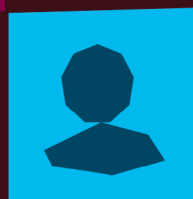
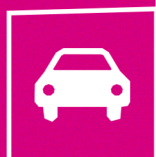
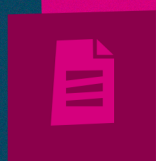


Desafíos del Pix y Gov.br:

soberanía, seguridad e
inclusión de las infraestructuras
públicas digitales (IPD) brasileñas





**instituto de defesa
de consumidores**

Somos una organización independiente que desde hace más de 38 años trabaja en la defensa y promoción de los derechos e intereses de las personas consumidoras.

Denunciamos abusos, presionamos a las autoridades y participamos en el desarrollo de leyes y políticas públicas en la búsqueda de relaciones de consumo justas, saludables y sostenibles en diversas áreas, incluyendo servicios financieros y derechos digitales.

Y eso no es todo. También nos dedicamos a brindar información a la población sobre nuestros derechos y los cambios que necesitamos.

**Para continuar esta lucha,
necesitamos el apoyo de la
sociedad. ¡Únete a nosotros y
fortalece este trabajo!**



idec.org.br/associe-se



bilby

Equipo Técnico



Dirección Ejecutiva

Igor Rodrigues Britto

Gestión de Comunicación y Participación

Cláudia Focking

Gestión de Desarrollo Organizacional

Marina Nascimento

Gestión Legal

Christian Printes

Gestión de Marketing y Relaciones

Carla Yue

Gestión de Políticas

Renato Barreto

Coordinación de Investigación

Camila Leite Contri

Dayana Moraes

Luã Cruz

Nahema Falleiros

Nathan Paschoalini

Viviane Fernandes

Comunicación, Marketing y Asesoría de Prensa

Luive Osiano

Jéssika Elizandra

Diseño Gráfico y Diagramación

Coletivo Piu

Apoyado por

Co-Develop

Tabla de Contenidos:



Introducción: Infraestructuras Públicas Digitales (IPD) en Brasil	6
Los desafíos de las IPD brasileñas	11
■ Pix - El sistema brasileño de pagos instantáneos	13
Introducción	14
Conociendo el Pix	16
Lentes de Análisis	38
Inclusión Digital	39
Seguridad	49
Soberanía	67
Consideraciones Finales	77
Referencias	82
Gov.br – el portal único del Estado Brasileño	85
Introducción	87
Histórico	88
Servicios	93
Lentes de Análisis	102
Inclusión Digital	103
Seguridad	118
Soberanía	127
Consideraciones Finales	137
Referencias	142
Nuestras principales recomendaciones	150
Recomendaciones de Inclusión Digital	150
Recomendaciones de Seguridad	152
Recomendaciones de Soberanía	156

Introducción: **Infraestructuras Públicas Digitales (IPD) en Brasil** ➔

La digitalización se ha convertido en un elemento estructurante de las sociedades contemporáneas. Gobiernos, empresas y ciudadanos recurren cada vez más a los sistemas digitales para realizar actividades cotidianas, desde el acceso a servicios públicos hasta las transacciones económicas, pasando por la comunicación interpersonal y la gestión de políticas sociales. En este contexto, el concepto de **Infraestructura Pública Digital (IPD)** ha cobrado fuerza en los últimos años.

Para comprender qué son las Infraestructuras Públicas Digitales (IPD), se recurre con frecuencia a metáforas que las acercan a sistemas ya conocidos, como carreteras, tuberías o redes eléctricas. En general, estas comparaciones ayudan a visualizar la función social de estas infraestructuras, que proporcionan acceso a servicios públicos o privados a gran escala. Sin embargo, ante el desarrollo de diferentes Infraestructuras Públicas Digitales en todo el mundo, con diversas formas de gobernanza, implementación y experiencias de uso, aún no existe un consenso en torno a una definición consolidada del término.

Aunque el debate en torno a las IPD ha adquirido protagonismo desde la edición de 2023 del G20 (bajo la presidencia de la India), se observa que el concepto de Infraestructuras Públicas Digitales (IPD) sigue siendo objeto de disputa. La Declaración de los Líderes, emitida por la Cumbre del G20 India, caracterizó las IPD como un concepto en desarrollo, que debe ser construido conjuntamente por los sectores público y privado. Según el documento, estas infraestructuras deben acelerar el desarrollo sostenible e inclusivo, siempre que sean seguras, confiables y respeten los derechos humanos, como el derecho a la protección de datos personales, la privacidad y la propiedad intelectual.

En resumen, el concepto de IPD deriva de la propia noción de infraestructura que, al aplicarse a un contexto de hiperconectividad e intensa digitalización de

la vida, adquiere el significado de infraestructuras que permiten la participación en la vida pública y cívica en el entorno *digital* (Zuckerman, 2020¹).

En un informe publicado en 2023 por el Programa de las Naciones Unidas para el Desarrollo (PNUD), las IPD fueron descritas como un conjunto de sistemas digitales compartidos, seguros e interoperables, basados en protocolos y estándares abiertos para proporcionar acceso equitativo a servicios públicos y/o privados. El documento establece que estos sistemas deben estar sujetos a las leyes y regulaciones aplicables, promoviendo el desarrollo, la inclusión, la innovación, la confianza y la competencia, siempre con respeto a los derechos humanos y las libertades fundamentales (UNDP, 2023)².

La falta de consenso en torno al concepto de IPD se hace aún más evidente cuando se discute el significado del adjetivo “pública” atribuido a estas infraestructuras. Mazzucato, Eaves y Vasconcellos (2024)³, sin embargo, señalan una convergencia entre diversos investigadores: las IPD no necesitan ser gestionadas exclusivamente por el poder público, pero deben ser concebidas tomando como referencia el interés público y bajo supervisión (*oversight*) pública.

En el mismo sentido, Co-Develop⁴ considera que las IPD deben, necesariamente, cumplir con cuatro características esenciales: 1) inclusividad; 2) ser modelos fundacionales; 3) interoperabilidad; y 4) estar sujetas a supervisión y control públicos. Según la organización, serían tres los componentes estructurales de una IPD: i) inclusión financiera; ii) sistema de identidad verificable; y iii) flujo de datos seguro.

El punto común de todas estas conceptualizaciones reside en el intenso proceso de digitalización de la sociedad, cuyo fundamento se encuentra en el

1. ZUCKERMAN, Ethan. What Is Digital Public Infrastructure? [S. l.]: Center for Journalism & Liberty, nov. 2020. Disponible en: <<https://static1.squarespace.com/static/5efcb64b1cf16e4c487b2f61/t/5fb41b6aac578321b0c50717/1605639019414/zuckerman-digital-infrastructure-cjl-nov2020.pdf>>. Consultado el: 20 de septiembre de 2025.

2. UNITED NATIONS DEVELOPMENT PROGRAMME (UNDP). Accelerating the SDGs Through Digital Public Infrastructure: A Compendium of the Potential of Digital Public Infrastructure. New York, Aug. 21, 2023. Disponible en: <https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure>. Consultado el: 20 de septiembre de 2025.

3. MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital Public Infrastructure and Public Value: What is ‘public’ about DPI? London: UCL Institute for Innovation and Public Purpose, 2024. Working Paper Series (IIPP WP 2024-05). Disponible en: <https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi>. Consultado el: 20 de septiembre de 2025.

4. For more details about the framework produced by Co-Develop, visit: <https://www.codevelop.fund/insights-1/what-is-digital-public-infrastructure>

uso y la producción de datos personales y no personales para el funcionamiento de las infraestructuras digitales.

La trayectoria de Brasil hacia el desarrollo de lo que hoy se denomina IPD se entrelaza con la historia del desarrollo tecnológico nacional, considerando que el país ha acumulado, en las últimas décadas, una experiencia significativa en el uso de sistemas digitales para el tratamiento de los datos personales de sus ciudadanas y ciudadanos. En este proceso, el país incluso ha alcanzado proyección internacional al implementar, a gran escala, sistemas como la plataforma Gov.br y el Pix, ejemplos de cómo la combinación entre innovación tecnológica, coordinación estatal y participación social puede transformar el acceso a los servicios públicos, las dinámicas del sistema financiero y el ejercicio de la ciudadanía.

A pesar de las proyecciones alcanzadas, el desarrollo de las IPD brasileñas atraviesa diferentes etapas de evolución, lo que plantea cuestiones críticas y desafíos:

- ➔ ¿Cómo garantizar la universalización de las IPD en Brasil, considerando las desigualdades en el acceso y la calidad de la conexión a internet, así como la baja competencia digital de las personas?
- ➔ ¿Qué medidas se están tomando para que la población no solo tenga acceso a las IPD, sino que también sepa utilizarlas de manera crítica y segura?
- ➔ Ante las fallas y sesgos del reconocimiento facial que afectan a grupos vulnerables, ¿es posible afirmar que las IPD son realmente inclusivas?
- ➔ ¿Existen planes de contingencia y protocolos claros para la respuesta a ataques cibernéticos que puedan paralizar estas infraestructuras?
- ➔ ¿Qué salvaguardas se están aplicando para evitar la vigilancia indebida y el uso abusivo de los datos por parte de agentes públicos y privados?
- ➔ ¿Cómo evitar la dependencia tecnológica de grandes proveedores extranjeros que puedan comprometer la soberanía y la seguridad de las IPD brasileñas?
- ➔ Si el uso de estas tecnologías puede ser cooptado por intereses de actores privados, ¿dónde está la garantía de que servirán al interés colectivo?

Preocupado por los debates que rodean estas cuestiones, el programa de Telecomunicaciones y Derechos Digitales del Idec se dedicó a seguir de cerca el desarrollo de dos IPD brasileñas: Pix y Gov.br.

Gov.br es una de las principales plataformas digitales para acceder a los servicios públicos y, en 2025, alcanzó aproximadamente 170 millones de usuarios registrados. Este portal, lanzado en 2019, es un ejemplo de cómo Brasil busca optimizar la relación entre el Estado y la ciudadanía, con el objetivo de que los servicios públicos sean más rápidos, eficientes y accesibles. Desde una cuenta registrada en Gov.br, los ciudadanos pueden, por ejemplo, consultar beneficios sociales, realizar el seguimiento de trámites legales, obtener documentos como la Libreta de Trabajo Digital, renovar pasaportes, simular la jubilación, presentar impuestos o participar en programas gubernamentales. Gov.br es ahora un pilar de la transformación digital en Brasil.

GOV.BR

gov.br

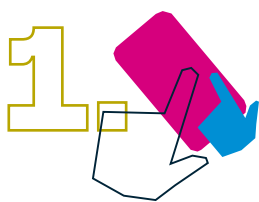
Pix es el principal método de pago y transferencia en Brasil. Creado y administrado por el Banco Central de Brasil, el Pix fue lanzado a finales de 2020, permitiendo que las transferencias de dinero en pocos segundos, funcionando las 24 horas del día, los 7 días de la semana. A diferencia de otros países, donde soluciones similares son privadas, el Pix es una infraestructura pública digital, gratuita para personas físicas e integrada prácticamente con todos los bancos y fintechs del país. El impacto del Pix es enorme: en 2024, movió aproximadamente R\$26,5 billones (aprox. 5,2 billones de dólares estadounidenses) y, según encuestas, fue utilizado por el 76,4% de la población. Esta amplia aceptación ha convertido a Pix en un motor de inclusión financiera y se ha convertido en el método de pago más utilizado en Brasil, superando a las tarjetas de débito, crédito e incluso al efectivo en muchas situaciones cotidianas.

PIX



Basándonos en estudios de estos sistemas y plataformas, y en conversaciones con expertos en el tema, buscamos formular recomendaciones destinadas a contribuir a la mejora de estas tecnologías, para que se desarrollen de forma segura, inclusiva y confiable, maximizando los beneficios sociales sin reproducir desigualdades.

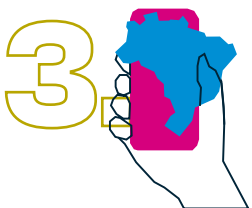
La investigación **“Desafíos del Pix y Gov.br: soberanía, seguridad e inclusión de las IPD brasileñas”** resume la genealogía de estas tecnologías y desarrolla recomendaciones basadas en tres perspectivas analíticas:



Inclusión digital para todas las personas: garantía del derecho universal de acceso y uso de las tecnologías digitales, sin discriminación relacionada con el género, la edad, la raza, la discapacidad, la condición socioeconómica, el nivel educativo o la ubicación geográfica. Guiados por el concepto de conectividad significativa, buscamos garantizar que todos los ciudadanos tengan sus derechos respetados al acceder a los servicios.



Seguridad, privacidad y protección de datos: Los principios de privacidad del consumidor y protección de datos deben ser requisitos fundamentales en el desarrollo de las IPD. Basadas en el concepto de “*privacy by design*” y guiadas por la seguridad, las IPD deben prevenir el fraude, las fugas de datos, la vigilancia indebida y las interrupciones del servicio, a la vez que deben ser capaces de reparar los daños.



Soberanía y gobernanza: que el desarrollo de estas plataformas priorice la soberanía digital brasileña, rompiendo con la dependencia tecnológica de corporaciones extranjeras y combatiendo la extracción económica de datos estratégicos del país. Sus operaciones deben estar alineadas con el interés público, la autonomía científica, la diversidad tecnológica y la legislación nacional, garantizando que Brasil controle y desarrolle sus propias infraestructuras digitales, proteja los datos sensibles y fortalezca su capacidad de innovación para promover el bienestar social y abordar las desigualdades.

Los desafíos de las IPD brasileñas ➔

Las infraestructuras digitales públicas (IPD) se han consolidado en la última década como una de las áreas más estratégicas para la formulación de políticas públicas. Como sistemas digitales compartidos, seguros e interoperables, orientados al interés público, las IPD se han consolidado como la columna vertebral de la prestación de servicios digitales, del acceso a derechos y de la construcción de soberanía en el entorno digital.

Sin embargo, si bien representan avances, Pix y Gov.br también plantean dilemas centrales para las políticas públicas digitales. El primero es la **inclusión digital**. En Brasil, el acceso a los servicios digitales aún se caracteriza por desigualdades estructurales: el ingreso, la educación, la ubicación geográfica, el género y la raza determinan quiénes pueden beneficiarse plenamente de las innovaciones. Personas mayores, poblaciones rurales, pueblos de la Amazonía Legal y familias de bajos ingresos continúan en situación de desventaja. Incluso con una alta penetración de internet en el país, los datos muestran que la **conectividad significativa aún es baja** para más de la mitad de la población. En términos de políticas públicas, esto significa que el avance de las IPD no puede lograrse sin inversiones en infraestructura de red, alfabetización digital y estrategias de inclusión que abarquen a todos. El programa **Balcão Gov.br**, que ofrece asistencia presencial a los usuarios, es un ejemplo concreto de respuesta del gobierno a este desafío, pero sigue siendo una iniciativa limitada dada la magnitud del problema.

Otro punto importante se refiere a la privacidad y la **protección de datos personales**. En 2018, Brasil aprobó la Ley General de Protección de Datos (LGPD), que creó parámetros normativos robustos. Sin embargo, en la práctica, el crecimiento acelerado de las IPD ha revelado fragilidades: integrantes del sistema de pagos ya han informado filtraciones masivas de claves Pix y, con frecuencia, los consumidores sufren **fraudes y estafas**; el Gov.br, al centralizar múltiples servicios y datos sensibles, **se ha convertido en un objetivo preferente de esquemas de phishing y de ingeniería social**. Esto refuerza la necesidad de una estrategia continua de seguridad cibernética, basada en protocolos de “privacy by design” y campañas de educación digital para los consumidores. Desde una perspectiva de política pública, la seguridad debe considerarse no solo como un atributo técnico, sino como un marco de rendición de cuentas para los sectores involucrados, como parte de una agenda regulatoria que **garantice la confianza en el entorno digital**.

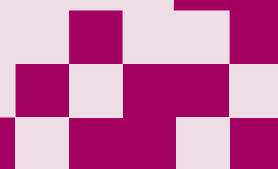
Finalmente, es evidente que el mayor desafío político reside en cuestiones de **soberanía y gobernanza**. Aunque Pix y Gov.br estén concebidos como infraestructuras públicas, su operación y sostenimiento tecnológico aún dependen, en parte, de **servicios y soluciones de empresas extranjeras**. El caso de la “nube soberana”, anunciada como una estrategia para mantener los datos sensibles bajo jurisdicción nacional, ilustra estas tensiones y los intentos de solución. Al mismo tiempo, las disputas comerciales que involucran el Pix (con Estados Unidos investigando su impacto en las empresas de pago estadounidenses y considerando barreras comerciales) demuestran que las IPD no son solo herramientas técnicas, sino también activos geopolíticos, capaces de influir en la posición de Brasil a nivel global.

La gobernanza, en este sentido, se convierte en una palabra clave. El Foro Pix y los Comités (como el Comité Central de Gobernanza de Datos - CCGD y el Comité Consultivo de la Estrategia Nacional de Gobierno Digital - CC-ENGd) son ejemplos de instancias creadas para ampliar la participación social y federativa en el debate sobre las IPD, pero aún necesitan avanzar en **transparencia, diversidad de voces y rendición de cuentas**. Una infraestructura digital robusta requiere equilibrar la eficiencia tecnológica con el control social, garantizando que estas infraestructuras sirvan principalmente al interés colectivo y no sean cooptadas por intereses privados o lógicas autoritarias.



Pix

El sistema brasileño de
pagos instantáneos

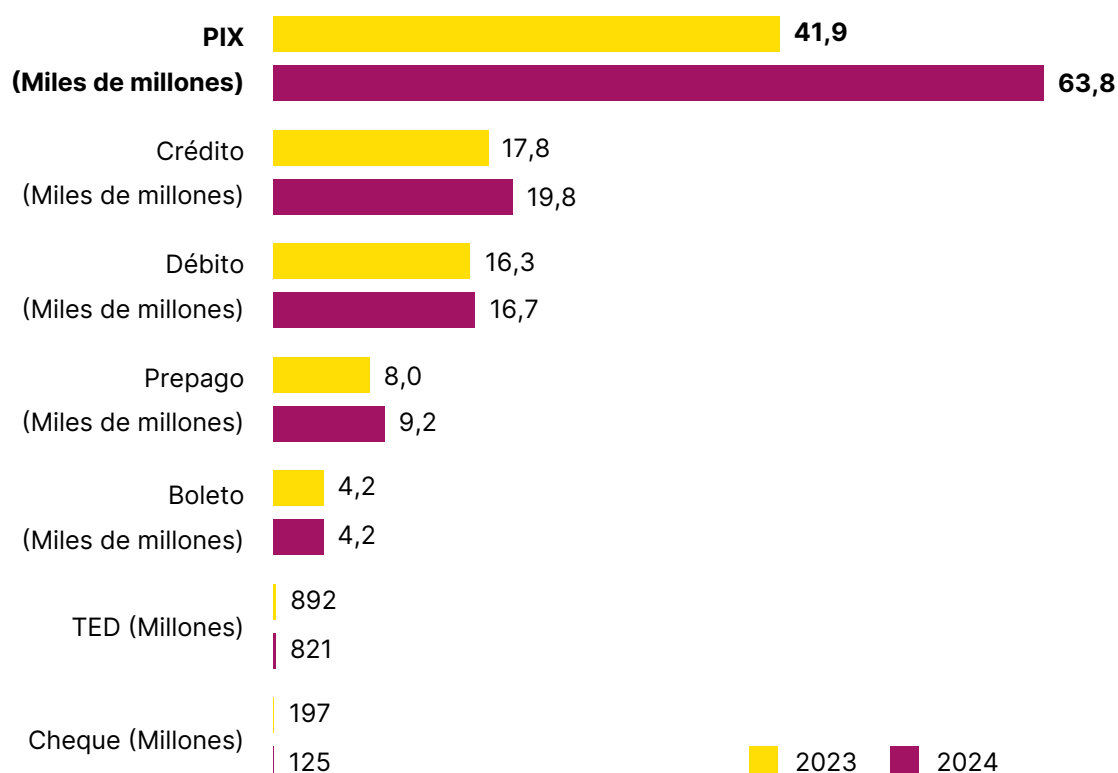


Introducción

«¡Haz un Pix!», «¿Aceptas Pix?», «¡Te paso el Pix!»: expresiones como estas se han vuelto cada vez más frecuentes en el día a día de los brasileños en los últimos años. La implementación del Pix, un medio de pago instantáneo se llevó a cabo junto con una serie de transformaciones tecnológicas en el sistema de pagos brasileño. Si en 2021 el efectivo era la forma de pago más utilizada en el país, esa realidad cambió en 2024 (BCB, 2024a). Pix solo necesitó cuatro años de funcionamiento para **consolidarse como el principal método de pago de Brasil**.

Las cifras son impresionantes: Pix cerró 2024 con 63.800 millones de transacciones, lo que representa un aumento del 52% en comparación con 2023. El volumen supera, con una ventaja significativa, los 50,8 mil millones de operaciones realizadas a través de todos los demás medios de pago combinados (débito, crédito, boletos, TED, cheques y tarjetas prepago) (Febraban, 2024).

Figura 1. Comparación - Métodos de pago (2023 vs. 2024)



Fuente: Adaptado de Febraban (2024)

Este éxito tuvo repercusión en Internet, con publicaciones que destacaban la desaparición del dinero en efectivo. Encontrar dinero en el suelo, dejar una propina o colaborar con el trabajo de un músico callejero son prácticas que se han transformado, ya que las monedas y los billetes han perdido protagonismo en las transacciones cotidianas, desapareciendo de los bolsillos.

