sistema más amplio de identidad digital. Tampoco es claro si el modelo actual es descentralizado (como indica la regulación de firma electrónica avanzada), centralizado (como funcionan la ClaveÚnica y la cédula de identidad digital), o federado. Todo esto limita la capacidad del Estado para tomar decisiones estratégicas que involucren múltiples actores, aprovechar economías de escala, disminuir costos administrativos, definir casos de uso, coordinar verticalmente a los actores involucrados, y utilizar de manera eficiente su infraestructura pública digital, entre otros problemas.

2. Visión

Para el año 2030, Chile contará con un ecosistema de identidad digital al servicio de las personas, construido sobre una sólida alianza público privada, lo que le permitirá consolidarse como líder regional en economía digital y transformarse en uno de los nuevos líderes mundiales en identidad digital.

3. Objetivo de la Estrategia de Identidad Digital

Implementar un nuevo sistema de identidad digital inclusivo, seguro y confiable que permita a las personas naturales que actúen por sí y eventualmente, aquellas que actúen en representación de otra persona natural o jurídica, acceder de manera simple y amigable a toda clase de productos y servicios digitales públicos y privados, nacionales e internacionales.

4. Nuevo sistema público-privado de identidad digital



4.1 Explicación del modelo

En general, en el mundo existen dos grandes sistemas de identidad, el centralizado y el descentralizado. El modelo centralizado, adoptado en gran parte de América Latina, supone la existencia de una única institución pública que gestiona el registro de identidad y emite documentos oficiales. En otros países, como Canadá, Estados Unidos y Reino Unido se ha optado por un modelo descentralizado, en el que existen múltiples entidades que emiten identificaciones funcionales para usos específicos.

Esta estrategia propone construir un marco de confianza de identidad digital en base al **modelo centralizado para el otorgamiento de la identidad fundacional** actualmente en funcionamiento en el país. La mesa público-privada consideró fundamental mantener esta característica del modelo actual, aprovechando su robustez y asegurando la continuidad del sistema análogo de identidad digital, que ya cuenta con altos niveles de adopción y confianza a nivel nacional. Sin ir más lejos, el principal activo de identidad digital del país, la plataforma ClaveÚnica, está construida sobre el rol único nacional que le entrega a las personas el Registro Civil.

Este modelo deberá ser necesariamente implementado mediante una colaboración público-privada. En primer lugar, para asegurar la adopción y escalabilidad en el sector privado, será imprescindible que entidades privadas complementen las capacidades de la Administración para (i) integrar instituciones al sistema, asumiendo, en el mediano plazo, la co-responsabilidad de ejercer como canal de distribución, y (ii) identificar las necesidades de los distintos sectores de la economía y grupos de personas usuarias. En segundo lugar, para asegurar la seguridad, interoperabilidad y resiliencia del sistema también será fundamental contar con la asesoría técnica y servicios de confianza prestados por entidades privadas, los que podrían sumarse a la infraestructura pública digital ofrecida por la SGD, bajo el modelo de un marco de confianza. Así, el sistema será construido sobre la experiencia de las prestadoras de servicios de certificación de firma electrónica avanzada y aprovechará las capacidades de operación, innovación, agilidad y adaptación del sector privado. En este sentido, el sistema será en parte descentralizado tanto en la integración (canal de distribución) como en la operación (provisión de servicios de confianza).



4.2 Implementación del nuevo sistema

La presente estrategia propone implementar este nuevo modelo en dos etapas corto y mediano plazo, las que reflejan un enfoque progresivo y adaptativo, que equilibra la implementación inmediata de las soluciones con la preparación para el escalamiento futuro. A continuación se describen la gobernanza, modelo tecnológico y estrategias de financiamiento propuestos para cada una de estas etapas.

De cara al año 2026 (corto plazo), se propone implementar un nuevo modelo de identidad digital aprovechando el marco legal y de gobernanza vigente, consolidar a ClaveÚnica como la componente de identidad de la infraestructura pública digital del país y mantener el modelo de financiamiento transaccional que utiliza tradicionalmente el Registro Civil. El foco estará puesto en servicios de autenticación y la seguridad del sistema, incluyendo el establecimiento colaborativo de estándares técnicos, para que éste pueda escalar en el mediano plazo sobre una base sólida.