La aparición de nuevas tecnologías, la popularización de los smartphones y el aumento de la capacidad de procesamiento de datos fueron decisivos para los cambios en las formas de pago. En la última encuesta del Banco Central de Brasil (BCB, 2024b) sobre los hábitos de uso de efectivo de los brasileños, Pix aparece como el método de pago más utilizado para compras y pago de facturas. En comparación con otros métodos, se considera la opción más ventajosa en prácticamente todos los aspectos evaluados: **seguridad; posibilidad de obtener descuentos; facilidad de uso; costos; control de gastos; y aceptación en los establecimientos.**

Es interesante observar que el uso de un nuevo método de pago trae cambios significativos en la forma en que las personas conducen su vida diaria y, especialmente, en cómo administran su dinero. Los nuevos mecanismos digitales reemplazan prácticas como ir al banco, manejar y contar efectivo físico, emitir cheques y llevar múltiples tarjetas. El smartphone asume el papel de una billetera, especialmente para quienes tienen acceso a internet.

Figura 2. Ejemplo de ilustración sobre el Pix compartida en redes sociales.



Conociendo el Pix

El Pix es el sistema brasileño de pago instantáneo, concebido, lanzado y regulado por el BCB. Fue diseñado para reducir el uso de dinero en efectivo, simplificar y abaratar los pagos y transferencias, así como para resolver lagunas de conveniencia y de costos identificadas en otros medios de pago (Brasil, 2023).

Antes de la implementación del Pix, las transferencias entre instituciones financieras, especialmente para montos pequeños y en moneda local, estaban sujetas a comisiones y restricciones de tiempo, y podían tardar horas o días en completarse, especialmente para transacciones fuera del horario bancario (Brasil, 2025). Con la modernización del sistema de pagos, el BCB buscó cubrir las deficiencias identificadas en productos como cheques, tarjetas (prepago, débito y crédito), TED, DOC y boletos. Así, con la llegada del Pix, las transacciones comenzaron a completarse en segundos y sin costo para las personas. Además, se volvieron disponibles las **24 horas del día, los 7 días de la semana, durante todo el año** (Brasil, 2025).

Un Pix se puede realizar siguiendo pasos simples: solo se necesita un Código QR o una clave de identificación, que actúa como una dirección a la que se enviará el dinero.

5. Como se señala en el Relatório de Gestão do Pix (Informe de Gestión del Pix), el efectivo es costoso de producir, almacenar, distribuir y transportar, además de los costos de seguridad (BCB, 2023).

6. Considerando la experiencia del usuario, el tiempo promedio de transferencia es de hasta 10 segundos. Existe un acuerdo de nivel de servicio con los participantes del Pix, con penalizaciones por incumplimiento, que estipula que el 99% de las transacciones del Pix deben liquidarse en 10 segundos y el 50% en 5 segundos. Según el “Manual de Tempos do Pix”. Disponible en: <https://www.bcb.gov.br/content/estabilidade financeira/pix/Regulamento_Pix/versoes_futuras/IX_ManualdeTemposdoPix-versao-7-0.pdf> Consultado el: 6 de octubre de 2025.

Figura 3. Procedimientos para realizar una transferencia o pago a través del Pix



Fuente: Own elaboration

La elección de la **clave Pix** depende del usuario, quien puede optar por usar su número de teléfono celular, CPF (en el caso de personas físicas) o CNPJ (en el caso de empresas)⁷, correo electrónico o incluso un código alfanumérico de 32 dígitos generado aleatoriamente por el sistema. Por razones de seguridad, las claves Pix funcionan unidireccionalmente, utilizándose únicamente para recibir fondos, nunca para enviarlos. Para garantizar la flexibilidad de los usuarios, las claves pueden migrarse entre las instituciones participantes del ecosistema financiero, siempre que se solicite la portabilidad.

La implementación del Pix, bajo la infraestructura del Sistema de Pagos Instantáneos (SPI), incrementó la competencia en el sistema financiero brasileño al reducir las barreras de entrada y proporcionar una infraestructura pública

7. El CPF (Registro de Personas Físicas) es un número de 11 dígitos que sirve como número de registro de identificación único. Gestionado por la Administración Federal de Ingresos Públicos de Brasil (Receita Federal), sirve para identificar a los brasileños (e incluso a los extranjeros) en diversos contextos, tanto en sus relaciones con el gobierno como con instituciones públicas y privadas. El CNPJ (Registro Nacional de Personas Jurídicas), también emitido por la Administración Federal de Ingresos Públicos de Brasil, es obligatorio para todas las empresas brasileñas. Este número único sirve como documento de identificación fiscal, permitiendo que la empresa sea identificada en todas sus transacciones.

estandarizada operada por el BCB. La unificación de la red de pagos eliminó la necesidad de que cada agente mantuviera sus propios sistemas, favoreciendo la interoperabilidad entre plataformas. Gracias a esta tecnología, instituciones financieras y de pago de diversos tamaños, incluyendo fintechs y cooperativas, comenzaron a operar bajo las mismas normas técnicas y de regulación.

Con el desarrollo de una infraestructura única, cualquier institución autorizada pudo ofrecer transferencias instantáneas. Esta amplia competencia generó innovación y reducciones de costos para los usuarios, quienes dejaron de pagar comisiones por transferencia. El impacto también fue significativo para los comerciantes, que antes dependían de contratos, como el de alquiler de terminales de tarjeta, y con el Pix pasaron a contar con una alternativa de pago más simple y económica. En un entorno con mayor diversidad de agentes y modelos de negocio, la competencia se intensificó, lo que redujo los costos y amplió las opciones para consumidores y empresas.

Entre los **principales objetivos del Pix**, enumerados por el Banco Central (2023), se encuentran:

- ➔ reducir el uso de efectivo y promover una mayor **digitalización** de los métodos de pago;
- ➔ fomentar la **competencia** y promover la **eficiencia** en el mercado de pagos minoristas;
- ➔ impulsar la **innovación** y habilitar **nuevos modelos de negocio**, no solo en el sector financiero y de pagos, sino también en otras actividades de la economía real;
- ➔ democratizar el acceso a los métodos de pago electrónicos y contribuir a la **inclusión** financiera y digital;
- ➔ **reducir el coste** de las transacciones electrónicas
- ➔ ofrecer una experiencia sencilla, segura y **sin fricciones**⁸ al utilizar medios electrónicos.

8. Esta ventaja también resulta ser uno de los aspectos más desafiantes del Pix. La falta de fricción dificulta la resolución de estafas y fraudes, situación que se analizará en los siguientes apartados.

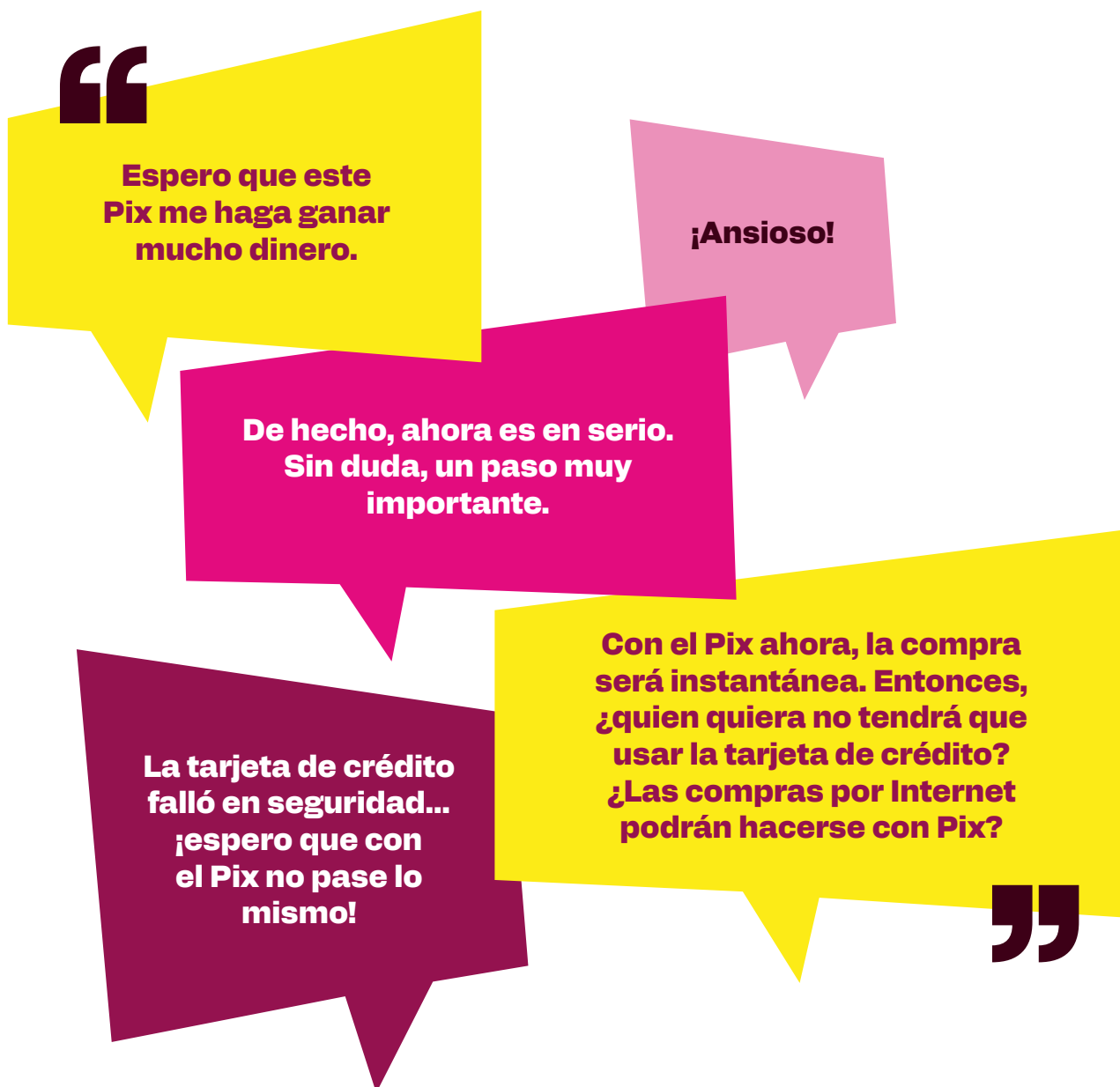
Lanzamiento y Adhesión al Pix

La implementación del Pix en Brasil no fue un proceso aislado. El BCB aprovechó diversas experiencias internacionales relacionadas con los servicios de pago. Como explican Schapiro, Mouallem y Dantas (2023), la participación activa del BCB en foros regulatorios internacionales, como el *Basel Committee*, el *Financial Stability Board* y, especialmente, el *Committee on Payments and Market Infrastructures del Bank for International Settlements* (BIS), fue fundamental para el desarrollo del Pix. Estos espacios permitieron comprender la urgencia de promover un sistema de pagos instantáneos y seguir los desafíos y oportunidades de la digitalización de los medios de pago. Estos foros de cooperación fomentaron el intercambio de conocimiento entre reguladores y ayudaron a definir el rol de los bancos centrales ante las transformaciones tecnológicas en el sector financiero, con especial atención a la necesidad de prevenir la concentración del mercado en manos de unos pocos actores privados.

El modelo adoptado en India el – Unified Payments Interface (UPI), lanzado en 2016 – consolidó diferentes servicios en una única plataforma interoperable, permitiendo transferencias instantáneas a bajo costo a través de aplicaciones bancarias y no bancarias. Esta infraestructura pública se presentó como un impulsor de la inclusión financiera en India (CORNELLI et al., 2024). Integró a millones de personas al sistema de pagos digitales y redujo la dependencia del efectivo⁹. Como señalan Schapiro, Mouallem y Dantas (2023), basándose en una evaluación de los resultados obtenidos en India —como la rápida adhesión por parte de la población, el impacto en la competencia y la transformación del comercio minorista digital—, el BCB identificó elementos clave que se replicarían y adaptarían en la creación del Pix. El modelo chino, basado en aplicaciones privadas como *WeChat* y *Alipay*, sirvió como advertencia sobre los riesgos de fragmentación y falta de interoperabilidad. El control del ecosistema por parte de grandes plataformas destacó la posibilidad de una pérdida de soberanía regulatoria. Por lo tanto, el Banco Central de Brasil centró sus esfuerzos en crear una infraestructura pública interoperable, inclusiva y controlada por el Estado (Schapiro; Mouallem; Dantas, 2023). Esto evitó la dependencia de las *Big Techs*, garantizó una regulación y supervisión unificadas y, en consecuencia, preservó la soberanía regulatoria nacional.

9. Estudios centrados en la digitalización de pagos en India destacan el impacto de la desmonetización implementada por el gobierno de Modi en noviembre de 2016. Esta medida eliminó el 86,4% del efectivo de la circulación, afectando gravemente a las poblaciones vulnerables. Datos del Reserve Bank of India indican que, entre 2014 y 2020, las retiradas de efectivo en cajeros automáticos disminuyeron significativamente, mientras que las transacciones a través de terminales de pago y mobile banking aumentaron significativamente. El sistema UPI se ha consolidado como un instrumento de inclusión financiera y formalización económica, aunque sus resultados sociales siguen siendo controvertidos (Fouillet; Guérin; Servet, 2021).

Así, el 16 de noviembre de 2020, el Banco Central brasileño concretó los esfuerzos de un largo período de trabajo con el lanzamiento de su propio sistema de pagos digitales. A través del canal oficial de *YouTube* de la agencia, representantes del BCB presentaron oficialmente el Pix, el sistema de pagos instantáneos. El *hashtag* #Agoraépix (#Ahoraespix) anunció “una nueva forma de recibir, pagar y transferir”. Los comentarios de las personas que seguían la *transmisión en vivo* de divulgación expresaban diferentes expectativas sobre el uso del nuevo medio de pago.



10. Disponible en: <<https://www.youtube.com/watch?v=0Xkv-e46hJQ>> Consultado el: 23 de octubre de 2024.

En aquel momento, el BCB exploró la naturaleza innovadora de la herramienta, señalando un «lanzamiento revolucionario» capaz de cambiar la vida de los brasileños. El entonces presidente de la agencia, Roberto Campos Neto, inauguró la transmisión en vivo destacando la transformación tecnológica que estaba experimentando el sector financiero. Explicó tales transformaciones haciendo referencia a un proceso compuesto por “6 Ds”: **digitalización, desmonetización, desintermediación, desmaterialización, disrupción y**, por último, **democratización**. Presentó el Pix, clasificándolo con una serie de adjetivos, destacando la llegada de **un método de pago más económico, rápido, seguro, transparente y accesible** (Banco Central de Brasil, 2020).

Tras su lanzamiento, en su primer día de operaciones, Pix registró más de un millón de transacciones y movilizó R\$777,3 millones (aproximadamente US\$145 millones en ese momento¹¹). En su primer mes de uso, Pix superó las transacciones mediante DOC¹² y, en el segundo mes, las transacciones mediante TED¹³. Cinco meses después, en abril de 2021, el Pix superó al DOC, TED y boletos bancarios combinados¹⁴, sin dejar dudas sobre la aceptación masiva del nuevo medio de pago. Las transacciones Pix han superado las transacciones electrónicas y los comprobantes de pago, que presentaban importantes limitaciones: restricciones de tiempo, retrasos en la disponibilidad de fondos, la necesidad de introducir códigos de barras o conocer los datos de varios destinatarios (banco, sucursal, cuenta, CPF/CNPJ). Además, estos métodos tradicionales solían implicar costes.

El marco regulatorio que estableció oficialmente Pix fue la [Resolución del BCB n.º 1/2020](#), publicada el 12 de agosto de 2020, antes de su lanzamiento público. Esta regulación sentó las bases del sistema de pagos y las reglas de participación en el ecosistema, permitiendo la participación de diversas instituciones financieras y de pago, garantizando una amplia cobertura desde su lanzamiento.

11. Para convertir valores a las tasas actuales, consulte: <https://www.bcb.gov.br/conversao>.

12. El DOC – Documento de Orden de Crédito – realizaba transferencias bancarias entre cuentas, limitadas a montos de hasta R\$ 4.999,99 y con un plazo de hasta un día hábil para la disponibilidad del dinero.

13. El TED – Transferencia Electrónica Disponible – realiza transferencias bancarias entre diferentes bancos y otras instituciones (financieras o de pagos) que poseen cuenta en el Banco Central. No hay límite en el monto de las transferencias TED. Cuando las transferencias involucran a clientes, el tiempo de envío lo determinan las instituciones, respetando el plazo máximo de procesamiento establecido por el Banco Central (17:00 h en días hábiles).

14. BANCO CENTRAL DO BRASIL. **Pix hoje e agenda evolutiva**. Brasília, DF: 7 de junho de 2021. Disponible en: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/JM_8.6.pdf Consultado el: 15 de noviembre de 2024.

La participación en el Pix se instituyó como obligatoria para las instituciones financieras y de pago autorizadas por el BCB y con más de quinientas mil cuentas de clientes activas (considerando cuentas de depósito a la vista, de ahorro y de pago prepago). Para otras instituciones financieras y de pago, la participación es opcional¹⁵. Posteriormente, la Resolución del BCB n.º 506, del 26 de septiembre de 2025, determinó que las instituciones financieras y de pago deben solicitar autorización para operar al BCB como condición para participar en Pix.

La Resolución del BCB n.º 1/2020 también establece las normas técnicas para los componentes esenciales de la infraestructura, como el [Sistema de Pagos Instantáneos](#) (SPI) para la liquidación y el [Directorio de Identificadores de Cuentas Transaccionales](#) (DICT) para la gestión de las Claves Pix. Asimismo, define los requisitos mínimos de seguridad y gestión de riesgos que las instituciones participantes deben cumplir para proteger a los usuarios¹⁶.

En cuanto a los consumidores, la Resolución BCB N.º 19, del 1 de octubre de 2020, definió la política de comisiones, enumerando las ocasiones en que se pueden aplicar cargos¹⁷ y especificando las situaciones en las que el envío y la recepción de fondos por parte de particulares es gratuito, un factor decisivo en la rápida adopción de este nuevo método de pago.

El hecho de que el Pix entró en vigor durante la pandemia de Covid-19 también puede mencionarse como otro aspecto relevante para su adhesión. Debido a las medidas de distanciamiento social y al cierre de algunos negocios, hubo un aumento de las compras *en línea* y una preferencia por los métodos de pago digitales (Lima e Francisco, 2021). En este sentido, Pix facilitó pagos rápidos sin necesidad de contacto físico. Cuatro años después de su lanzamiento, el número de transacciones demuestra la excelente adaptación del Pix a la vida cotidiana. Además de las ventajas ya descritas, las transacciones del Pix también han reducido los costos en comparación con otros métodos de transferencia y pago existentes¹⁸.

15. BANCO CENTRAL DO BRASIL. Participantes. Brasília, DF, s.d. Disponible en: <<https://www.bcb.gov.br/estabilidadefinanceira/participantespix>>. Consultado el: 2 de noviembre de 2025.

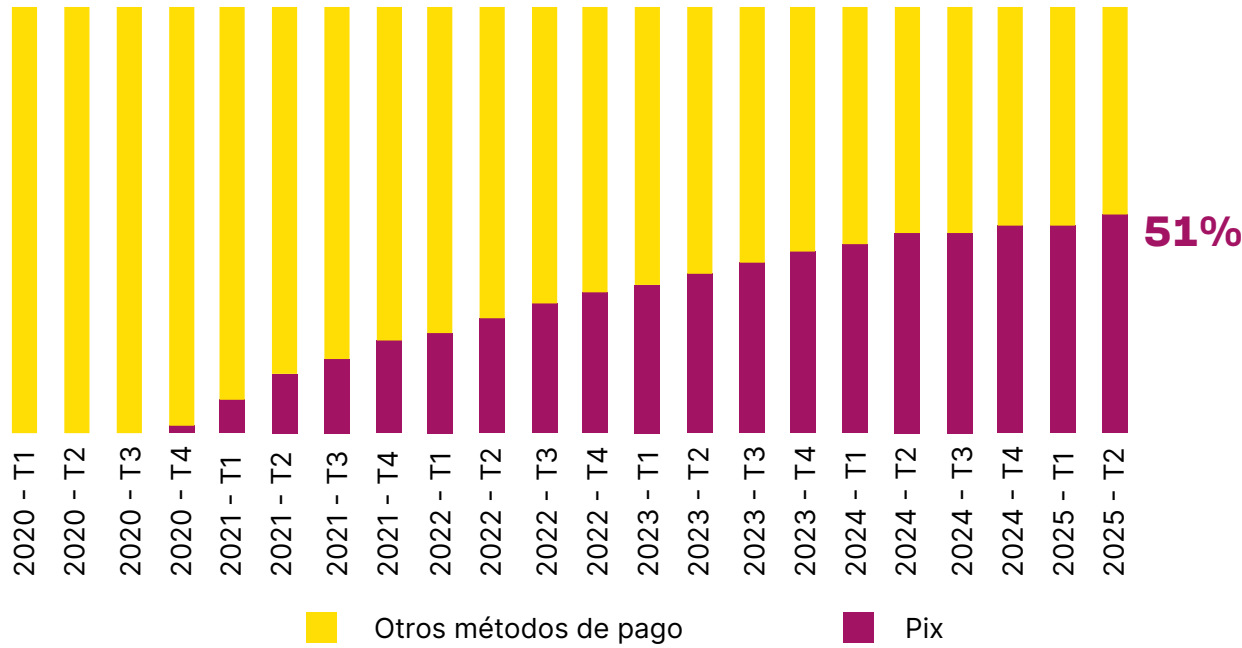
16. Para obtener más información sobre el SPI y el DICT, visite el sitio web del BC. Disponible en: <<https://www.bcb.gov.br/estabilidadefinanceira/sistemapagamentosinstantaneos?ano=2025>> e <<https://www.bcb.gov.br/estabilidadefinanceira/dict>>. Consultado el: 2 de octubre de 2025.

17. BANCO CENTRAL DO BRASIL. PIX - Quanto o cidadão (pessoa física) paga para usar o Pix. Brasília, DF: Banco Central, 12 dez. 2024. Disponible en: <https://www.bcb.gov.br/meubc/faqs/p/quanto-o-cidadao-paga-para-usar-o-pix>. Consultado el: 2 de octubre de 2025.

18. Para más información, consulte la página 5 del Informe de Gestión del Pix. Disponible en: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/relatorio_de_gestao_pix/relatorio_gestao_pix_2023.pdf. Consultado el: 2 de octubre de 2025.

Actualmente, Pix es el principal instrumento de pago para los brasileños (véase la Figura 4). Hay más de 800 millones de claves activas (considerando que cada persona física o jurídica puede tener más de una clave), y el número de usuarios registrados ya supera los 170 millones (incluyendo personas físicas y jurídicas)¹⁹.

Figura 4. Transacciones realizadas en Brasil, por método de pago



Fuente: Adaptado de Banco Central de Brasil, 2024.

19. BANCO CENTRAL DO BRASIL. **Estatísticas do Pix: Estatísticas de Chaves Pix.** Brasília, DF: Banco Central do Brasil, [2025]. Disponible en: <https://www.bcb.gov.br/estabilidade financeira/estatisticaspix>. Consultado el: 2 de octubre de 2025.

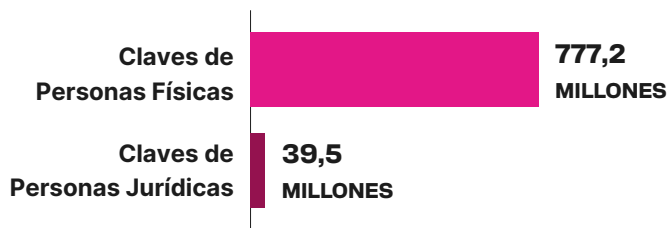
Los números del Pix

El BCB publica las estadísticas del Pix²⁰, en su sitio web, actualizadas mensualmente.

➔ NÚMERO DE CLAVES REGISTRADAS:

Stock de claves Pix activas al último día del mes, por tipo de usuario

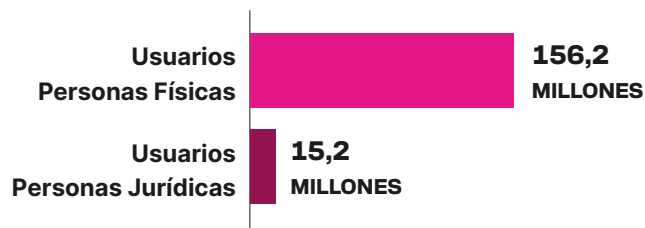
816 millones de claves en (Dic/2024), siendo:



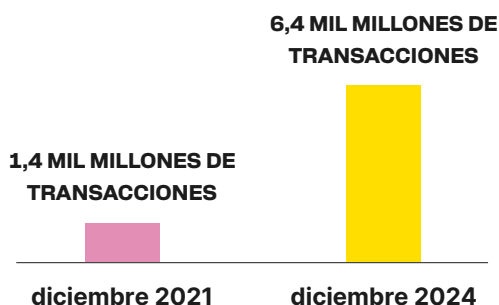
➔ NÚMERO DE USUARIOS REGISTRADOS:

Stock de usuarios registrados en el DICT al último día del mes, por tipo de usuario

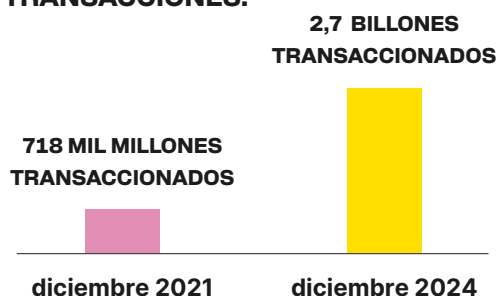
171.5 millones de usuarios en Dic/2024.



➔ CANTIDAD DE TRANSACCIONES :



➔ VOLUMEN FINANCIERO DE LAS TRANSACCIONES:



VALOR PROMEDIO DE LAS TRANSACCIONES (INDIVIDUALES):

En diciembre de 2022, el valor promedio de las transacciones Pix entre personas físicas fue de R\$257²¹. Cabe destacar que el 93,1% de estas transacciones fueron por montos inferiores a R\$200.

El estudio publicado por FGV, Geografia do Pix (Trevisan et al, 2025), actualizó esta cifra, añadiendo las diferencias por región en Brasil (Figura 5)²². Como se muestra, el valor promedio de las transacciones del Pix en 2024 fue de R\$190,57.

20. BANCO CENTRAL DO BRASIL. Estatísticas do Pix: Estatísticas de Chaves Pix. Brasília, DF: Banco Central do Brasil, [2025]. Disponible en: <https://www.bcb.gov.br/estabilidade financeira/estatisticaspix>. Consultado el: 2 de octubre de 2025.

21. BANCO CENTRAL DO BRASIL. Relatório de Gestão do Pix. Concepção e primeiros anos de funcionamento 2020-2022. Brasília, DF: 2023. Disponible en: https://www.bcb.gov.br/content/estabilidade financeira/pix/relatorio_de_gestao_pix/relatorio_gestao_pix_2023.pdf. Consultado el: 2 de octubre de 2025.

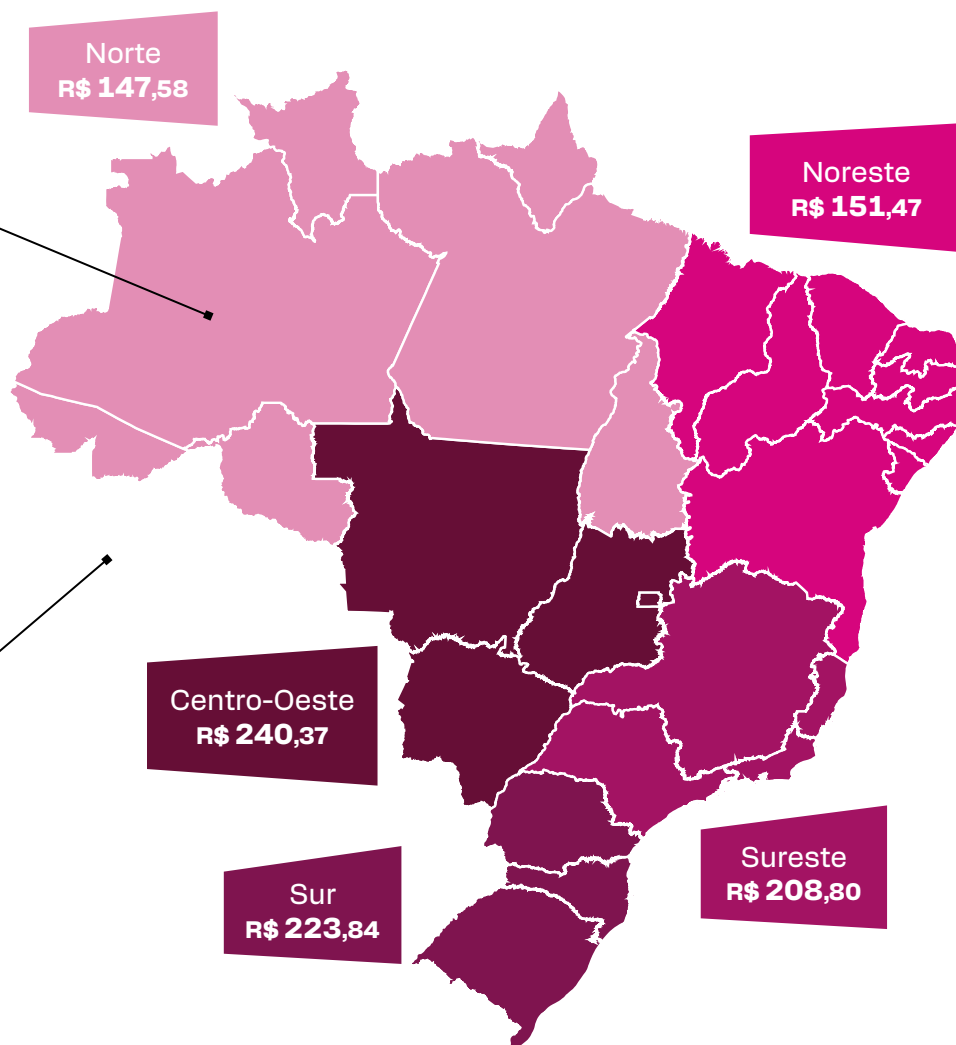
22. TREVISAN, F.; GONZALEZ, L.; DINIZ, E.; E CERNEV, A. Geografia do Pix: Como o Sistema de Pagamentos Instantâneos Redesenha o Mapa Financeiro do Brasil. FGV, 2025. Disponible en: <https://eaesp.fgv.br/producao-intelectual/geografia-pix-como-sistema-pagamentos-instantaneos-redesenha-mapa-financeiro>. Consultado el: October 16, 2025.

Figura 5. Valor promedio de las transacciones por región en Brasil.

Amazonas ilustra la diferencia entre acceso y uso. Este estado tiene el mayor número de transacciones por usuario en el país y, al mismo tiempo, el valor promedio de las transacciones más bajo (R\$120,53). Esto sugiere que el uso está **incorporado en los hábitos diarios, con transacciones frecuentes y de bajo valor**

PROMEDIO NACIONAL

El **valor promedio de las transacciones** del Pix en 2024 fue de **R\$190,57**



Los estados de las regiones **Norte y Noreste** registran valores promedio de transacciones **más bajos** en comparación con las regiones **Sur, Sureste y Centro-Oeste**. Esta diferencia puede reflejar desigualdades regionales: **los usuarios en áreas de mayores ingresos tienden a realizar transacciones de mayor valor**

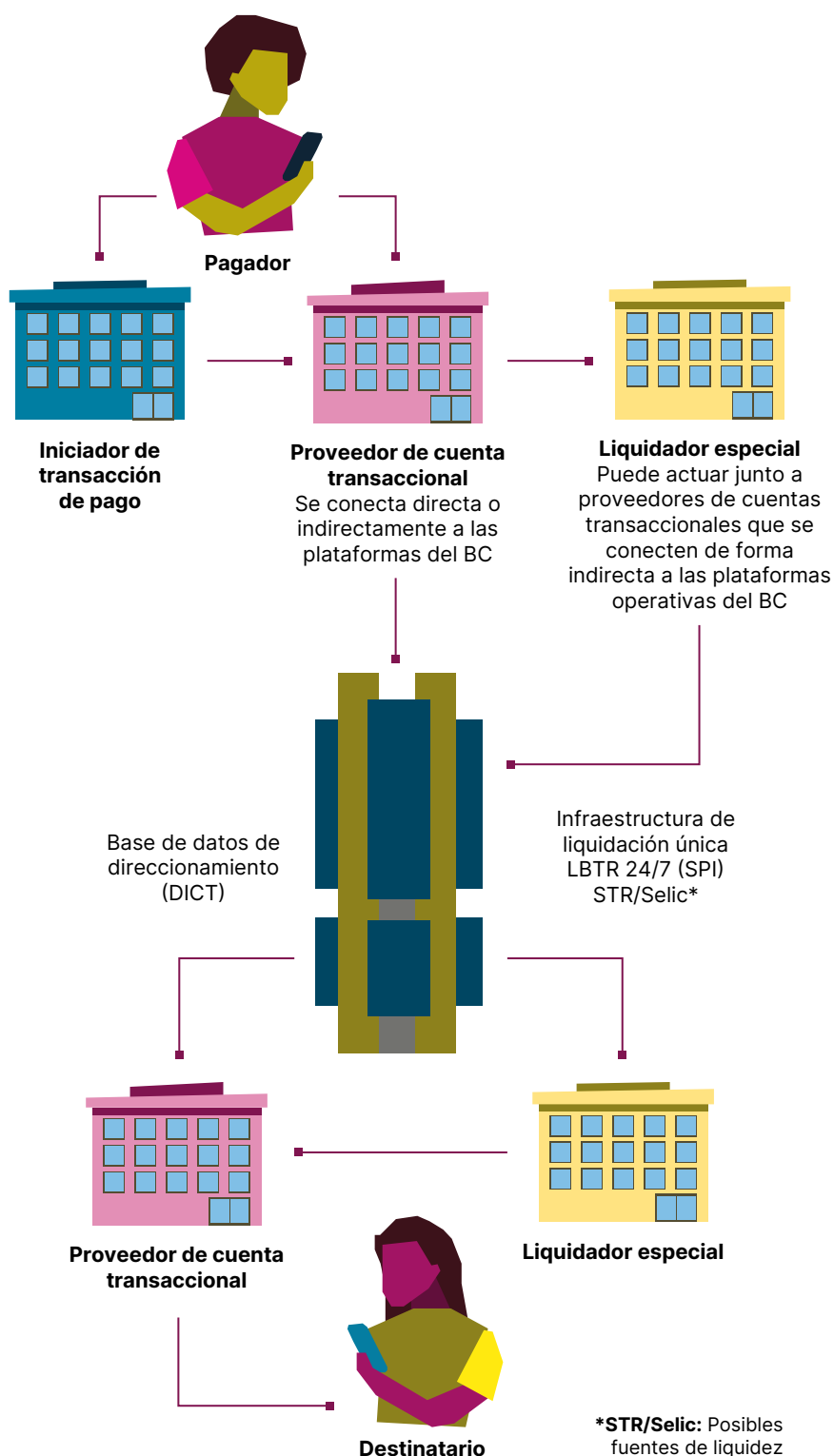
Fuente: Adaptado de Trevisan et al., 2025.

Los roles del Banco Central de Brasil (BCB)

El BCB desempeña un papel central en el diseño, operación y supervisión del Pix. Al actuar como la **institución responsable del sistema de pagos**, la agencia establece el conjunto de regulaciones que rigen el funcionamiento del sistema. Este papel incluye definir las reglas de participación para las instituciones financieras y de pago, los procedimientos operativos para realizar transacciones, los estándares de seguridad y los mecanismos de resolución de disputas. A través de circulares, resoluciones y otros instrumentos regulatorios, el BCB da forma al marco legal que rige el ecosistema Pix.

Además de su función reguladora, el BCB actúa como desarrollador, administrador y operador de la infraestructura tecnológica esencial para el funcionamiento del Pix. El Sistema de Pago Instantáneo (SPI) consiste en una infraestructura centralizada de liquidación bruta en tiempo real que garantiza el procesamiento y la liquidación de las transacciones. El Directorio de Identificadores de Cuentas Transaccionales (DICT) es una base de datos encargada de almacenar la información de registro de los usuarios receptores y sus respectivas cuentas transaccionales. Al gestionar las claves del Pix, el DICT simplifica el proceso de iniciación de pagos, eliminando la necesidad de compartir datos bancarios tradicionales (Figura 6).

Figura 6. Rol del Banco Central de Brasil (BCB)



Fuente: Banco Central de Brasil, s.f.

Referencias²³

Proveedor de cuenta transaccional

Una institución financiera o institución de pago que ofrece una cuenta de depósito o cuenta de pago prepago a usuarios finales, incluyendo instituciones de pago no sujetas a autorización para operar por el Banco Central de Brasil.

Liquidador especial

Una institución financiera o institución de pago autorizada para operar por el Banco Central de Brasil que, dentro del alcance del Pix, tiene el propósito exclusivo de proporcionar servicios de liquidación a otros participantes, no ofreciendo el envío o recepción del Pix a usuarios finales; que cumple con los requisitos para actuar como participante de liquidación en el SPI; y que no cumple con los criterios de participación obligatoria en Pix.

Iniciador de transacción de pago

Una institución de pago que proporcionará servicios de iniciación de transacciones de pago sin administrar una cuenta de pago y sin retener, en ningún momento, los fondos transferidos en la prestación del servicio (la prestación de este servicio aún requiere regulación por parte del BC).

BC

Responsable de desarrollar y gestionar la base única y centralizada de direccionamiento (DICT) y la infraestructura única y centralizada de liquidación de las transacciones (SPI), que funcionará las 24 horas del día, todos los días del año.

23. BANCO CENTRAL DO BRASIL. **Papel do BC.** Brasília, DF: s.d. Disponible en: <<https://www.bcb.gov.br/estabilidade financeira/papel do bcb pix>>. Consultado el: 10 de noviembre de 2024.

Cabe destacar que, si bien el BCB tiene la prerrogativa de establecer y operar Pix, el proceso de desarrollo y mejora continua del sistema depende de la participación de otras partes interesadas a través del Foro Pix. Este espacio colaborativo reúne a instituciones financieras, *fintechs*, empresas tecnológicas y otras *stakeholders*, quienes pueden presentar propuestas relacionadas con nuevos servicios, funcionalidades y ajustes al sistema.

Desde mayo de 2024, Idec es miembro del **Foro Pix**, representando a los usuarios finales de servicios de pago. En el momento de su inclusión, Idec era el único representante de los consumidores en este espacio de gobernanza.

Las discusiones y debates dentro del Foro se realizan a través de grupos de trabajo específicos, que en ocasiones cuentan con la Federación Brasileña de Bancos (Febraban) como institución centralizadora y responsable de la secretaría, como en el caso del Grupo de Seguridad Estratégica del Pix (GE-Seg). Sin embargo, todos los participantes reconocen que la decisión final sobre el desarrollo e implementación de nuevas reglas y funcionalidades en el Pix recae en el Banco Central de Brasil.

El Foro Pix

El Foro Pix, compuesto por más de 200 instituciones participantes, fue diseñado para promover un **entorno de cocreación** centrado en el desarrollo y la mejora del sistema de pagos instantáneos²⁴. Meses antes del lanzamiento público del Pix, el Banco Central estableció el Foro mediante la [Ordenanza](#)

24. Las explicaciones sobre la constitución y funcionamiento del Foro Pix se pueden encontrar en: <https://www.youtube.com/watch?v=Fd7k37rE41w&list=PLvZdUvzf-GwBpskryQyG56sy5jG2ZXuf8V&index=11>.

N.º 102,166 del 19 de marzo de 2019²⁵. Sirve como un **órgano consultivo permanente** y permite que los cambios en las regulaciones o la creación de nuevos productos y servicios pasen por una fase de consulta con sus miembros, durante la cual los miembros del grupo de trabajo tienen la oportunidad de analizar las propuestas y ofrecer sus contribuciones. Actualmente, cuatro grupos de trabajo (GT) están en funcionamiento:

- ➔ **GT de Negocios:** Responsable de brindar información relacionada con la definición de productos y servicios del ecosistema Pix, mapeando sus flujos y funcionalidades.
- ➔ **GT de Estandarización y Requisitos Técnicos:** Responsable de discutir los aspectos tecnológicos del sistema, como estándares de comunicación, requisitos de seguridad, conectividad, base de datos de direcciones y estándar de *QR Code*.
- ➔ **GT de Mensajes PI:** Dedicado a definir mensajes en el estándar ISO 20022 utilizado en la comunicación con la infraestructura de liquidación única y centralizada de Bacen.
- ➔ **GE Seguridad:** Responsable de proponer soluciones para hacer que el sistema Pix sea más resistente a fraudes y garantizar la privacidad de los datos de los usuarios.

Los miembros del Foro Pix, según la Ordenanza n.º 102.166 del 19 de marzo de 2019, incluían representantes de: (1) asociaciones que representan a proveedores de servicios de pago; (2) proveedores de servicios de conectividad; (3) proveedores de servicios de iniciación de pagos; (4) asociaciones que representan a usuarios finales de servicios de pago, tanto pagadores como receptores; y (5) el Banco Central de Brasil. Además de estos participantes, se podrá invitar a otros organismos y entidades, como reguladores de servicios de pago, agencias de competencia y protección al consumidor, y entidades públicas o privadas que puedan contribuir a los debates.

El objetivo principal del Foro es apoyar al BCB en la definición de las normas y directrices que rigen el funcionamiento del ecosistema de pagos instantáneos. Mediante debates en sesiones plenarias y grupos de trabajo, se estableció una dinámica que busca promover la participación de los diversos actores involucrados. Sin embargo, como se mencionó, la decisión final sobre la implementación de mejoras o nuevas funcionalidades recae en el Banco Central.

25. Consultado en: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/67765121/do2-2019-03-20-portaria-n-102-166-de-19-de-marco-de-2019-67764964. Disponible el: 5 de enero de 2025.

Otra característica del Foro es el intercambio de materiales de la reunión plenaria a través del sitio web del Banco Central. En la página del **Foro Pix**, puede descargar las regulaciones del Pix, acceder a las fechas de las reuniones plenarias y a los documentos presentados por el BC y los grupos de trabajo.

Además de las discusiones del Foro Pix, el Banco Central estableció un mecanismo de consulta pública²⁶. Esta iniciativa se utilizó en la implementación de dos nuevas funcionalidades vinculadas al Pix: Pix Retiro y Pix Cambio. En ese momento, a través del **Sistema de Consulta Pública y otras formas de participación social**, alojadas en el sitio web del Banco Central, cualquier persona podía acceder al aviso de consulta pública y dejar comentarios o sugerencias a través del formulario.

Aunque no sea un instrumento utilizado con frecuencia, la consulta pública es un importante canal de participación social. Reconocerlo como un espacio relevante para la expresión pública es fundamental para que más miembros de la sociedad se sientan invitados a expresar sus opiniones y contribuir a la formulación de políticas públicas y decisiones que afectan el funcionamiento del Sistema Financiero Nacional.

La experiencia del **idec** en el Foro Pix

Durante la participación de Idec en el Foro Pix, fue posible seguir de cerca las consultas del Banco Central con los miembros del grupo de trabajo, así como los debates sobre la agenda evolutiva del Pix. A medida que se familiarizaba con los procedimientos de desarrollo de propuestas y la dinámica de participación de las partes interesadas, se hizo evidente la importancia de contar con más instituciones

que representen a los usuarios, tanto agencias de protección de los derechos del consumidor como agencias de defensa de los derechos digitales. Incorporar las preocupaciones de estas instituciones en los debates puede ayudar a la ciudadanía a tener mayor voz en este espacio de gobernanza y, en consecuencia, a contar con soluciones más inclusivas y menos influenciadas por empresas privadas.