◆ **Gobernanza.** La rectoría del sistema estará a cargo de un Comité Ejecutivo de Identidad Digital integrado por (i) el Registro Civil, como responsable del establecimiento de la identidad original y proveedor de la cédula de identidad digital; (ii) la SGD, como líder y coordinador del uso de tecnologías digitales en la Administración y proveedor de ClaveÚnica; (iii) la Agencia Nacional de Ciberseguridad (en adelante e indistintamente, “ANCI”) como auditor de la seguridad del modelo de identidad; y (iv) la Entidad Acreditadora del Ministerio de Economía, Fomento y Turismo, como ente regulador e inspector de un servicio de confianza en particular (firma electrónica). Este Comité podrá apoyarse en otras instancias asesoras, de carácter técnico y consultivo para el ejercicio de sus funciones.

◆ **Tecnología.** Esta etapa estará enfocada en proveer una solución tecnológica que facilite la autenticación segura de las personas en servicios públicos y privados disponibles en línea. En específico, se avanzará en una pasarela o broker de identidad digital para ofrecer diversos servicios de autenticación sobre la infraestructura de ClaveÚnica. El primer servicio que se agregará será la Cédula de Identidad Digital provista por el Registro Civil. De esta forma, se podrá elegir entre un factor primario de autenticación (ClaveÚnica) y otro mecanismo que, por diseño, entrega un mayor estándar de seguridad (Cédula de Identidad Digital). Este modelo asegura un equilibrio entre usabilidad y seguridad, facilita la interoperabilidad, le otorga flexibilidad y adaptabilidad al sistema y, eventualmente, incluso podría fortalecer la seguridad del proceso de obtención de certificados de firma electrónica avanzada, el que, por mandato legal, requiere de la comprobación fehaciente de la identidad de la persona solicitante.

Este **broker** o pasarela, construido sobre la infraestructura pública digital provista por la SGD (ClaveÚnica) podrá ser utilizada por los órganos de la Administración, en la forma que determina la Norma Técnica de Autenticación asociada a la Ley de Transformación Digital del Estado, y por otras entidades públicas y privadas, según los criterios, forma, alcance y gradualidad que determine el Comité Ejecutivo de Identidad Digital.

Financiamiento. Para implementar el nuevo sistema de identidad digital es fundamental contar con un modelo de financiamiento claro y que atienda a los costos de inversión inicial, el soporte continuo de la operación, el despliegue de campañas de difusión, el desarrollo de modelos de adopción y, eventualmente, la generación de subsidios o apoyo para la implementación de proyectos específicos. Bajo este entendimiento, en esta etapa, se propone mantener el modelo de “costo distribuido”, asociado al volumen de transacciones, actualmente utilizado por el Registro Civil para cobrar por los servicios de ClaveÚnica a las entidades privadas que la utilizan para autenticar a sus clientes. En el caso del sector público, estos costos seguirán siendo financiados por el presupuesto corriente de la SGD. Esta propuesta es concordante con lo acordado por la mesa público-privada, la que recomendó optimizar los recursos existentes, garantizando que los servicios públicos de identidad digital sean gratuitos y accesibles para toda la población.

De cara al año 2030 (mediano plazo), se propone expandir el nuevo modelo de identidad digital bajo un nuevo marco de gobernanza, encabezado por una única entidad rectora, que abarque todos los servicios de confianza. Sin perjuicio de lo anterior, se seguirá implementando el broker, con la intención de sumar servicios de confianza provistos por entidades públicas y privadas, en principio, bajo un modelo de costo distribuido basado en el número de transacciones.