Es importante enfatizar que, aunque la resolución del Foro Pix prevé pluralidad de instituciones y amplia participación de los agentes, no existen procedimientos claros de selección o nombramiento de miembros, ni una lista pública actualizada de los participantes. Además, las contribuciones al Foro no se publican ni son respondidas sistemáticamente por el Banco Central, lo

26. Más información está disponible en: <<https://www3.bcb.gov.br/audpub/AudienciasAtivas?1>>. Consultado el: 5 de julio de 2025.

que restringe el acceso público a los debates y decisiones que configuran la evolución del sistema.

Otro punto crítico se refiere a la influencia que ciertos actores pueden ejercer en la dinámica del Foro. La Febraban, por ejemplo, es la institución responsable de la secretaría del grupo de trabajo de seguridad, y no parece haber rotación en la gestión. Este modelo, a largo plazo, podría cuestionar la imparcialidad y legitimidad del proceso de toma de decisiones, dado el peso del sector bancario tradicional en comparación con los demás miembros del Foro.

Para superar estos desafíos, Idec recomienda medidas que fortalezcan la legitimidad del Foro Pix y lo conviertan en un referente internacional en la gobernanza de la infraestructura pública digital. Estas incluyen: **1) Directrices claras para la participación de los diferentes stakeholders**, con procesos de selección transparentes y mandatos definidos; **2) Procesos para recopilar inputs e incorporar contribuciones**, considerando mecanismos para recopilar, publicar y responder a las contribuciones externas; **3) Iniciativas de capacitación de los actores**: capacitación que amplía y mejora el conocimiento del sistema, permitiendo la participación significativa de todos los actores, incluidos los consumidores. Estas medidas son esenciales para garantizar que el Pix siga siendo eficiente, inclusivo, seguro e innovador, a la vez que se mantiene alineado con las mejores prácticas para el desarrollo de la infraestructura pública digital.

Innovaciones o “Agenda Evolutiva del Pix”

Se pensaron diferentes innovaciones para el perfeccionamiento del Pix. El objetivo del BCB, como se indica en el informe de gestión, es permitir que todos los pagos y transferencias realizadas en Brasil, independientemente del monto, el propósito o los agentes involucrados, también se realicen a través del Pix²⁷. El documento se refiere al conjunto de productos, iniciativas y soluciones como la “Agenda Evolutiva del Pix”.

A continuación, algunos ejemplos de funcionalidades lanzadas y otras previstas:

27. BANCO CENTRAL DO BRASIL. Relatório de Gestão do Pix. Concepção e primeiros anos de funcionamento 2020-2022. Brasília, DF: 2023. Disponible en: <https://www.bcb.gov.br/content/estabilidade financeira/pix/relatorio_de_gestao_pix/relatorio_gestao_pix_2023.pdf>. Consultado el: 2 de octubre de 2025.



PIX RETIRO

Vigencia: noviembre de 2021

Esta función elimina la necesidad de tarjetas de débito o crédito para realizar retiros. Permite la retirada de dinero en efectivo en establecimientos comerciales que ofrezcan esta opción.



PIX CAMBIO

Vigencia: noviembre de 2021

En la compra de un producto o servicio, prevé la oferta de cambio en efectivo en establecimientos que ofrezcan esta función.



PIX A PLAZOS

Vigencia: previsto para finales de 2025

Permite pagos a plazos, incluso si el cliente no tiene saldo en cuenta corriente al momento de la transacción. La entidad financiera ofrece crédito al cliente, asegurando que el importe total se transfiera inmediatamente al vendedor. El consumidor paga el importe en plazos, con intereses que se cobran según las condiciones definidas por el banco.



PIX PROGRAMADO

Vigencia: Octubre 2024

Permite al usuario programar un pago único para una fecha futura. En lugar de transferir el dinero instantáneamente, el usuario define el importe, el destinatario y el día en que debe completarse la transacción.



PIX PROGRAMADO RECURRENTE

Vigencia: Octubre 2024

Permite programar pagos regulares del mismo importe para que se transfieran a la cuenta del destinatario el mismo día de cada mes.



PIX AUTOMÁTICO

Vigencia: Junio 2025

Permite, con autorización previa, que los pagos recurrentes (como facturas de electricidad, agua, teléfono o servicios de suscripción) se automaticen de forma recurrente. En esta modalidad, la empresa (persona jurídica) define los importes (fijos o variables) y las fechas de pago.



PIX POR APROXIMACIÓN

Vigencia: febrero de 2025

A través de la tecnología NFC, permite el pago sin contacto, por aproximación. Simplemente registre el Pix en su billetera digital y acerque su teléfono al terminal. La información de pago aparecerá en la pantalla del teléfono, a la espera de autorización.



PIX EN GARANTÍA

Fecha prevista: 2026-2027

Dirigido a establecimientos comerciales, permite que flujos futuros de cobranzas vía Pix se utilicen como garantía en operaciones de crédito.



PIX OFFLINE

Sin fecha de lanzamiento prevista

Esta función busca habilitar pagos sin conexión a internet. Se espera que los clientes bancarios puedan realizar transacciones acercando su teléfono celular a la terminal de pago, incluso si el dispositivo no tiene conexión. Esto permitirá la inclusión de nuevos públicos y regiones con acceso limitado a internet.



PIX INTERNACIONAL

Sin fecha de lanzamiento prevista

Esta función permite pagos y transferencias internacionales.



Visión del Idec:

Considerando el papel central que el Pix ha asumido en la economía del país, permeando la vida cotidiana de millones de personas y empresas en todo el país, es esencial que cualquier cambio en su funcionamiento o normativa se introduzca con extrema precaución.

Cualquier cambio en la forma de uso o en la normativa vigente debe ser precedido de un debate sobre la implementación de las funcionalidades, sus desafíos, riesgos y beneficios.

A continuación, es necesario considerar una estrategia de comunicación que se caracterice no solo por su claridad y precisión, sino también por su continuidad en el tiempo. Dado el alcance del Pix -desde grandes centros urbanos hasta las zonas más remotas-y la variedad de sus usuarios (con distintos niveles de habilidades tecnológicas), es esencial que los cambios planificados solo se implementen eficazmente tras un período significativo dedicado a su difusión, utilizando múltiples canales e idiomas adecuados para cada público.

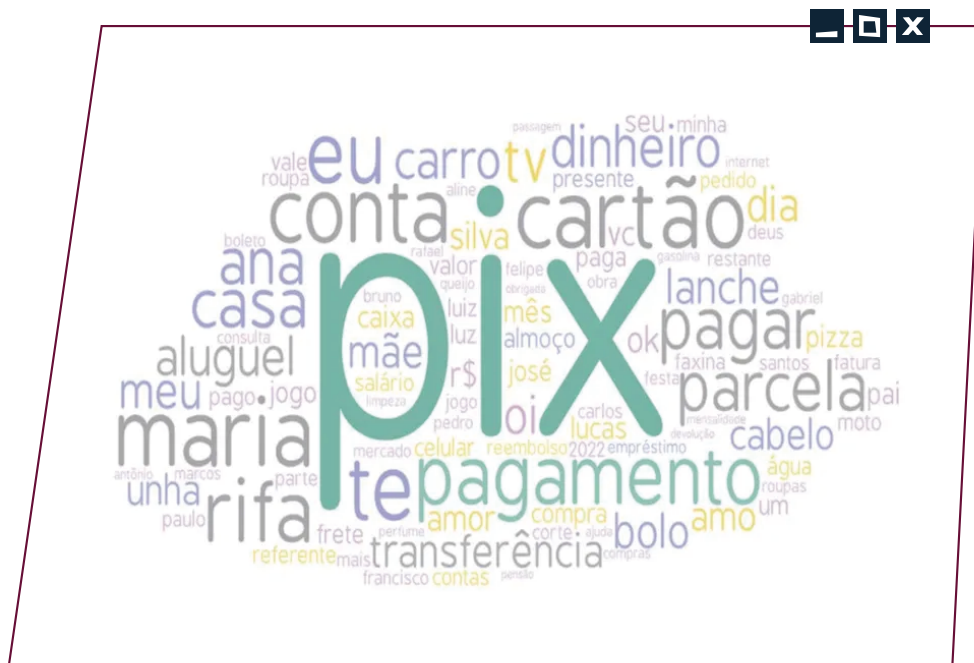
Garantizar este tiempo para la difusión y comprensión de la información es importante para fomentar la comprensión colectiva, así como para prevenir lagunas que podrían ser cubiertas por desinformación. La incertidumbre generada por la novedad es peligrosa y puede causar inseguridad y resistencia al cambio. Además, la desinformación puede servir como detonante para la actividad delictiva de quienes aprovechan la confusión para difundir rumores, realizar estafas de ingeniería social o crear páginas y comunicaciones falsas, aprovechando la falta de claridad de las instituciones oficiales.

Usos no previstos del Pix: ¿Medio de pago o medio de comunicación?

Todas las transferencias y pagos realizados a través del Pix permiten al pagador enviar un breve mensaje al destinatario, generalmente una descripción de la transacción.

En 2022, una encuesta realizada por el BCB (2023) identificó que las palabras más utilizadas por los usuarios se referían al pago de obligaciones (facturas, tarjeta, boleto, alquiler, pago a plazos, pago, casa, etc.), ciertos tipos de bienes (pastel, auto, ropa, regalo, perfume, TV, etc.) y servicios (peluquería, uñas, refrigerio, almuerzo, dentista, limpieza, envío, etc.).

Figura 7. Las 100 palabras más utilizadas en la descripción de un Pix



Fuente: BCB, 2023, p.24.

Sin embargo, este espacio descriptivo dio lugar a usos inusuales del Pix. Entre los usuarios, se identificó la práctica de enviar una pequeña cantidad, generalmente un céntimo, para escribir un mensaje de hasta 140 caracteres al destinatario. En 2023, se enviaron más de 35 millones de mensajes en este formato, un aumento del 43 % con respecto al año anterior²⁸.

El pago de un centavo del Pix puede usarse para verificar la información del destinatario y servir como método de prueba. Sin embargo, este medio de pago también se ha utilizado como medio de comunicación, sirviendo como una forma alternativa de contactar. Los mensajes mapeados abarcan desde propuestas de matrimonio hasta disculpas, bromas entre amigos, solicitudes de préstamos o mensajes a equipos de fútbol: la creatividad de los usuarios es inmensa²⁹.

Sin embargo, esta práctica también tiene efectos negativos. Individuos bloqueados de las redes sociales, o incluso cumpliendo determinaciones judiciales de distanciamiento, encontraron en el campo de mensajes del Pix una forma de acceder a personas con las que ya no mantienen contacto. Se han identificado casos de acoso, hostigamiento, amenazas o persecuciones a exparejas y están siendo investigados³⁰.

Las empresas también adoptaron este formato de comunicación. En noviembre de 2024, durante el Black Friday, la cadena Burger King envió Pix a sus clientes y utilizó el campo de descripción de la transferencia bancaria para comunicar su promoción. Se realizaron más de 19 millones de transferencias Pix ese mismo día³¹.

Enviar dinero para llegar directamente a los consumidores a través de un canal de comunicación inesperado generó likes y sorpresa, pero la estrategia de *marketing* también apunta a problemas de seguridad y abuso publicitario. ¿Sería admisible utilizar la información bancaria de los clientes con fines publicitarios?

28. Según datos publicados en: <<https://g1.globo.com/jornal-nacional/noticia/2024/03/16/mais-de-35-milhoes-de-transferencias-por-pix-no-valor-de-um-centavo-foram-realizadas-em-2023.ghtml>>. Consultado el: 3 de mayo de 2024.

29. Se pueden encontrar ejemplos del uso del Pix como medio de comunicación en diversos artículos periodísticos. Disponible en: <<https://www1.folha.uol.com.br/mercado/2024/03/pix-de-um-centavo-vira-meio-de-comunicacao-com-353-milhoes-de-operacoes-em-2023.shtml>>. Consultado el: 2 de diciembre de 2024.

30. Disponible en: <https://tribunaonline.com.br/brasil/pix-de-1-centavo-e-usado-para-ameacas-e-assedio-sexual-176553>. Consultado el: 2 de diciembre de 2024.

31. Disponible en: <<https://www.meioemensagem.com.br/comunicacao/burger-king-envia-pix-a-consumidores-para-divulgar-promocao-de-black-friday>>. 5 de febrero de 2025.



Preocupado por las repercusiones de la práctica de envío de mensajes con fines publicitarios, el Idec notificó al Ministerio de Justicia y al Banco Central para que investigaran la campaña “Pix de 1 centavo en Black Friday” de Burger King.

La campaña de marketing violó artículos del Código de Defensa del Consumidor (CDC) y la Ley General de Protección de Datos Personales (LGPD) al usar indebidamente y sin consentimiento los datos de los miembros registrados en su programa de fidelización. Burger King hizo un uso indebido de los datos personales de los consumidores para enviar mensajes promocionales masivos en un medio inesperado. Enviar R\$0,01 como mensaje promocional a través del Pix puede considerarse una práctica invasiva, ya que utiliza una herramienta bancaria diseñada para transacciones financieras para entregar mensajes publicitarios. Este enfoque viola las expectativas de privacidad de los consumidores, ya que no pueden imaginar ser el objetivo de comunicaciones comerciales a través de un sistema tan íntimo y sensible como su cuenta bancaria. En ese momento, también se envió una notificación al Banco Central de Brasil (BCB) para evitar prácticas similares en el futuro.

El mensaje del Idec fue claro: ¡Pix no es Spam!



PIX



Lentes de Análisis

Lente: Inclusión Digital



Historial

Los esfuerzos para ampliar el acceso a los servicios bancarios se remontan a finales de la década de 1990. **Antes de la década de 2000, la infraestructura financiera de Brasil estaba marcada por la desigualdad: solo 25 millones de brasileños tenían una cuenta bancaria (aproximadamente el 15% de la población) y casi el 30% de los municipios (aproximadamente 1680 de 5600) no contaban con sucursales bancarias.** La disparidad regional también fue bastante pronunciada: siete estados, particularmente en el norte del país, tenían más del 70% de sus municipios sin sucursales. Además, en las regiones Norte y Noreste, incluso cuando existían sucursales bancarias, los servicios ofrecidos eran limitados (IPEA, 2004)³².

La expansión de la red de servicio comenzó con la expansión de los cajeros automáticos (que crecieron de 3.500 a 22.500 entre 1994 y 2002), los corresponsales bancarios³³, las cooperativas de crédito y los puntos de servicio (IPEA, 2004)³⁴. El uso de sucursales de correos y establecimientos comerciales, incluidas las loterías, los supermercados y las farmacias, como corresponsales bancarios fue una estrategia decisiva para expandir el alcance de los servicios financieros, especialmente en áreas remotas o pequeñas

32. Durante este período, incluso en economías consideradas desarrolladas, la exclusión financiera también era un problema. Datos de 2003 del Federal Reserve indicaron que casi el 13% de los hogares estadounidenses carecían de cuenta corriente, y casi el 60% de este grupo pertenecía a minorías (no blancos/hispanos) y a personas de bajos ingresos. En el Reino Unido, se estima que el 8% de la población no tenía acceso a servicios bancarios en Inglaterra y Gales, y el 15% en Escocia. Para más información, consulte el informe “Brasil: acesso a serviços financeiros (Brasil: Acceso a Servicios Financiero)”, publicado por el IPEA en 2004.

33. Estas empresas, como las loterías o los bancos postales, son contratadas por bancos y otras instituciones autorizadas por el BCB para prestar servicios a sus clientes y usuarios.

34. Ubicados dentro de una organización pública o privada, como una empresa, agencia gubernamental o universidad, ofrecen servicios bancarios a empleados, clientes o al público en general de la organización donde se encuentran.

ciudades. Como resultado, para 2002, todos los municipios brasileños contaban con servicios bancarios³⁵. Esta red de corresponsales también desempeñó un papel importante en los programas gubernamentales de transferencia de ingresos, sirviendo como el principal canal de pago para Bolsa Família (BCB, 2010).

Además de una estructura física más amplia, la creación de cuentas especiales (como cuentas de nómina y cuentas de ahorro simplificadas) también desempeñó un papel relevante en la reducción de obstáculos burocráticos, impulsando a más personas a convertirse en usuarias de servicios bancarios. Las cuentas de depósitos especiales a la vista o de ahorro, usualmente conocidas como cuentas simplificadas, instituidas por la **Resolución nº 3.211**, de 30 de junio de 2004, fueron concebidas por el Banco Central de Brasil como una “puerta de acceso al sistema bancario”³⁶. Aunque se promovieron como estímulo al hábito de ahorrar, también buscaban facilitar el uso de productos financieros más sofisticados, en especial el crédito. Por un lado, estas cuentas tenían un límite máximo de saldo y restricciones en cuanto a las formas de movimiento y el número de retiros mensuales; por otro, ofrecían exención de comisiones y requerían, para su apertura, una documentación reducida en comparación con las cuentas corrientes tradicionales, factores que facilitaron el acceso de los consumidores de bajos ingresos.

Fue en 2010 que la política de inclusión financiera ganó impulso y se integró a los objetivos estratégicos de la agencia para el período 2010 a 2014. En este momento, la institución comenzó a establecer la meta de garantizar el acceso a servicios financieros como crédito, ahorro, pagos, seguros, pensiones e inversiones, enfatizando la importancia de adaptar los productos a las necesidades individuales³⁷. En el mismo año, también se lanzó la Estrategia Nacional de Educación Financiera (ENEF) como política estatal, con el objetivo de brindar orientación a las personas sobre los productos y servicios financieros

35. Para comprender el alcance de los corresponsales bancarios, vale la pena señalar que, en 2009, mientras que el número de sucursales era cercano a 20.000, el número de corresponsales bancarios era de alrededor de 150.000 a nivel nacional (Febraban, 2009; Jayo; 2010).

36. Disponible en: <<https://g1.globo.com/economia/seu-dinheiro/noticia/2014/11/limite-para-conta-simplificada-isenta-de-tarifas-sobe-para-r-3-mil-diz-bc.html>>. Consultado el: 5 de mayo de 2025.

37. BANCO CENTRAL DO BRASIL. **Relatório de Inclusão Financeira**, 2010.

disponibles, con el objetivo de que los ciudadanos sean más conscientes de los riesgos y las oportunidades asociadas con estos productos financieros³⁸.

El Sistema de Pagos Brasileño (SPB)

Las primeras décadas de la década de 2000 también fueron cruciales para el Sistema de Pagos Brasileño (SPB). La Ley nº 10.214/2001, de 27 de marzo de 2001, que establece las actividades de las cámaras de compensación y liquidación y de los proveedores de servicios en el sistema de pagos brasileño, marcó un hito para el país al establecer formalmente el SPB y crear un marco regulatorio esencial para las transformaciones vinculadas a los servicios de pago.

El SPB es la infraestructura que permite a empresas y particulares realizar sus transacciones bancarias diarias. Para facilitar su comprensión, es común comparar esta infraestructura de pagos con un sistema de tuberías: a través de este sistema básico y esencial circularía el dinero, manteniendo el flujo y la seguridad de las diversas transacciones financieras realizadas, ya sea mediante tarjetas, recibos de pago, cheques (o incluso Pix)³⁹.

Antes de 2001, no existía la funcionalidad de transferencia financiera en tiempo real. Las transacciones se procesaban mediante instrumentos como Documentos de Orden de Crédito (DOC), recibos bancarios y cheques, y la liquidación generalmente se realizaba al día siguiente. Este modelo presentaba fragilidades de seguridad, ya que la eventual insuficiencia de fondos para la realización de una operación solo podía verificarse al finalizar los procesos diarios. La no realización de una transacción por falta de recursos podía

38. Presentes en varios países, los programas de educación financiera se desarrollaron con mayor relevancia a partir de finales de la década de 1990 (Lazarus, 2016). La OCDE (Organización para la Cooperación y el Desarrollo Económicos) desempeñó un papel central en este ámbito, impulsando y apoyando dichos programas mediante la investigación, el debate y el intercambio de experiencias entre los países miembros y sus socios. Mediante la creación de la Red Internacional de Educación Financiera (INFE), la OCDE reunió a diversas instituciones gubernamentales que elaboraban regularmente estudios y evaluaciones, con el objetivo de crear un espacio de colaboración centrado en el análisis de los programas de educación o alfabetización financiera. La estrategia brasileña, denominada ENEF, se estableció en 2010 mediante el Decreto n.º 7.397 del 22 de diciembre (Fernandes, 2019).

39. Disponible en: <https://www.bcb.gov.br/detalhenoticia/751/noticia>. Consultado el: 14 de mayo de 2025. El sitio web del PSR del Reino Unido incluye un video explicativo sobre el sistema de pagos, que también utiliza imágenes de tuberías para explicar el sistema. Disponible en: <https://www.psr.org.uk/how-we-regulate/payment-systems-explained/>.

interpretarse como un indicio de inestabilidad, comprometiendo la confianza en el sistema financiero⁴⁰.

Con la creación del SPB, se definieron reglas claras para el funcionamiento de los principales sistemas de transferencia y liquidación de dinero, cheques, facturas y tarjetas. Además, en 2002, con la creación del Sistema de Transferencia de Reservas (STR), operado por el BCB, se comenzó a garantizar la liquidación en tiempo real de las transacciones interbancarias, reduciendo el riesgo crediticio y de liquidez en el sistema financiero.

En este nuevo escenario, centrado en la reducción de riesgos y el aumento de la eficiencia, la Transferencia Electrónica Disponible (TED) se destaca como una característica resultante de la creación del STR, cuyos beneficios llegan directamente a los consumidores. Con la nueva tecnología, se creó un canal seguro para transferir grandes cantidades: un servicio que permitía a personas y empresas enviar dinero entre diferentes bancos y recibirlo en sus cuentas el mismo día (en cuestión de minutos u horas, si se realizaba durante el horario bancario). Sin embargo, vale la pena recordar que, a pesar de los avances, el TED aún estaba sujeto a restricciones como horarios bancarios y, muchas veces, tarifas elevadas, que limitaban su uso por parte de los segmentos de menores ingresos de la población.

Posteriormente, en 2013, dada la evolución tecnológica de este período y un contexto de creciente digitalización, se hizo evidente la necesidad de modernizar el SPB. En este contexto, entró en vigor la Ley n.º 12.865/2013, del 9 de octubre de 2013, como marco regulatorio, estableciendo normas para que nuevas empresas, principalmente *fintechs*, pudieran ofrecer servicios de pago, como cuentas digitales, tarjetas prepago y terminales de tarjeta. Esta ley, además de definir con mayor precisión los actores que operan en el sistema y sus responsabilidades, también amplió la función reguladora del BCB, que comenzó a supervisar no solo a las instituciones financieras tradicionales, sino también a otras entidades, como los establecimientos comerciales que actuaban como entidades de pago minoristas (Schapiro; Mouallem; Dantas, 2023).

Desde la perspectiva del consumidor, los efectos de esta liberalización regulatoria fueron significativos. En primer lugar, se produjo un aumento significativo de proveedores de servicios: además de los bancos tradicionales, comenzaron a operar nuevas instituciones como bancos digitales e

40. Para más información, visite: <<https://www.jota.info/colunas/regulacao-financeira/sistema-de-pagamentos-brasileiro>>.

instituciones de pago (IP)⁴¹, lo que generó un aumento significativo de la competencia. En segundo lugar, surgió la oferta de servicios financieros, a veces más económicos y ágiles, que contribuyeron a la inclusión financiera al facilitar la integración de personas que aún tenían dificultades para abrir cuentas o acceder a métodos de pago electrónicos.

En este entorno más dinámico y competitivo, la innovación en el sistema de pagos cobró un nuevo impulso. El [Informe de Vigilancia del SPB de 2013](#), publicado en 2014, destaca la necesidad de seguir el ritmo de las transformaciones tecnológicas y la importancia de las políticas para la expansión de los servicios de pago móvil. Tales acciones, que buscaban la inclusión financiera, también son relevantes porque indican claramente el interés del BCB en soluciones que permitieran, a bajo costo, pagos minoristas en tiempo real e ininterrumpidos.

Como se indica en el texto que históricamente describe a Pix⁴², esta mención en el Informe de Vigilancia del SPB de 2013 fue la primera declaración pública sobre “pagos en tiempo real en el comercio minorista”. En su momento, incentivó el desarrollo de una solución abierta e interoperable por parte del sector. Este fue el embrión de lo que posteriormente se convertiría en el sistema de pagos instantáneos. El posicionamiento institucional del BCB en ese momento buscaba no solo aumentar la inclusión y la eficiencia de los servicios bancarios, sino también responder a los crecientes movimientos de modernización del sistema financiero global, con el objetivo de situar a Brasil junto a otros países que ya trabajaban en el desarrollo e implementación de los pagos instantáneos. En este sentido, en mayo de 2018, el Banco Central estableció un Grupo de Trabajo sobre Pagos Instantáneos⁴³.

41. Según la definición del Banco Central, una Institución de Pago (IP) es una entidad jurídica que presta servicios de compraventa y movimiento de fondos en el marco de un acuerdo de pago, sin la posibilidad de otorgar préstamos ni financiación a sus clientes. Las instituciones de pago permiten a los ciudadanos realizar pagos independientemente de su relación con bancos y otras instituciones financieras. Con recursos financieros móviles, por ejemplo, a través de una tarjeta prepago o un teléfono móvil, los usuarios pueden llevar fondos y realizar transacciones sin necesidad de efectivo. Gracias a la interoperabilidad, los usuarios también pueden recibir y enviar dinero a bancos y otras instituciones de pago. Disponible en: <https://www.bcb.gov.br/estabilidadefinanceira/instituicaopagamento>. Consultado el: 12 de mayo de 2025.

42. BANCO CENTRAL DO BRASIL. Relatório de Gestão do Pix. Concepção e primeiros anos de funcionamento 2020–2022. Brasília, DF: 2023.

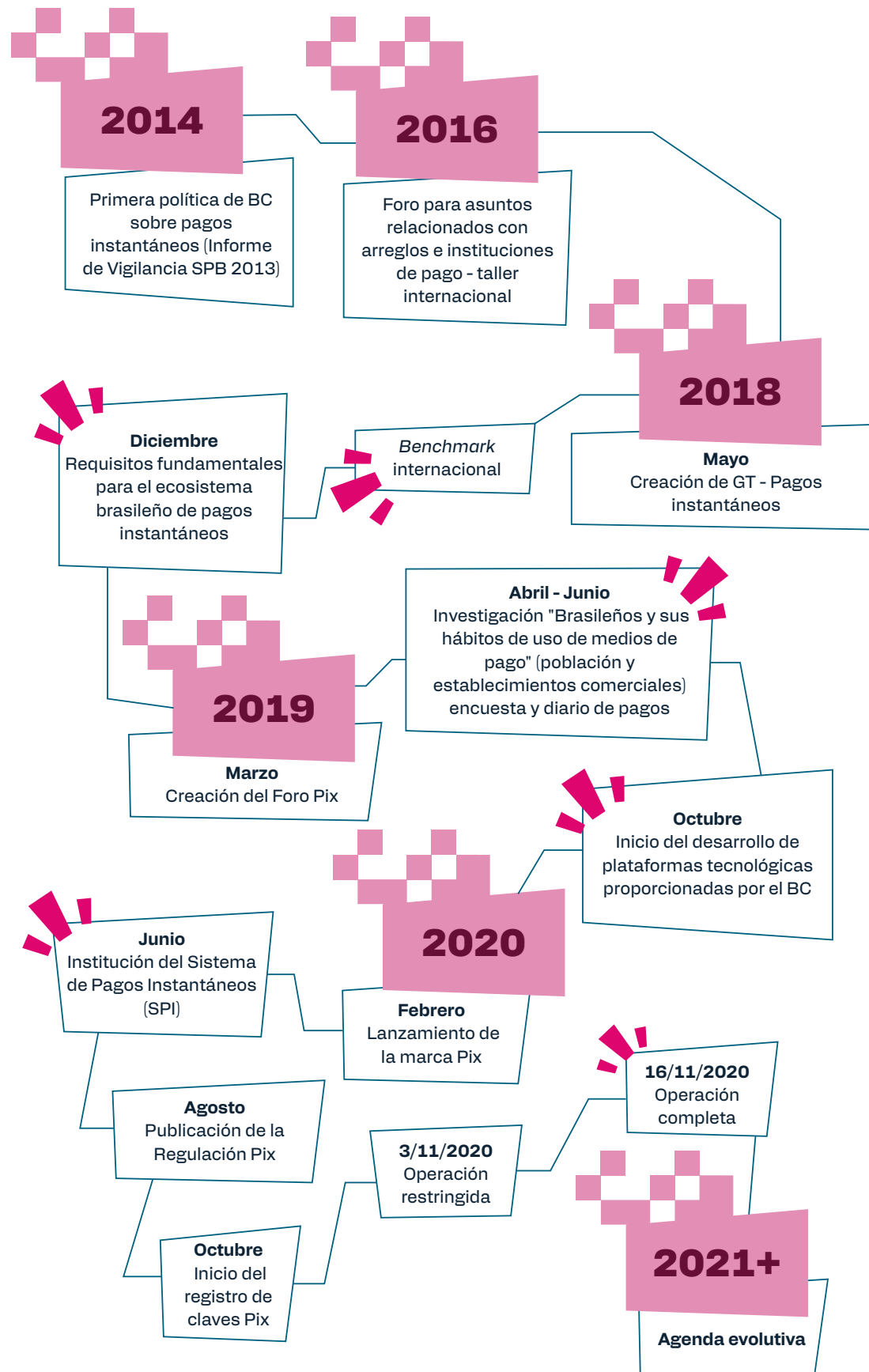
43. Puede encontrar más información en el sitio web del Grupo de Trabajo sobre Pagos Instantáneos. Disponible en: <https://www.bcb.gov.br/estabilidadefinanceira/gtpagamentos>. Consultado el: 3 de octubre de 2025.

Precisamente por identificar la lentitud o falta de coordinación entre los actores del mercado en la creación de un sistema de pagos instantáneos, la agencia asumió el rol de líder y catalizador en la implementación de este nuevo ecosistema de pagos. Solicitó la participación de otros actores del mercado, pero expresó claramente su interés en participar activamente, tanto en la definición de las reglas como en la provisión de la infraestructura⁴⁴. Siete meses después, el GT concluyó sus actividades con la publicación del [**Comunicado n.º 32.927**](#), que describió los requisitos fundamentales para el ecosistema brasileño de pagos instantáneos, sentando las bases de lo que posteriormente se convertiría en Pix. Posteriormente, en marzo de 2019, se creó el Foro Pix como órgano de gobernanza y espacio para la cocreación del Pix entre el Banco Central y el mercado⁴⁵. La historia de la creación del Pix hasta 2021 se puede ver en la Figura 8.

44. El discurso inaugural del Grupo de Trabajo de Pagos Instantáneos (GT) ofrece una visión general del contexto en aquel momento y de los principales objetivos del Banco Central al implementar el grupo. Disponible en: https://www.bcb.gov.br/content/estabilidadefinanceira/gt_pagamentos_instantaneos/Discursoabertura.pdf. Además de este material, el Informe de Gestión del Pix (BCB, 2023), en la sección “La Construcción y el Lanzamiento del Pix”, también presenta más información sobre el papel del Banco Central en el desarrollo del Pix.

45. Para más información sobre el desarrollo del Pix, visite “LiveBC#14 - Pix: como ele mudou e continuará mudando nossa vida?”. Disponible en: <https://www.youtube.com/watch?v=hzu8VgpXf3g&t=212s>. Consultado el: 3 de julio de 2025.

Figura 8. Línea del tiempo de creación del Pix



Fuente: Adaptado de BCB, 2023.

Para saber más:

El Idec y el Nuced publicaron, en 2023, un libro sobre el mercado de medios de pago titulado: “Perspectivas y Controversias en la Innovación Regulatoria en el Sistema Financiero de Pagos”.

PERSPECTIVAS E
CONTROVÉRSIAS

DA INOVAÇÃO
REGULATÓRIA NO

SISTEMA FINANCEIRO
DE PAGAMENTOS

Camila Leite Contrí
Vinicius Marques de Carvalho
Marcela Mattiuzzo
(Coord., Org.)

EDITORA SINGULAR

La inclusión financiera se encuentra con la exclusión digital

A lo largo de los últimos años, la inclusión financiera en Brasil ha sido un proceso dinámico, marcado por diferentes momentos: la expansión de los servicios bancarios, la llegada de nuevos actores, el desarrollo de nuevas tecnologías, la existencia de políticas sociales y, hasta incluso, eventos imprevistos como la pandemia de coronavirus. En este camino, observamos el lanzamiento del Pix y una aceleración en las tasas de adopción de la banca. Mientras el porcentaje de adultos con relación con instituciones financieras se mantuvo en torno al 85 % entre 2018 y 2019, en 2020 se registró un salto al 96 %⁴⁶.

Una de las principales razones de la significativa expansión de la relación de las personas con el sistema financiero nacional fue la pandemia de COVID-19 y el pago de la Ayuda de Emergencia. Esta ayuda financiera, destinada a una parte de la población, requería la apertura de cuentas bancarias para recibir los fondos. En un corto período, 14 millones de nuevas personas comenzaron a interactuar con el Sistema Financiero Nacional.⁴⁷ Los canales digitales adquirieron una creciente relevancia para las transacciones, principalmente gracias a la conectividad que ofrecen los smartphones. El Pix se lanzó e implementó precisamente en este contexto.

46. Consulte el Informe de Ciudadanía Financiera del Banco Central (2021). Disponible en: <https://www.bcb.gov.br/content/cidadaniafinanceira/documentos_cidadania/rif/relatorio_de_cidadania_financeira_2021.pdf>. Consultado el: 3 de octubre de 2025.

47. Puede encontrar más información en la página 43 del Informe de Ciudadanía Financiera (2021). Disponible en: <https://www.bcb.gov.br/content/cidadaniafinanceira/documentos_cidadania/RIF/Relatorio_de_Cidadania_Financeira_2021.pdf>. Consultado el: 3 de octubre de 2025.

Además, la fuerte presencia de *fintechs* e instituciones de pago impulsó nuevas formas de interacción.

La estructura bancaria tradicional, basada en sucursales físicas, presentaba limitaciones para llegar a regiones remotas y poblaciones de bajos ingresos. Aunque los corresponsales bancarios han desempeñado un papel importante en la ampliación del acceso, especialmente en las zonas rurales y las periferias urbanas, todavía existían importantes barreras que superar, como los elevados costes operativos y los procesos burocráticos, que dificultaban la plena inclusión de todos los ciudadanos.

El lanzamiento del Pix en noviembre de 2020 ofreció una alternativa de pago más rápida, segura y accesible. **Su rápida adopción se debió principalmente a las transferencias gratuitas garantizadas para personas físicas, la disponibilidad de transacciones 24/7 y su facilidad de uso.** Como resultado, se ha producido una expansión significativa de la inclusión financiera en el país. Según estimaciones del BCB, el Pix fue responsable de la inclusión de 71,5 millones de usuarios en el sistema financiero (datos de diciembre de 2022)⁴⁸.

Sin duda, el Pix representó una transformación significativa en el panorama financiero brasileño. Su rápida adopción y sus impresionantes cifras de transacciones demuestran la eficacia del sistema para satisfacer las necesidades de la población, especialmente de quienes anteriormente estaban excluidos del sistema financiero formal. Sin embargo, aunque Pix ha logrado una adopción exitosa en Brasil, convirtiéndose rápidamente en el método de pago más utilizado en el país, una parte significativa de la población aún permanece fuera de este sistema o en una inclusión precaria. **Reflexionar sobre la naturaleza de estas personas que no utilizan Pix es esencial para comprender los límites de la inclusión financiera digital y para orientar las políticas públicas que hagan este proceso aún más integral.**

Las investigaciones dedicadas a comprender quiénes no usan Pix aún son escasas. Datos del BCB (2023) indican que los pagos y transferencias a través del Pix se realizan principalmente por adultos de entre 20 y 39 años. El número de transacciones entre los mayores de 60 años aún es modesto. En general, las personas con vulnerabilidad socioeconómica y digital tienden a tener mayores dificultades para usarlo. Este grupo incluye a personas con bajos niveles de educación, personas de bajos ingresos, residentes de zonas rurales

48. Las cifras de los primeros tres años del Pix fueron publicadas por el BCB. Disponible en: <<https://www.bcb.gov.br/detalhenoticia/744/noticia>>. Consultado el: 25 de mayo de 2025.

o remotas, personas sin acceso a internet y personas con discapacidad. Estos perfiles son más susceptibles a enfrentar barreras —cognitivas, técnicas, estructurales y culturales— que dificultan la adopción de métodos de pago digitales.

La barrera de la exclusión digital es bastante evidente. El uso del Pix depende del acceso a teléfonos celulares y a una conexión estable a internet, especialmente *smartphones* con aplicaciones bancarias o de billeteras digitales. Sin embargo, según datos de la encuesta TIC Domicilios (2024), aún existe una desigualdad significativa en el acceso a internet en Brasil.

Incluso entre las personas bancarizadas con acceso a internet, hay quienes no usan Pix por temor al fraude o desconocimiento del sistema. Según una encuesta de Fiserv (2024), el 2% de las personas bancarizadas no realizan transacciones a través del Pix. Esta cifra, aunque aparentemente baja, debe tenerse en cuenta al considerar a los usuarios que necesitan ayuda de un amigo o familiar para usar Pix. La investigación identificó que el 46 % de los entrevistados ya había necesitado pedir a algún amigo o familiar que realizara un Pix por ellos.⁴⁹

Sería importante investigar más sobre estos temas y comprender la dinámica de uso para evaluar no solo el acceso a Pix, sino también la calidad de uso. Algunos usuarios pueden encontrarse con obstáculos recurrentes o experimentar un uso inseguro⁵⁰. La incapacidad de realizar transacciones financieras de forma independiente y segura puede generar sentimientos de exclusión, incapacidad o frustración.

Las debilidades mencionadas convergen con los datos del **Indicador de Alfabetización Funcional (INAF)**. El estudio, publicado en 2024, reveló una realidad preocupante: el 29% de la población brasileña de entre 15 y 64 años se considera analfabeta funcional (INAF, 2024, p. 10). En otras palabras, aproximadamente 40 millones de jóvenes y adultos tienen habilidades limitadas de lectura, escritura y aritmética, lo que les dificulta satisfacer las demandas cotidianas. Esta condición impacta directamente en la capacidad de estas personas para usar herramientas digitales.

El INAF 2024 evaluó, por primera vez, el nivel de alfabetización digital entre la población brasileña.

49. Más información disponible en la encuesta *Fiserv Insights: Pix e as Novas Modalidades sob a ótica do Cliente* (2024). Disponible en: <<https://www.fiserv.com.br/pesquisa-pix-insights-2024-fiserv/>>. Accessed on: 6 de junio de 2025.

50. Ocasionalmente, los artículos periodísticos brindan información para el consumidor y ofrecen pistas sobre las dificultades de usar Pix. Por ejemplo, véase: <<https://cbn.globo.com/media/audio/409542/apos-dois-anos-e-meio-cerca-de-28-milhoes-de-brasi.htm>>. Consultado el: 6 de junio de 2025.

Usar la lectura y la escritura en las prácticas sociales hoy también significa saber cómo usar los recursos del mundo digital para realizar diversas tareas y comunicarse. (INAF, 2024, p. 21)

Los resultados también indican que el 95% de las personas analfabetas funcionales tienen un desempeño deficiente en actividades digitales básicas, como comprar o completar formularios en línea. Incluso entre las personas con un nivel de alfabetización avanzado, el 40 % presentó dificultades con tareas digitales más complejas. Estos datos muestran que la alfabetización tradicional no garantiza la plena inclusión digital (INAF, 2024, p. 17).

La alta tasa de analfabetismo funcional en Brasil representa un obstáculo significativo para la adopción de herramientas digitales, incluyendo Pix. Superar este desafío requiere un esfuerzo conjunto para promover la alfabetización en sus múltiples dimensiones, garantizando una inclusión financiera verdaderamente inclusiva y segura. Para promover una inclusión financiera efectiva, será fundamental invertir en programas de alfabetización digital y funcional, especialmente dirigidos a adultos y poblaciones vulnerables. También es necesario desarrollar interfaces más accesibles e intuitivas en las aplicaciones, considerando las limitaciones de alfabetización de la población. La colaboración entre el gobierno, el sector privado y la sociedad civil es esencial para superar estas barreras y garantizar que todos los brasileños puedan beneficiarse de las innovaciones tecnológicas en el sector financiero.

51. Disponible en: https://www.correiobraziliense.com.br/cidades-df/2025/05/7152593-pagamento-a-moda-antiga-ainda-posso-utilizar-dinheiro-em-especie.html#google_vignette. Consultado el: 3 de octubre de 2025.

Lente: Seguridad



Desde el lanzamiento del Pix, la preocupación por fraudes y delitos cibernéticos ha salido a la luz. Inicialmente, se observaron los esfuerzos de la institución para generar confianza en torno a un nuevo método de pago. En ese momento, se entrevistó a expertos para explicar las medidas de seguridad implementadas por el Banco Central⁵².

Aunque el nuevo sistema exige cambios y adaptaciones, tanto para los consumidores como para las instituciones financieras, se reforzó que los datos y las transacciones relacionadas con el Pix se realizarían de forma encriptada a través de la red del sistema financiero nacional. Esta red representa una estructura de comunicación de datos en funcionamiento desde 2002 y reconocida por su resiliencia. Además, los usuarios del Pix utilizan la aplicación del banco o el entorno de *internet banking*, que cuenta con mecanismos de seguridad como biometría, reconocimiento facial, contraseñas y autenticación de dos factores⁵³.