◆ **Gobernanza.** En esta etapa, la rectoría debería ser asumida por una única autoridad pública claramente establecida por ley. Además, cualquier entidad debidamente acreditada, sea pública o privada, podrá prestar servicios de confianza de manera independiente y, tratándose de servicios de autenticación, eventualmente sumarse al broker tecnológico administrado por la SGD. La acreditación respectiva podrá ser realizada directamente por la autoridad o en base a informes o auditorías de terceros. Sin perjuicio de lo anterior, el establecimiento de la identidad fundacional seguirá siendo responsabilidad del Registro Civil. Eventualmente, si las condiciones legales y técnicas lo permiten, a este marco de confianza de identidad digital de las personas podrán también sumarse objetos y sistemas, así como otras entidades, como la Subsecretaría de Telecomunicaciones.

◆ **Tecnología.** En lo referido a la infraestructura pública digital para la autenticación, se podrán sumar al modelo de broker de identidad otros mecanismos administrados por entidades públicas y privadas que cumplan con los requisitos exigidos por la autoridad pública establecida por ley. Respecto de otros servicios de confianza, se fomentará el desarrollo y operación de estas soluciones por parte de entidades públicas y privadas, mediante el establecimiento de estándares que permitan generar nuevas oportunidades de negocio.

◆ **Financiamiento.** A mediano plazo, el sector privado se espera que siga contribuyendo a la prestación de servicios de autenticación mediante un modelo de financiamiento de cobro distribuido (pago por transacción). Respecto del sector público, actualmente bajo un modelo de costos centralizado, deberá evaluarse si corresponde que también adopte un modelo de costo distribuido, en el que las instituciones contribuyan con presupuesto propio a la operación de los servicios de autenticación, en proporción al volumen de transacciones que realizan sus personas usuarias.

La Tabla N° 1 contiene un resumen del nuevo sistema de identidad digital. Además, esta estrategia cuenta con un plan de acción, el que será revisado y actualizado cada seis meses por la SGD.

Actividad	Responsable(s) corto plazo	Responsable(s) mediano plazo
Establecer o verificar la identidad original	Registro Civil	Registro Civil
Elaborar decretos, reglamentos y leyes	- Ministerio de Hacienda - Ministerio de Justicia y DDHH	- Ministerio de Hacienda - Ministerio de Justicia y DDHH
Liderar y coordinar el sistema Establecer estándares funcionales, tecnológicos, de confianza y de seguridad Acreditar cumplimiento de estándares	- Comité Ejecutivo de Identidad Digital ◇ SGD ◇ ANCI ◇ Registro Civil ◇ Entidad Acreditadora (MINECON)	Autoridad pública claramente definida
Fiscalizar el cumplimiento de estándares	- ANCI - Registro Civil	Autoridad pública claramente definida
Prestar servicios de confianza	- SGD - Registro Civil	- Entidades acreditadas - SGD - Registro Civil
Sumar servicios de confianza al broker de identidad digital	SGD	SGD
Integrar servicios de confianza en entidades públicas y privadas para autenticar a sus usuarios/clientes	- SGD - Entidades privadas	- SGD - Entidades privadas
Cobrar a las entidades privadas que utilicen servicios de confianza públicos para autenticar a sus clientes	Registro Civil	Autoridad pública claramente definida
Proveer el servicio de claves que cumplan estándares	SGD	SGD

5. Bibliografía

- **European Comission. (2021).** Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea <https://eur-lex.europa.eu/legal-content/CS-EN/TXT/?from=EN&uri=CELEX%3A52021PC0281>
- **Banco Interamericano de Desarrollo. (2017).** La gestión de la identidad y su impacto en la economía digital. <https://publications.iadb.org/en/la-gestion-de-la-identidad-y-su-impacto-en-la-economia-digital>
- **Banco Mundial. (2024).** Tendencias en identificación para el desarrollo: Conjunto de datos global ID4D 2021, Volumen 3. Banco Mundial. <https://documents1.worldbank.org/curated/en/099031924132035631/pdf/P17634114229a80dc18ea11c4c279817517.pdf>
- **CEPAL (2021).** Panorama Social de América Latina 2020. Publicación de las Naciones Unidas. Santiago. <http://www.cepal.org/en/publications/46688-social-panorama-latin-america-2020>
- **ClaroVTR & Criteria. (2024).** Informe de resultados: Radiografía Digital Senior Tech - Personas mayores. Santiago, Chile: ClaroVTR y Criteria. Recuperado de <https://www.clarovtr.com/informe-senior-tech-2024>.
- **Centro de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Gobierno de Chile. (2020).** Procedimiento para denunciar suplantación de identidad en redes sociales. CSIRT. <https://csirt.gob.cl/ciberconsejos/procedimiento-para-denunciar-suplantaci%C3%B3n-de-identidad-en-redes-sociales/>
- **e-Estonia. (2019).** Global Digital Society Fund. Recuperado de <https://e-estonia.com/global-digital-society-fund/>
- **Foro Económico Mundial. (2022).** Acelerando los pagos digitales en América Latina y el Caribe. Recuperado de https://www3.weforum.org/docs/WEF_Accelerating_digital_payments_SP_2022.pdf
- **Gobierno del Reino Unido. (2022).** Consulta sobre identidad digital y atributos. Recuperado de <https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation>