Sin embargo, estas medidas de seguridad no han impedido que los consumidores sean víctimas de una amplia variedad de estafas relacionadas con Pix. La velocidad de las transacciones se considera un factor facilitador de diversas acciones fraudulentas. **La inmediatez del Pix, una característica clave, ha dificultado la identificación y la detención de estafas y fraudes realizados a través del sistema.**

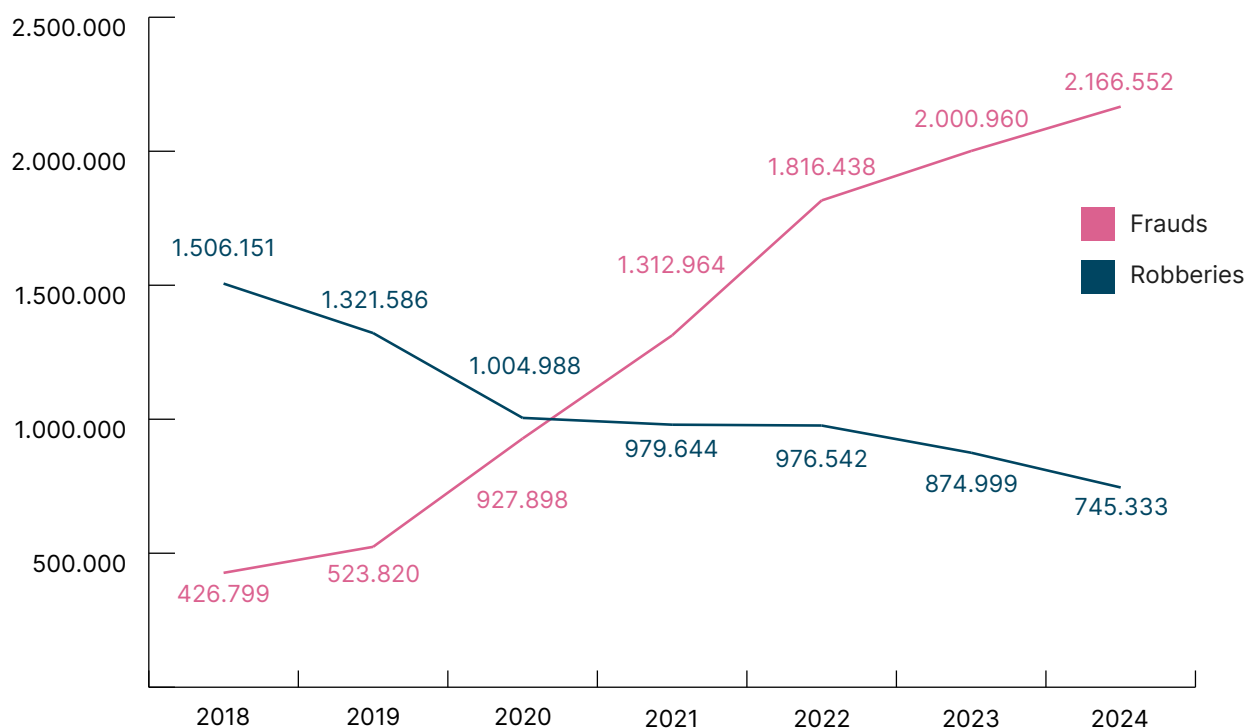
La introducción de un nuevo método de pago, combinada con otras transformaciones tecnológicas y sociales, ha impactado directamente en las estrategias delictivas. Esta redefinición táctica es evidente en los registros de delincuencia del país, que muestran una nueva dinámica operativa. Se ha observado una disminución en la incidencia de robos, mientras que, por otro lado, especialmente desde 2021, delitos como el fraude, las estafas en línea y el hurto han mostrado un crecimiento significativo (Figura 9).

52. Para ver un ejemplo de artículos sobre seguridad en el momento del lanzamiento del Pix, acceda a: <<https://www1.folha.uol.com.br/mercado/2020/12/especialistas-divergem-sobre-riscos-a-seguranca-em-transacoes-com-o-pix.shtml>> y <<https://g1.globo.com/jornal-nacional/noticia/2020/11/05/pix-os-cuidados-com-a-seguranca-do-novo-sistema-de-pagamento-instantaneo-criado-pelo-bc.ghtml>>. Consultado el: 24 de septiembre de 2025.

53. Como afirma el Banco Central, la seguridad del Pix se basa en cuatro dimensiones: (1) autenticación del usuario; (2) trazabilidad de la transacción; (3) flujo seguro de datos; y (4) reglas operativas del Pix. Disponible en: <https://www.bcb.gov.br/estabilidadefinanceira/pix?utm_medium=referral%2F>. Consultado el: 15 de enero de 2025.

El fraude electrónico aún no se registra de forma estandarizada en todos los estados brasileños, lo que dificulta su contabilización. Sin embargo, como se muestra en el Anuario Brasileño de Seguridad Pública (2024; 2025), existe un claro cambio en la naturaleza de los delitos contra la propiedad.

Figura 9. Evolución de los delitos de robo y fraude entre 2018 y 2024



Fuente: Foro Brasileño de Seguridad Pública, 2025.

Para comprender esta transición, vale la pena considerar los robos residenciales, tan comunes hace décadas. En estas acciones, los delincuentes apuntaban a activos físicos como automóviles, televisores, computadoras, equipos de música o joyas, artículos que alimentaban un mercado para recibir bienes robados. A medida que las transformaciones digitales alteran la sociedad y la forma en que las personas interactúan, cambiando los hábitos y las relaciones, se abren nuevas vías para la actividad delictiva. Los riesgos de robar físicamente una casa son significativamente mayores que cometer estafas y fraudes en línea. El entorno digital permite la expansión del alcance geográfico, eliminando la interacción cara a cara y el uso de la violencia física. Dado que gran parte de los activos de las personas (cuentas bancarias, inversiones, criptomonedas) se gestionan digitalmente a través de *smartphones*, sitios web y aplicaciones, se abren nuevas oportunidades

para que los delincuentes cometan fraudes financieros y extorsión en línea, explotando la dependencia tecnológica y nuevas formas de relaciones⁵⁴.

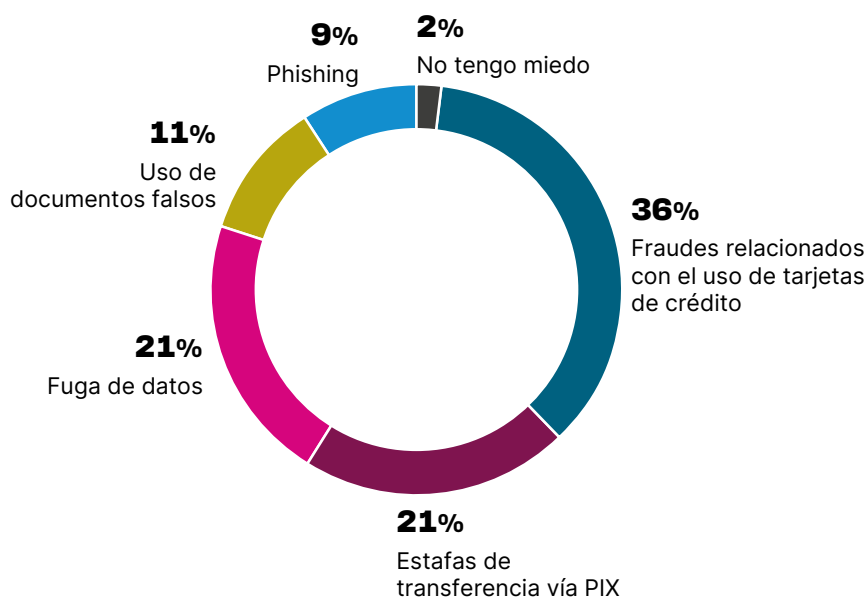
No es casualidad que los robos y hurtos de celulares sean motivo de gran preocupación. Esto se debe no solo al valor físico del dispositivo y a los canales de comercio ilegal, sino principalmente a que, con el celular en mano, los delincuentes pueden acceder a mensajes, *aplicaciones* bancarias, contraseñas, fotos y contactos: datos valiosos que pueden usarse para cometer fraudes o estafas.

1 de cada 3 brasileños es engañado y desaparecen R\$ 297,7 mil millones en un año.

(Fuente: Gasa, 2024)

Ante el avance de los delitos cibernéticos, el miedo a ser víctima de estafas es una constante para la población brasileña. El informe “Identidade Digital e Fraude (Identidad Digital y Fraude)” presentado por Serasa Experian (2024) indica que el fraude con métodos de pago (como tarjetas de crédito y transacciones Pix) representa la principal preocupación de los participantes del estudio.

Figura 10. Miedo por tipo de estafa



Fuente: Adaptado de Serasa Experian, 2024.

54. Se pueden encontrar más detalles sobre los factores que llevaron al cambio en los delitos contra la propiedad en Brasil en los Anuarios Brasileños de Seguridad Pública 18 y 19, publicados en 2024 y 2025, respectivamente.

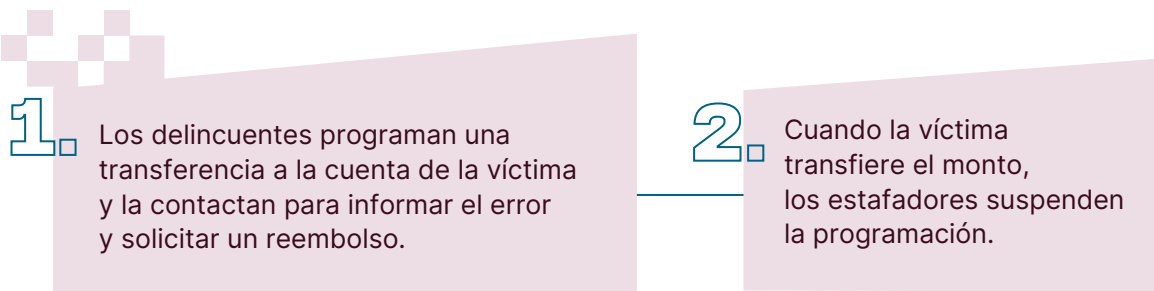
El temor de ser víctima de fraudes relacionados con medios de pago está justificado. Las acciones más comunes son: (1) la clonación o el intercambio de tarjetas bancarias y (2) estafas en las que el defraudador solicita dinero haciéndose pasar por alguien conocido o emulando un centro de atención al cliente. En este caso, el delincuente finge ser un representante de la propia institución financiera. También existen las llamadas “estafas del PIX” (Febraban/lpespe, 2025).

Principales estafas relacionadas con el Pix

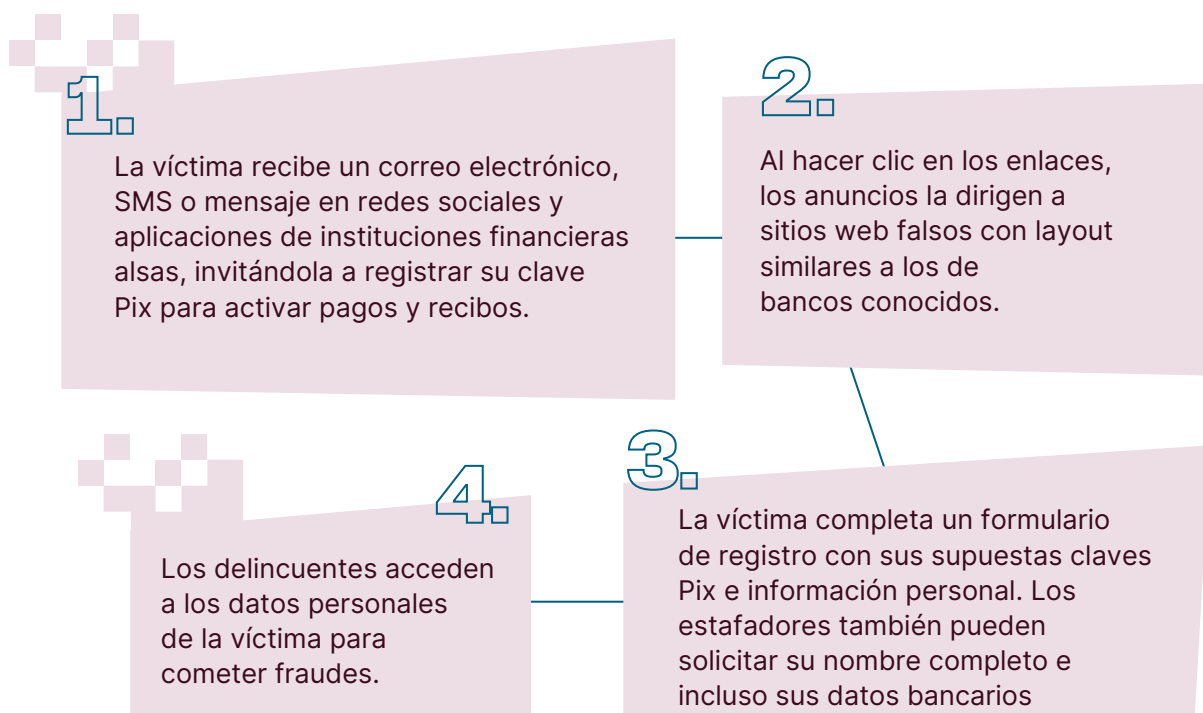
Estafa del Pix incorrecto



Estafa del Pix Programado



Estafa de registro del Pix



Estafas del tipo APP (*Authorized Push Payment*)

En lo que respecta específicamente a los delitos relacionados con transferencias de fondos a través del Pix, el 97 % de los fraudes denunciados fueron estafas de *Authorized Push Payment* (APP)⁵⁵. En resumen, las estafas denominadas APP se refieren a pagos autorizados por error. En este tipo de fraude financiero, los delincuentes manipulan a las víctimas para que,

55. Los datos publicados por Silverguard en el Estudio “Golpes con Pix (Estafas del Pix)” se recopilaban a partir de 5000 denuncias de víctimas a las que respondió el Centro de Estafas SOS entre enero y junio de 2024.

aparentemente, transfieran fondos directamente a una cuenta controlada por los estafadores o para que proporcionen la información necesaria para que estos completen la transacción. A diferencia de otras estafas que implican el acceso no autorizado a la cuenta de la víctima, en los casos de APP, la transferencia la inicia y autentica el propio usuario, a menudo engañado mediante elaboradas tácticas de ingeniería social.

La complejidad de estas estafas radica en su capacidad para ocultar la naturaleza fraudulenta de la transacción hasta que es demasiado tarde. Los delincuentes emplean tácticas elaboradas para ganarse la confianza de la víctima y convencerla de la legitimidad de la solicitud de pago.

En estos casos, la recuperación de fondos se vuelve significativamente más compleja, ya que la restitución a las víctimas a menudo solo se realiza si aún existen fondos en las cuentas de los estafadores. La jurisprudencia brasileña ha sido favorable a los consumidores víctimas de fraude, reconociendo su vulnerabilidad a la sofisticación de las estafas digitales y la responsabilidad objetiva tanto de las instituciones financieras como de las plataformas digitales involucradas. Los tribunales, con base en el Código de Protección al Consumidor, han establecido que es responsabilidad del proveedor de servicios garantizar la seguridad de las transacciones y proteger los datos de los clientes. Por lo tanto, cuando se prueba una falla en la prestación del servicio (como la falta de mecanismos de autenticación efectivos, la liberación indebida de transacciones o la negligencia en la supervisión de actividades sospechosas), es común reconocer el deber de indemnizar, tanto por daños materiales como, en algunos casos, por daños morales. Por otro lado, también es común que las instituciones financieras no se consideren responsables de reembolsar a sus clientes y desestimen su responsabilidad alegando que el acceso indebido a la cuenta no está probado, sino que es una acción voluntaria de la víctima, incluso si fue inducida por engaño. Esta falta de apoyo ante estafas y el bajo nivel de restitución a las víctimas son puntos críticos que merecen mayor atención, además de un debate urgente sobre responsabilidades. Es necesario garantizar la construcción de sistemas y procedimientos cada vez más seguros para los consumidores, considerándolos el punto más vulnerable de toda la cadena.

Hoy en día, debido a la velocidad de las transacciones instantáneas y al tiempo que transcurre entre la denuncia y el bloqueo de la cuenta, las víctimas suelen experimentar frustración al intentar recuperar los fondos transferidos. La denuncia de estafas a las autoridades es baja. Según el informe Estafas Digitales en Brasil (Gasa, 2024), solo el 31 % de las víctimas contactó a la policía u otras autoridades para denunciar la estafa o el intento de estafa. La falta de denuncia se debe a dos razones principales: (1) la percepción de que denunciar el incidente no resultará en una resolución y (2) la complejidad de los procesos, incluida la incertidumbre sobre a quién contactar en estos casos.

Además de estos factores destacados por el estudio de Gasa (2024), la falta de denuncia de estafas también puede estar relacionada con sentimientos de vergüenza o culpa, miedo a una mayor exposición, desconocimiento de cómo actuar o a quién contactar, y la percepción de que no se puede hacer nada (Freitas, 2024).

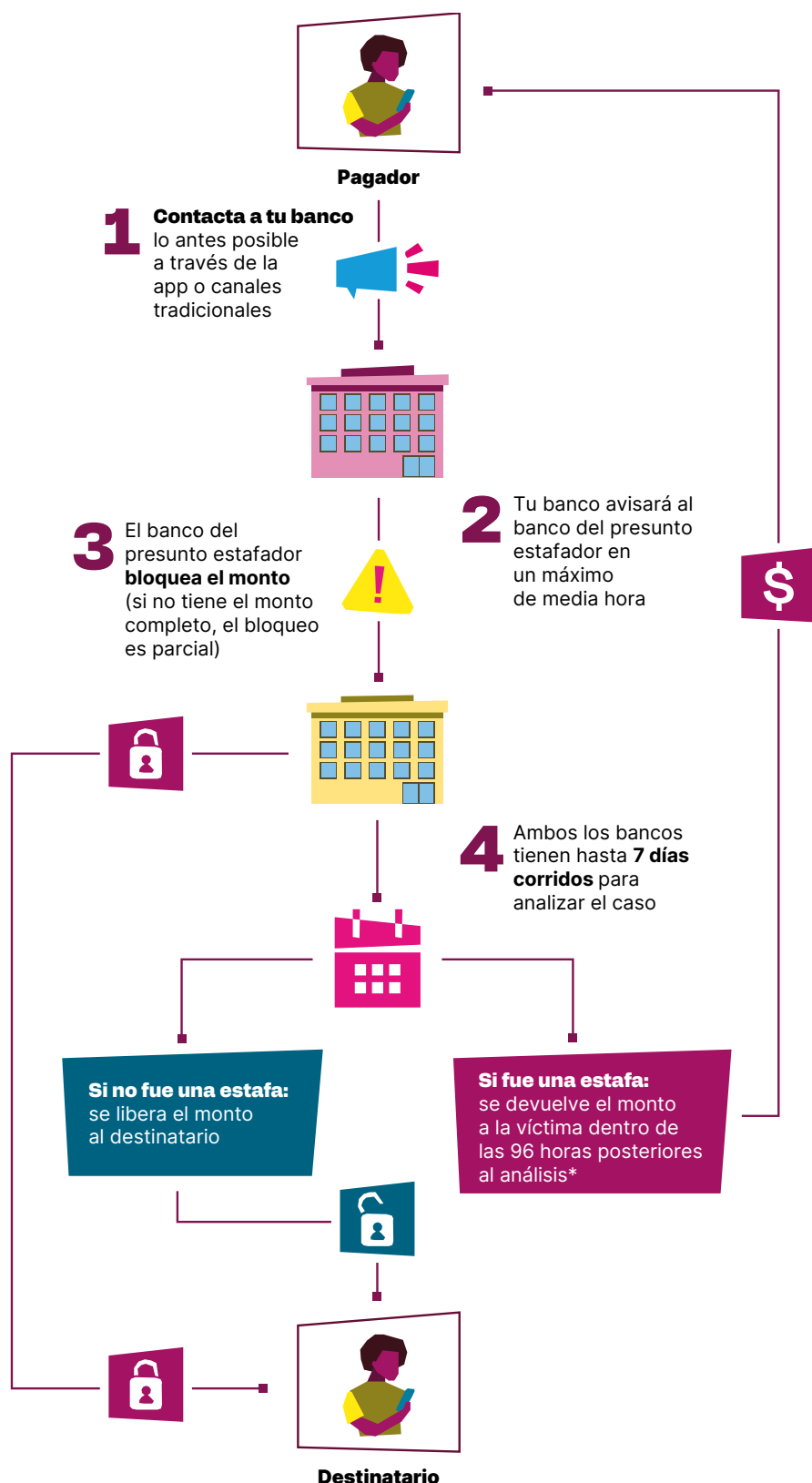
MED: Mecanismo Especial de Devolución del Pix

Una de las principales herramientas de seguridad del Pix es el **Mecanismo Especial de Devolución (MED)**, definido como un conjunto de reglas y procedimientos para recuperar montos en caso de fallas operativas, estafas o fraudes.

Lanzado en 2021, el MED se activa por la queja de un pagador y el registro de la disputa ante la institución financiera, el organismo responsable de evaluar el caso. Al recibir la queja, la institución financiera responsable de la cuenta receptora coloca una retención preventiva en el saldo disponible por hasta 7 días hábiles, un período designado para analizar la transacción. Si se verifica el fraude, se autoriza la devolución de los fondos a la víctima. El BCB estableció un período de hasta 80 días para que las víctimas de fraude registren su caso para activar el MED (Figura 11)⁵⁶.

56. Disponible en: <<https://www.bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-mecanismo-especial-de-devolucao-med>>. Consultado el: 10 de enero de 2025.

Figura 11. Cómo funciona el MED



*Si no hay saldo suficiente para la devolución total de los montos, el banco del destinatario debe monitorear la cuenta hasta 90 días desde la transacción original y, de surgir recursos, debe realizar reembolsos parciales.

Después de 90 días, no habrá reembolso como se describe arriba, incluso si hay un crédito en la cuenta del destinatario.

¡Importante!

1 - El banco del destinatario no está obligado a utilizar sus propios recursos para reembolsar el monto solicitado.

2 - Si su problema no se resuelve, presente una queja ante el Banco Central. También puede visitar www.consumidor.gov o comunicarse con la Agencia de Protección al Consumidor de su estado (Procon) o el Poder Judicial.

Fuente: Adaptado de Banco Central

Es importante tener en cuenta que, a pesar de la popularidad del nuevo sistema de pago, con millones de transacciones diarias, el mecanismo para garantizar el reporte de fraudes y quejas en caso de inconsistencias en las transacciones solo se puso a disposición después de que Pix hubiera estado en vigencia durante un año.

Debido a que es un nuevo instrumento de pago, en el que podrían ocurrir todo tipo de errores operativos, se prestó poca atención a abordar las dificultades que los usuarios podrían enfrentar. Antes de la creación del MED, no existía un proceso estandarizado para manejar casos de fraude o errores operativos, lo que dificultaba los reembolsos. Los canales de apoyo existentes fueron manejados por las instituciones participantes, sin lineamientos específicos para estas situaciones.

Además, cabe destacar que el MED opera en casos muy específicos y solo puede activarse en caso de fraude o fallos operativos por parte de las instituciones financieras. No se prevé su activación en situaciones de desacuerdos comerciales ni en casos de errores del usuario. Por lo tanto, al usar Pix, se requiere extrema precaución, especialmente debido a la inmediatez del sistema. Los errores tipográficos, como introducir una clave o un importe incorrectos, no se pueden cancelar una vez confirmada la transacción y no están cubiertos por el MED. En estos casos, el usuario debe contactar con su institución financiera, que, en algunos casos, puede ofrecer instrucciones para intentar un reembolso al destinatario, aunque no hay garantía de éxito. Lo que se observa al realizar una transferencia Pix incorrecta es la ausencia de una vía institucionalmente diseñada para que el consumidor recupere los fondos transferidos.

A pesar de la implementación del MED, su eficacia ha sido limitada. En 2022, por ejemplo, 7 de cada 10 solicitudes de reembolso a través del MED fueron rechazadas, el 89% de ellas por falta de fondos o cierre de la cuenta receptora (Silverguard, 2023)⁵⁷. Esto se debe a que el MED, en su versión inicial, solo bloquea la primera cuenta a la que se destinaron los fondos enviados por la víctima. Dado que el reembolso solo es posible si la cuenta receptora aún tiene fondos disponibles, es común que los estafadores, aprovechándose de las limitaciones del sistema, distribuyan rápidamente el monto recibido entre diferentes cuentas, lo que dificulta el bloqueo y, por consiguiente, la devolución de los fondos a la víctima. En estas transacciones, el uso de cuentas fantasma para distribuir los fondos ha sido una práctica común⁵⁸.

57. Datos divulgados en el estudio “Golpes com Pix”, elaborado por Silverguard y publicado en 2023.

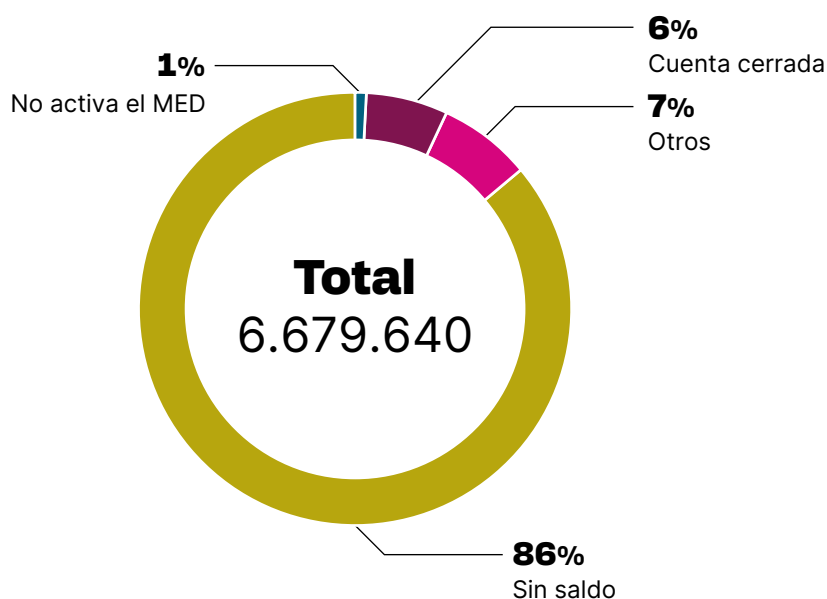
58. SERASA EXPERIAN. **Entenda como fraudadores usam o Pix para impulsionar a abertura de contas laranjas.** São Paulo, December 8. 2022. Disponible en: <<https://www.serasaexperian.com.br/conteudos/entenda-como-o-pix-impulsiona-a-abertura-de-contas-laranjas/>>. Consultado el: 4 de octubre de 2025.

En 2024, solo se aceptó el 31% de los 5 millones de solicitudes de MED por transferencias fraudulentas vía Pix. Durante este período, el Banco Central solo devolvió alrededor del 7% de los fondos malversados (R\$459 millones de un total de R\$6,98 mil millones)⁵⁹. Ante una tasa de recuperación muy baja, MED resultó ineficaz y, en consecuencia, poco conocido entre los usuarios e incluso los empleados de las instituciones financieras. Según datos de Silverguard (2023), **9 de cada 10 brasileños desconocen qué es MED ni cómo funciona**⁶⁰.

Datos de solicitud de MED



Figura 12. Motivos de la negación del reembolso financiero por parte del BCB



Fuente: Adaptado de Folha de S. Paulo basándonos en datos del Banco Central.

59. Datos proporcionados por el BCB a solicitud del periódico Folha de S. Paulo. Disponible en: <<https://www1.folha.uol.com.br/mercado/2025/06/nova-ferramenta-do-banco-central-vai-seguir-dinheiro-roubado-em-golpe-do-pix.shtml>>. Consultado el: 7 de octubre de 2025.

60. Datos publicados por Silverguard en el estudio «Golpes com Pix» de 2023.

MED 2.0: La nueva versión del mecanismo

En 2022, se inició el desarrollo de una nueva versión del Mecanismo Especial de Devolución, temporalmente denominada MED 2.0. **Este sistema rediseñado busca permitir el seguimiento y el bloqueo de recursos incluso cuando los defraudadores los transfieren a múltiples cuentas.** Programada para su lanzamiento entre finales de 2025 y principios de 2026, la nueva versión de MED se desarrolló para identificar posibles rutas de dinero y notificar a todas las instituciones con cuentas involucradas en las transacciones, garantizando reembolsos dentro de los 11 días posteriores a la disputa del cliente⁶¹.

Figura 13. Dibujo de alto nivel de MED 2.0 - Algoritmo de retorno

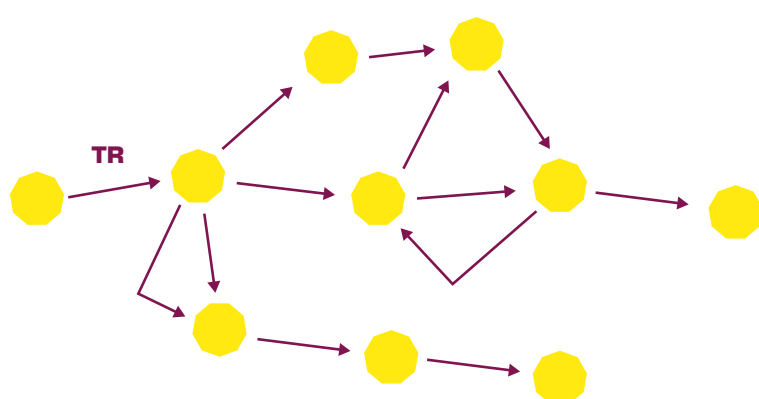
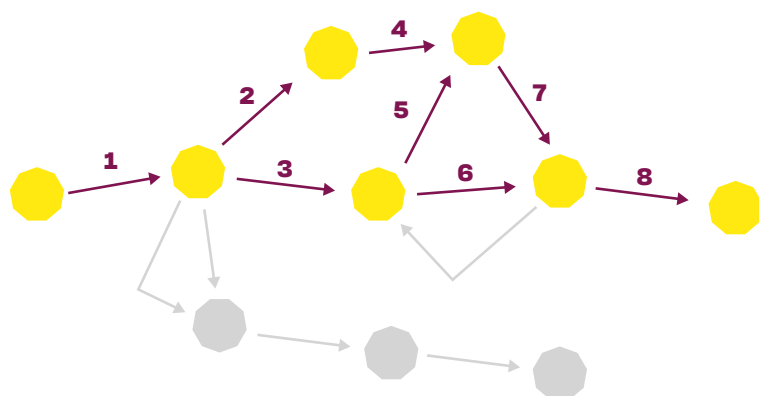


Gráfico de seguimiento

Seguimiento: La participante víctima solicita un seguimiento. El DICT genera el Gráfico de Seguimiento de la Transacción a partir de la Transacción Raíz.



Priorización de las Rutas de Bloqueo

Con base en el Gráfico de Seguimiento, se elige una **priorización de las rutas de bloqueo**. Los participantes pueden optar por utilizar un algoritmo estándar o definir la priorización con sus propios medios.

Fuente: BCB, 2024c.

61. Como parte del Foro Pix, Idec monitoreó las discusiones de GE-Seg sobre el desarrollo de MED 2.0. El hecho de que MED 2.0 solo active el seguimiento de recursos para fraudes superiores a R\$200,00 fue una de las preocupaciones planteadas por Idec. Una de las contribuciones de Idec está disponible en: <https://idec.org.br/sites/default/files/consideracoes_ao_subgrupo_do_med_2.0_decisoes_5_e_6_idec.docx.pdf>. Consultado el: 28 de mayo de 2025.

Los caminos del dinero:

Con MED 2.0, el BCB busca aumentar su capacidad para identificar cuentas fantasmas utilizadas en fraudes y eliminarlas. Sin embargo, a pesar de dificultar el trabajo de los delincuentes, algunos expertos ya anticipan que, además de mover fondos con extrema rapidez, los estafadores también podrían adoptar la práctica de transferir los fondos robados al extranjero o convertirlos en criptomonedas. En este último caso, se garantizaría el anonimato y el dinero abandonaría el sistema financiero tradicional.



Para monitorear la eficiencia de la nueva versión de MED, también se planea incorporar indicadores que podrían aportar mayor transparencia al uso del mecanismo. Según las discusiones establecidas en el Foro Pix, la forma en que cada institución responde a los casos de fraude es bastante diferente. Mientras que algunas implementan con prontitud el protocolo establecido por MED, otras rechazan con frecuencia las solicitudes de detección de fraude. Esta disparidad es sorprendente y revela que aún se necesitan ajustes para estandarizar este protocolo.

Junto con estas mejoras, también se desarrolló una función que permite a los usuarios impugnar transacciones fraudulentas sin necesidad de interactuar con representantes del banco. La función de autoservicio del Mecanismo Especial de Reembolso (MED) busca brindar mayor agilidad y eficiencia al proceso de disputa⁶². Cuanto más rápido se bloqueen los fondos en las cuentas utilizadas por los estafadores, mayor será la probabilidad de reembolsos exitosos para el usuario afectado.

62. Para más información sobre el botón de disputa del MED, consulte: <https://www.bcb.gov.br/detalhenoticia/20865/noticia>. Consultado el: 4 de octubre de 2025.

Otras medidas de seguridad del Pix:

Además del MED, se pueden destacar varias iniciativas implementadas por el BCB para garantizar una mayor seguridad en las transacciones del Pix. Estas incluyen:

- ➔ **Grupo de Trabajo dedicado a la seguridad:** La existencia, dentro del Foro Pix, de un grupo de trabajo dedicado exclusivamente a este tema (GE-Seg). En este sentido, existe un diálogo constante con diferentes actores involucrados en la seguridad de las transacciones, lo que permite evaluaciones y actualizaciones tanto de las reglas como de la infraestructura del Pix, si es necesario.
- ➔ **Gestión de Límites de Transacción:** Esta es una función obligatoria en las aplicaciones de las instituciones que ofrecen el Pix. Permite a los usuarios verificar y ajustar los límites de transacción, que pueden variar según el perfil del destinatario y la hora del día o de la noche.
- ➔ **Mecanismo de Bloqueo Precautorio:** Permite el bloqueo preventivo por hasta 72 horas en caso de sospecha de fraude.
- ➔ **Marcación en el DICT:** señalización de claves Pix y de CPFs/CNPJs involucrados en transacciones fraudulentas. Esta información, al compartirse con todas las instituciones participantes, tiene como objetivo prevenir nuevas estafas.
- ➔ **Campañas de comunicación:** Mensajes de alerta y concientización para los usuarios sobre temas de seguridad.

Fuga de datos

El informe Panorama de Amenazas para América Latina 2024, publicado por Kaspersky, revela que Brasil representó más de 700 millones de ciberataques en un período de 12 meses, lo que resultó en un promedio de 1.379 incidentes por minuto. Este volumen sitúa al país en segundo lugar en el ranking mundial de delitos cibernéticos, precedido únicamente por Estados Unidos.⁶³

63. Datos publicados por Kaspersky. Disponibles en: <https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2024/22888/> y <https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/>. Consultado el: 5 de julio de 2025.

Las consecuencias del fraude y las estafas son significativas en varios niveles. Para las empresas, además de las pérdidas financieras, existe la filtración de datos sensibles y confidenciales, lo que puede llevar a una erosión de la confianza de los clientes y usuarios de sus servicios. Desde la perspectiva del consumidor, además de las pérdidas monetarias, existen impactos emocionales significativos, como vergüenza, frustración, ira y, notablemente, una pérdida de confianza, tanto en las empresas y las personas de su entorno, como en su propia capacidad para tomar decisiones. Esto puede, en muchos casos, conducir al aislamiento social.

Las fugas de datos de registro asociados a las claves Pix han representado un desafío. Estas fugas, casi dos docenas, no expusieron contraseñas, saldos ni transacciones bancarias, pero sí difundieron datos que podrían servir de base para fraudes más complejos⁶⁴. Esta información, al ser utilizada por delincuentes, suele servir como cebo, dando credibilidad a tácticas fraudulentas.

El incidente más significativo, hasta el momento de redactar este documento, ocurrió en julio de 2025 e involucró al Sistema de Búsqueda de Activos del Poder Judicial (Sisbajud), operado por el Consejo Nacional de Justicia (CNJ). Según un comunicado oficial del BCB⁶⁵, se accedió a datos de registro vinculados a 46.893.242 claves Pix, lo que afectó a aproximadamente 11.000 personas (ya que un solo CPF puede tener más de una clave). El incidente constituye la mayor fuga de la historia y expuso los siguientes datos: nombre del titular de la cuenta, clave Pix, nombre del banco, número de sucursal y número de cuenta.

Independientemente del tamaño de las filtraciones ocurridas, incidentes de esta naturaleza indican que existen vulnerabilidades. Además, generan un desgaste de confianza en toda la cadena. Incluso si la fuga afectara a datos de registro no sensibles, su ocurrencia representa una violación de datos personales, protegidos por la LGPD.

Finalmente, cabe destacar que, a pesar de reportar los incidentes e informar que se han tomado medidas para investigar los casos, el Banco Central aún no ha impuesto multas relacionadas con estas fugas.

64. El Banco Central mantiene una página específica en su sitio web para reportar incidentes de seguridad de este tipo. Disponible en: <https://www.bcb.gov.br/acessoinformacao/lcpd?modalAberto=registro_de_incidentes_com_dados_pessoais>. Consultado el: 7 de octubre de 2025.

65. Disponible en: <<https://www.bcb.gov.br/detalhenoticia/20770/nota>>. Consultado el: 7 de octubre de 2025.

¿Qué ha estado haciendo el gobierno brasileño para combatir el fraude?

Alianza Nacional para el Combate de Fraudes Bancarias Digitales:

Anunciada en febrero de 2025, la Alianza Nacional para el Combate de Fraudes Bancarias Digitales, coordinada por el Ministerio de Justicia y Seguridad Pública (MJSP) y Febraban, es una alianza público-privada destinada a prevenir y reprimir las estafas y los delitos informáticos. La iniciativa se organiza en tres grupos temáticos: (1) mejores prácticas para la prevención, detección y respuesta; (2) intercambio y procesamiento de datos e información; y (3) asistencia a víctimas y capacitación de agentes (Figura 14)

Figura 14. Alianza Nacional para el Combate de Fraudes Bancarias Digitales



Fuente: Adaptado de Ministerio de Justicia y Seguridad Pública, 2025.

En el ámbito estatal, considerando el estado de São Paulo, una experiencia en favor de la seguridad en transferencias electrónicas fue la creación, en 2023, de una Comisión Parlamentaria de Investigación (CPI) “Estafas con Pix y Clonación de Tarjetas”, instalada en la Asamblea Legislativa del Estado de São Paulo (ALESP). Las actividades y debates que se llevaron a cabo representaron un esfuerzo investigativo estatal reciente para mapear, auditar y proponer soluciones a los fraudes que se han multiplicado en el entorno de pagos digitales en Brasil⁶⁶.

66. La CPI fue creada a mediados de 2023, mediante la Ley N.º 100/2023 de ALESP. Disponible en: <<https://www.al.sp.gov.br/norma/207721>>. Consultado el: 3 de octubre de 2025.

Otras entidades que también han sido víctimas de fraude relacionado con Pix están debatiendo estas acciones delictivas y buscando formas de combatirlas. En la Asamblea Legislativa del Estado de Paraíba (ALPB), la Defensoría Pública de Paraíba (DPE-PB), a través de su Inspección General, asistió a una audiencia pública para combatir las estafas de ingeniería social⁶⁷. La Corregeduría General de la DPE-PB registró cerca de 50 estafas que involucraban el nombre de la institución. Los delincuentes acceden a información de los casos patrocinados por la institución, se hacen pasar por defensores públicos u otros funcionarios y exigen el pago de costas judiciales a los beneficiarios, induciéndolos a realizar transferencias a través de aplicaciones bancarias. En Rio Grande do Sul, también se llevó a cabo una operación policial denominada “Diluvio Moral”, con el objetivo de detener a personas involucradas en estafas que utilizaban claves Pix y perfiles falsos para recibir donaciones⁶⁸.

Más recientemente, con el aumento de los ataques cibernéticos que las instituciones del sistema Pix han comenzado a sufrir, las iniciativas conjuntas de prevención y combate a fraudes se vuelven urgentes. **Los incidentes que involucran intentos de intrusión al sistema, robo de contraseñas y credenciales de acceso, o incluso la cooptación de empleados, muestran que existen brechas y puntos de vulnerabilidad que pueden poner en riesgo la seguridad del sistema de pago.** Aunque hasta ahora no se ha registrado ningún ataque *hacker* a la infraestructura del Banco Central, ni desvío de dinero de cuentas de clientes bancarios, los episodios ocurridos requieren extrema atención y revisión de los mecanismos de control. El crecimiento de la infraestructura del Pix y las grandes sumas transferidas a través de ella resultan atractivos para las organizaciones criminales.

Por lo tanto, además de invertir en tecnología capaz de frenar estas prácticas, también es necesario revisar constantemente los requisitos de seguridad del Pix, lo que exige la adopción de estos protocolos por parte de todos los conectados al sistema. Se necesitan urgentemente organismos de monitoreo, control y supervisión para garantizar que todos los agentes del sistema cumplan estrictamente las normas de seguridad.

Además, en caso de fugas, fallos o fraude, es importante dar visibilidad al incidente. Es crucial que los consumidores conozcan mejor la seguridad de las instituciones que eligen utilizar. Comprender el nivel de seguridad de las instituciones se convierte en un factor decisivo a la hora de decidir dónde invertir sus recursos financieros.

67. Más información disponible en: <https://defensoria.pb.def.br/defensoria-participa-de-audiencia-publica-sobre-golpe-do-falso-advogado-na-alpb/>. Consultado el: 3 de octubre de 2025.

68. Más información disponible en: <https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2024/05/16/policia-do-rs-prende-trio-no-abc-paulista-suspeito-de-golpe-usando-contas-pix-do-estado-gaucha.htm?>>. Consultado el: 3 de octubre de 2025.



Reembolsos a víctimas de estafas

El Proyecto de Ley 133/2022 propone modificar el Código de Protección al Consumidor para establecer normas de seguridad para los usuarios del Pix y crear mecanismos para la rápida recuperación de los fondos transferidos en caso de delitos contra la propiedad. El texto inicial del proyecto de ley preveía reembolsos a los consumidores por fondos transferidos indebidamente. Sin embargo, durante su revisión por la Comisión de Constitución, Justicia y Ciudadanía (CCJ), bajo el informe del senador Jorge Kajuru, el proyecto de ley añadió que los reembolsos solo se producirían si los fondos permanecían en cuentas bloqueadas (Senado, 2025).

Ante el aumento de las estafas, el Reino Unido adopta un modelo favorable al consumidor

En un avance hacia la protección del consumidor, el regulador de sistemas de pago del Reino Unido, *Payment Systems Regulator (PSR)*, ha establecido que, hasta un límite de £85,000, se debe garantizar a las víctimas el **reembolso completo** en un plazo máximo de cinco días. La norma, que entró en vigor en octubre de 2024, prevé una división de responsabilidad, con el reembolso dividido equitativamente (50-50) entre las instituciones financieras emisoras y receptoras.

Los reembolsos pueden ser denegados si el consumidor actúa con negligencia grave o no observa el estándar de cuidado requerido (pero corresponde al Proveedor de Servicios de Pago probar esta negligencia); esta excepción no puede aplicarse si el cliente es vulnerable.

El enfoque se centra en aumentar los mecanismos de seguridad de las instituciones y combatir activamente el fraude⁶⁹.

69. Puede encontrar más detalles sobre las normas de reembolso en el sitio web del Payment Systems Regulator (PSR). Disponible en: <<https://www.psr.org.uk/our-work/app-scams/>>. Consultado el: 3 de mayo de 2025.

Lente: Soberanía



Es común pensar en el dinero como una sola entidad: una unidad de valor utilizada para pagar y recibir pagos en cualquier lugar. Sin embargo, al observar la historia y el uso cotidiano del dinero, se revela que no es homogéneo. El dinero siempre ha adoptado diferentes formas y significados a lo largo del tiempo, y continúa cambiando.

Más que un medio de intercambio, el dinero es también un instrumento social y cultural. Refleja relaciones de poder, confianza y pertenencia⁷⁰. Un gobierno, por ejemplo, puede utilizar la emisión de moneda o el control de los sistemas de pago para afirmar su soberanía o influir en la economía. La confianza también es esencial: un billete de R\$100 o US\$100 se acepta porque se cree que también será aceptado por otros, incluso si no conlleva valor material en sí mismo. El dinero también puede crear o reforzar la pertenencia. Esto sucede cuando las comunidades inventan monedas locales para estimular el comercio entre sus miembros, cuando los programas de puntos y millas crean redes exclusivas de consumidores, o cuando las personas utilizan vales de comida o de transporte en sus rutinas laborales. **El dinero, en este sentido, no se limita al acto de “pagar y recibir”; revela circuitos de transacciones de valor, que tienen reglas que rigen quién participa, quién tiene poder y en quién se puede confiar.**

Incluso dentro de la economía formal, con monedas y billetes emitidos por el Estado, convivimos a diario con otras formas de transferir y almacenar valor. Las tarjetas de crédito, los puntos de programas de fidelización, las millas aéreas, el saldo de los teléfonos móviles y las criptomonedas son algunos ejemplos. En muchos contextos, todas funcionan como dinero. Se utilizan para intercambiar, comprar, comparar o almacenar valores, incluso si no son monedas en el sentido tradicional.

Con la digitalización, este abanico se ha ampliado aún más. Hoy en día, el dinero circula en aplicaciones bancarias, billeteras digitales, transferencias instantáneas (como el Pix) e incluso en redes globales que no pasan por los bancos tradicionales. Muchas personas pagan viajes a través de aplicaciones

⁷⁰. Un grupo de actores, desde una perspectiva socioantropológica, ha establecido debates que van más allá de las definiciones económicas formales del dinero, considerándolo como un artefacto social, cultural y político que expresa relaciones de poder, confianza y pertenencia. Por ejemplo, véanse Hart, 2007; Graeber, 2011; Zelizer, 1994; Maurer, 2015.

con *cashback*, intercambian millas por productos o usan saldo de sus teléfonos móviles para pagar servicios. Estas son formas de circulación de valor que funcionan como “dinero paralelo”, coexistiendo con lo que se considera dinero oficial.

Si seguimos la historia del dinero y de los “casi-dinero”, percibimos un camino largo y lleno de transformaciones. Se han usado como moneda promesas de pago, semillas, metales preciosos, monedas y billetes y, ahora, cada vez más, números en una pantalla. Este proceso demuestra cómo, en los últimos años, el dinero se ha vuelto más abstracto y menos ligado a los objetos físicos. Por lo tanto, hablar de “dinero” en singular, como si fuera una sola cosa, parece impreciso. En la práctica, vivimos en un ecosistema en constante cambio, donde diversas formas de dinero coexisten y cumplen diferentes funciones.

Ver el dinero de esta manera es esencial para comprender los debates actuales sobre nuevos métodos de pago, como el Pix. No se trata de una herramienta más que compite por espacio con las tarjetas o las transferencias tradicionales, sino que también forma parte de un cambio más amplio: una disputa sobre cómo se organizan las transacciones financieras, quién controla estas infraestructuras y cómo esto afecta la inclusión financiera, así como la soberanía de una nación.

La capacidad de emitir moneda, gestionar la cantidad de dinero en circulación, fijar las tasas de interés y establecer las leyes que rigen el sistema financiero nacional son ejemplos de acciones directamente vinculadas a la soberanía monetaria de un país. Controlar estas acciones permite al país implementar políticas de interés público – establecer sus prioridades – sin verse obligado a seguir las políticas definidas por otras jurisdicciones.

Al desarrollar el Pix, Brasil ejerció su autonomía monetaria al definir el rol del BCB como creador, regulador y operador del nuevo sistema de pagos, responsable de la gobernanza y la definición de estándares técnicos y de seguridad.

La decisión de utilizar una infraestructura pública, desde el inicio de la concepción del Pix, evitó el predominio de los sistemas privados, privilegiando los intereses colectivos y garantizando un método de pago libre, seguro y accesible.

El camino adoptado por Brasil, como reflejó Paul Krugman (2025), contrasta con la decisión de Estados Unidos, que prohibió la creación de una moneda digital coordinada por *Federal Reserve* y optó por incentivar las monedas digitales privadas, como las *stablecoins*⁷¹. Como evalúa el autor, la decisión de crear leyes para impedir el estudio e implementación de una moneda digital pública (*Central Bank Digital Currency* - CBDC) resalta la fortaleza del sector financiero en Estados Unidos. En la interpretación de Krugman, la adopción del Pix por miles de personas en un corto período de tiempo está vinculada a su método de pago rápido, seguro y gratuito, características que llevaron a muchos a preferir el nuevo método de pago sobre el efectivo y las tarjetas. Tal actuación amenazaría los intereses de las corporaciones privadas al oponerse a la idea profundamente arraigada de que el Estado no sería capaz de producir una solución eficiente. Finalmente, también señala que el éxito del Pix incluso cuestiona las criptomonedas, ya que estas, a pesar de ser fomentadas, aún no han alcanzado el mismo alcance y aceptación.

Disputas en torno al Pix

En julio de 2025, el gobierno de Estados Unidos, a través de la Oficina del Representante Comercial de Estados Unidos (USTR), anunció una investigación formal sobre las prácticas comerciales digitales de Brasil, entre ellas, un enfoque en el sistema brasileño de pagos digitales. Este anuncio tensó aún más las relaciones entre Estados Unidos y Brasil, ya que se produjo pocos días después de que Donald Trump anunciara que impondría aranceles del 50% a todas las importaciones de Brasil⁷².

Estas decisiones se basaron en argumentos políticos y comerciales. Inicialmente, el arancel impuesto por Trump estaba políticamente justificado, con el objetivo de presionar al gobierno brasileño para que detuviera los procedimientos legales contra Jair Bolsonaro, quien luego fue acusado de intento de golpe de estado. Las críticas dirigidas al Supremo Tribunal Federal revelaron la intención de Trump de acusar a la justicia brasileña de censurar las plataformas digitales estadounidenses.

La incorporación del Pix a la investigación, bajo acusaciones de prácticas anticompetitivas, intensificó aún más el conflicto diplomático y económico. La investigación sobre el sistema brasileño de pagos digitales, amparada por la

71. Véase el texto *Has Brazil Invented the Future of Money?*. Disponible en: <<https://paulkrugman.substack.com/p/has-brazil-invented-the-future-of>>. Consultado el: 23 de julio de 2025.

72. Puede encontrar más información sobre la investigación en: <<https://ustr.gov/about/policy-offices/press-office/press-releases/2025/july/ustr-announces-initiation-section-301-investigation-brazils-unfair-trading-practices>>. Consultado el: 3 de octubre de 2025.

Sección 301 de la Ley de Comercio de Estados Unidos⁷³, buscaría identificar si la estructura del Pix, o su expansión, otorga ventajas desproporcionadas a las empresas brasileñas sobre sus competidores estadounidenses. La acusación de prácticas económicas desleales podría interpretarse como una forma de cuestionar la legalidad de la creación del Pix y frenar su uso.

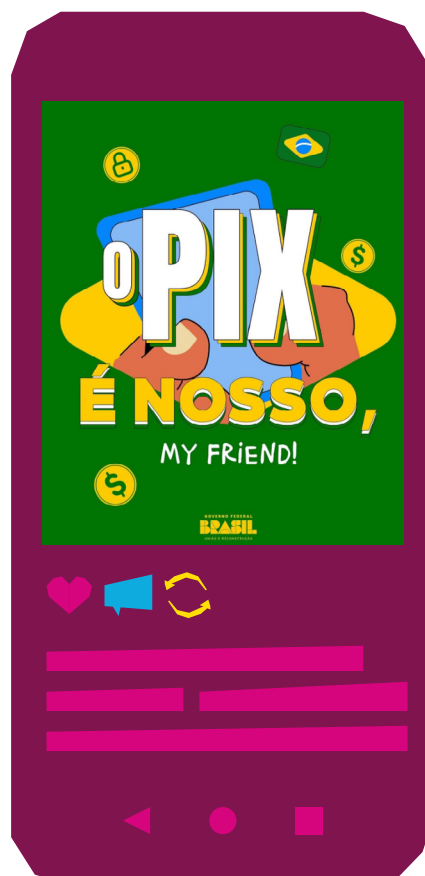
Temiendo que la información falsa generara inseguridad pública y nuevos rumores sobre los costos y las tarifas relacionados con Pix, el gobierno brasileño se apresuró a reafirmar su postura soberana⁷⁴. Las comunicaciones por radio, televisión y redes sociales reafirmaron que el funcionamiento del sistema no se vería afectado y que cualquier inquietud internacional se gestionaría a través de canales diplomáticos y multilaterales.

Figura 15. Ilustración con tema “Pix es de Brasil”



Fuente: Adaptado de Perfil de Instagram @lulaofical, 2025.

Figura 16. Ilustración del Gobierno Federal de Brasil con tema “el Pix es nuestro”



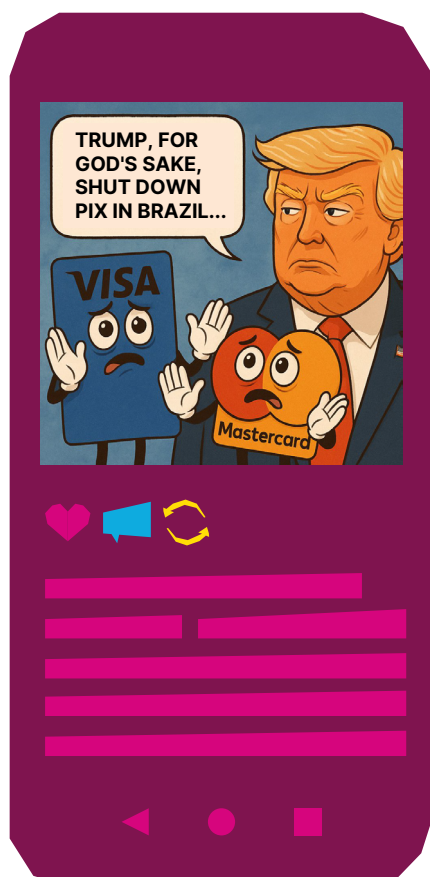
Fuente: Adaptado de Perfil de Instagram @govbr, 2025.

73. En resumen, la Sección 301 de la Ley de Comercio de 1974 permite al gobierno de Estados Unidos responder a prácticas comerciales desleales en otros países.

74. Más información disponible en: <<https://agenciabrasil.ebc.com.br/economia/noticia/2025-07/pix-e-modelo-e-problema-real-esta-em-tarifas-dos-eua-diz-alcckmin>>. Consultado el: 3 de octubre de 2025.

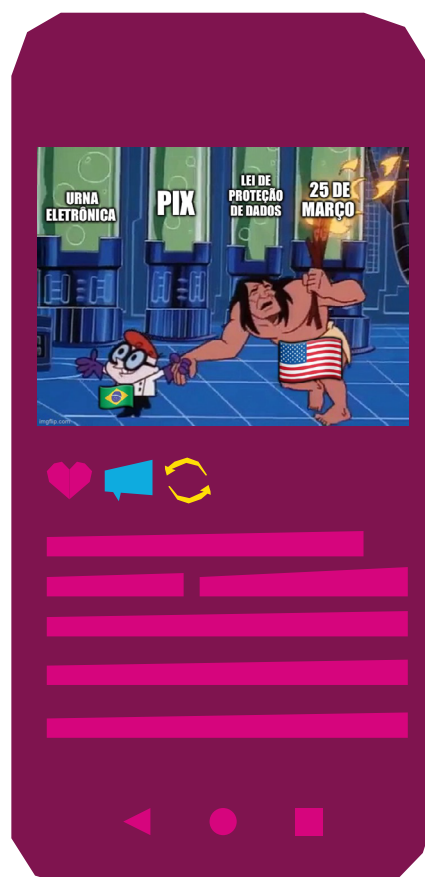
El gobierno adoptó un estilo de comunicación que alternaba entre tonos asertivos e irónicos, enfatizando que el Pix es “un patrimonio” del pueblo brasileño (Figuras 15 y 16)⁷⁵. Memes y otras expresiones proliferaron en redes sociales (Figuras 17 y 18), resaltando el orgullo por la infraestructura de pagos creada por el BCB y demostrando una postura de defensa colectiva ante la supuesta interferencia estadounidense.⁷⁶

Figura 17. Viñeta satírica ilustrando las quejas de las Big Techs del sector financiero



Fuente: imagem extraída de redes sociais

Figura 18. Viñeta satírica ilustrando la presentación de creaciones brasileñas a EE. UU.



Fuente: imagem extraída de redes sociais

75. Disponible en: <<https://www.instagram.com/lulaoficial/p/DMTb0ytO8jl/>> y <<https://www.instagram.com/p/DMLKn6xfx-o/>>. Consultado el: Julio de 2025.

76. Las figuras 17 y 18 fueron tomadas de Instagram, pero no indican la autoría. Disponibles en: <https://www.instagram.com/p/DMNbecqu6or/?img_index=7>. Consultado el: Agosto de 2025.

En un discurso oficial a la nación, el presidente Lula calificó los ataques a las instituciones brasileñas de “chantaje” y afirmó que el país no renunciaría a su soberanía. Añadió que utilizaría todos los instrumentos legales para defender la economía brasileña⁷⁷.

El Pix pertenece a Brasil. No aceptaremos ataques al Pix, que es un patrimonio de nuestro pueblo. Contamos con uno de los sistemas de pago más avanzados del mundo y lo protegeremos.
(Agência Gov, 2025)

Este episodio refleja una escalada de disputas en el ámbito político, comercial y tecnológico, donde Pix representa no solo la autonomía financiera nacional, sino también un símbolo del poder digital emergente.

Valores cobrados y datos transaccionados

El análisis de las prácticas comerciales en torno a Pix abre debates en dos frentes: el primero se refiere a las comisiones cobradas por el procesamiento de transferencias y pagos; el segundo, a los datos generados por las transacciones, que también se convierten en productos.

La decisión del gobierno brasileño de crear un método de pago interoperable y gratuito impulsó la aceptación del Pix, reemplazando rápidamente otros métodos. Con el Pix, los consumidores ahora tienen más opciones para realizar transacciones sin comisiones anuales ni comisiones por transferencia, tanto en tiendas físicas como en línea.

Las diversas funcionalidades incluidas en la agenda evolutiva del Pix han permitido que el sistema reemplace progresivamente no solo el efectivo, sino también las tarjetas de débito y crédito. Los comercios, a su vez, también han visto una ventaja en la adopción del Pix, ya que se benefician de la reducción de intermediarios y, en consecuencia, de los costos de la mediación de pagos.

En este sentido, Luca Belli (2025a) describe el Pix como un ejemplo de “buena soberanía digital”, dado que su creación rompió el fuerte duopolio de las

77. El discurso completo del presidente Lula se puede encontrar en: <<https://agenciagov.ebc.com.br/noticias/202507/pronunciamento-do-presidente-lula-brasil-soberano>>. Consultado el: 3 de octubre de 2025.

empresas Visa y Mastercard, que anteriormente eran las únicas compañías capaces de procesar pagos electrónicos las 24 horas del día, los 7 días de la semana, en el país⁷⁸. Como señala el investigador, la intermediación de pagos a través de las redes de estas empresas implicaba que, por cada transacción, entre el 3% y el 5% del valor se destinara a Visa o MasterCard⁷⁹.

Además, Belli (2025a) también señala que Visa y Mastercard almacenan datos de transacciones. Parte de los ingresos de estas empresas también proviene del análisis y la venta de los datos que recopilan. En este ámbito, las finanzas y la información se entrelazan⁸⁰.

En un mundo digitalizado, los datos ocupan un lugar central en la economía digital (Jiang; Belli, 2025), constituyendo fuentes valiosas para definir estrategias económicas. Por lo tanto, es fundamental reflexionar sobre la gobernanza de los datos, sus métodos de almacenamiento y los principales permisos de uso. Desarrollar dicha gobernanza requiere un esfuerzo para crear normas con validez nacional e internacional. En este sentido, el gobierno brasileño abrió recientemente una consulta pública sobre la creación de una “Política de Gobernanza e Intercambio de Datos” con el objetivo de fortalecer la Infraestructura Nacional de Datos (IND)⁸¹. Como señala Belli (2025b), muchos países terminan convirtiéndose en exportadores e importadores de datos de soluciones y servicios digitales desarrollados a partir de los datos generados dentro de sus territorios. En este sentido, la cuestión de quién genera los datos y quién tiene derecho a usarlos es ineludible en este momento. Y es precisamente en este punto donde la tecnología Pix entra en conflicto con los intereses de las *Big Techs*.

78. Luca Belli profundiza en el debate sobre la soberanía digital en el marco del proyecto *CyberBRICS*. Para obtener más información, visite el sitio web del proyecto: <https://cyberbrics.info/>.

79. Un resumen de la conferencia “A importância da economia de dados para desenvolver a soberania digital”, del investigador Luca Belli, se puede encontrar en <<https://www.estadao.com.br/economia/pix-soberania-digital-exemplo/>>. Consultado el: 26 de julio de 2025.

80. Disponible en: <<https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia>>. Consultado el: 26 de julio de 2025.

81. Disponible en: <<https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/julho/governo-abre-consulta-publica-sobre-a-criacao-da-politica-de-governanca-e-compartilhamento-de-dados#:~:text=A%20IND%20%C3%A9%20um%20conjunto,entidades%20do%20Poder%20Executivo%20Federal>>. Consultado el: 2 de agosto de 2025.

Pix y WhatsApp Pay

Cerca del lanzamiento del Pix, se lanzó en Brasil la función de pagos a través de *WhatsApp*. Con esta nueva función, los usuarios de la app de mensajería podían registrar un método de pago y, con ello, habilitar la función de envío de dinero⁸². La función, vinculada a *Meta Pay*⁸³, se promocionó como una forma rápida y segura de enviar y recibir dinero: “tan fácil como enviar un mensaje”⁸⁴. Usando el icono de pago de *WhatsApp*, sería posible transferir fondos a contactos personales o empresas, sin necesidad de descargar una nueva aplicación.

El lanzamiento en junio de 2020, tan cerca de la llegada del sistema Pix, generó repercusiones y planteó interrogantes entre los actores del sistema financiero brasileño. Esta medida permitiría a Meta unirse al mercado de métodos de pago, que manejaba grandes sumas de dinero en Brasil. Dada la importancia de *WhatsApp* como la aplicación móvil más utilizada por los brasileños⁸⁵, Meta estaba interesada en implementar un sistema que ya se estaba probando en India, pero que enfrentaba obstáculos regulatorios allí.⁸⁶ Con el anuncio de la operación, los brasileños serían los primeros en utilizar la funcionalidad⁸⁷. Basada en las transacciones entre usuarios de *WhatsApp* y empresas, la función de pagos transformaría el proceso de compra del consumidor al eliminar la necesidad de lectores de tarjetas. El enfoque se centró en la comodidad de las transacciones, ya que se permitiría comprar

82. En el momento del lanzamiento, las operaciones de pago podían realizarse usando tarjetas de débito y crédito de las marcas Visa y Mastercard emitidas por Banco do Brasil, Nubank y Sicredi.

83. *Meta Pay* es la plataforma de pagos digitales de Meta, que en el momento de su lanzamiento se llamaba *Facebook Pay*.

84. El video que explica su funcionamiento se puede acceder en: <<https://www.meta.com/pt-br/meta-pay/#:~:text=Centrais%20de%20Ajuda%20dos%20apps&text=O%20Meta%20Pay%20%C3%A9%20uma,de%20enviar%20dinheiro%20no%20WhatsApp.&text=Envie%20dinheiro%20para%20amigos%20e,voc%C3%AA%20n%C3%A3o%20precise%20se%20preocupar>>. Consultado el: 3 de octubre de 2025.

85. Datos publicados por Similarweb. Más información en: <<https://www.similarweb.com/pt/top-apps/google/brazil/>>

86. Para más detalles, consulte: <<https://www.uol.com.br/tilt/noticias/reuters/2020/11/06/india-limita-pagamentos-digitais-e-afeta-google-walmart-e-facebook.htm>>. Consultado el: 3 de octubre de 2025.

87. En ese momento, con aproximadamente 120 millones de personas usando *WhatsApp* (casi el 60% de la población brasileña), el país fue seleccionado por *Facebook* para lanzar el servicio en el área de pagos digitales.

y vender a través de la propia aplicación. El lanzamiento también anunció que no habría comisiones por enviar y recibir dinero a amigos y familiares. Sin embargo, las empresas que utilicen el sistema deberán tener una cuenta registrada de *WhatsApp Business* y pagar una comisión de procesamiento para recibir pagos de los clientes⁸⁸.

La iniciativa se difundió ampliamente como una potencial revolución para el comercio minorista y los microempresarios, pero enfrentó desafíos legales y de mercado. Por ello, una semana después de su lanzamiento, el BCB ordenó la suspensión de la operación, solicitando a Visa y Mastercard que suspendieran los pagos a través de WhatsApp bajo pena de sanciones y multas. La decisión se justificó por la necesidad de evaluar los riesgos y preservar un entorno competitivo adecuado. El texto también destacó el interés de la agencia en priorizar un sistema de pagos que fuera interoperable, rápido, seguro, transparente, abierto y asequible⁸⁹. De igual manera, el Consejo Administrativo de Defensa Económica (CADE) de Brasil bloqueó la alianza de *Facebook* con Cielo (responsable del sistema de pagos de *WhatsApp*), dado que el operador controlaba aproximadamente el 40% de las transacciones electrónicas del país. La decisión destacó el riesgo de concentración del mercado resultante de la combinación del amplio alcance de *WhatsApp*, con su gran número de usuarios, y el poder de mercado de Cielo. Inicialmente, la posibilidad de un contrato de exclusividad entre ambas compañías se consideró un riesgo competitivo⁹⁰.

Al mismo tiempo, el BCB finalizaba el desarrollo del Pix, que ya se encontraba en fase de pruebas y su lanzamiento estaba previsto para octubre y noviembre de 2020. Con la decisión regulatoria, WhatsApp Pay quedó fuera del mercado en un momento crucial. Nueve meses después de la suspensión, *Facebook