- **Kaspersky. (2023).** Nueva epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyo de la IA. Blog oficial de Kaspersky. <https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/>
- **McKinsey & Company. (2019).** Digital Identification: A key to inclusive Growth. <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20identification%20a%20key%20to%20inclusive%20growth/mgi-digital-identification-executive-summary.pdf>
- **McKinsey & Company. (2022).** How telcos can succeed in launching new businesses beyond connectivity. McKinsey & Company. <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-telcos-can-succeed-in-launching-new-businesses-beyond-connectivity>
- **Naciones Unidas. (2020).** Hoja de ruta para la cooperación digital. Naciones Unidas. Roadmap for digital cooperation. United Nations. https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
- **Naciones Unidas. (2023).** Informe sobre los Objetivos de Desarrollo Sostenible 2023. Naciones Unidas United Nations. https://unstats.un.org/sdgs/report/2023/The-Sustainable-Development-Goals-Report-2023_Spanish.pdf
- **OECD & CAF (2024).** Revisión del Gobierno Digital en América Latina y el Caribe: Construyendo Servicios Públicos Inclusivos y Responsivos, OECD Publishing, Paris, <https://doi.org/10.1787/7a127615-es>
- **OECD. (2024).** 2023 OECD Digital Government Index: Results and Key Findings. OECD Public Governance Policy Papers. <https://doi.org/10.1787/24bac82f-en>
- **OCDE. (2025).** Estudios Económicos de la OCDE: Chile 2025. OCDE. <https://www.oecd.org>
- **Policía de Investigaciones de Chile (PDI). (2022a).** Ciberdelitos continuaron al alza en 2021. PDI Chile. <https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2022/01/04/ciberdelitos-continuaron-al-alza-en-2021>
- **Policía de Investigaciones de Chile (PDI). (2022b).** Un 58% de las estafas se cometen por Internet. <https://pdichile.cl/centro-de-prensa/detalle-prensa/2022/07/04/un-58-de-las-estafas-se-cometen-por-internet>
- **Secretaría de Gobierno Digital (2024).** Gobierno Digital en Cifras. <https://digital.gob.cl/transformacion-digital/estadisticas/>

- **Servicio de Impuestos Internos. (2003).** Oferta de gobierno electrónico del Servicio de Impuestos Internos: Factur@ Electrónica, el servicio más revolucionario de la oficina virtual del SII en Internet. Santiago, Chile: Servicio de Impuestos Internos. Recuperado de https://www.sii.cl/home_factura/fasciculo_factura_completa.pdf
- **UNICEF. (1989).** Convención sobre los derechos del niño. Adoptada por la Asamblea General en su resolución 44/25, de 20 de noviembre de 1989. Recuperado de <https://www.unicef.org/es/convencion-derechos-nino/texto-convencion>
- **Universidad Gabriela Mistral & Black & White. (2023).** 50% de los chilenos ha sufrido un intento de fraude. Universidad Gabriela Mistral. <https://www.ugm.cl/encuesta-ugm-y-b-w-50-de-los-chilenos-ha-sufrido-un-intento-de-fraude-con>



SECRETARÍA
gob digital

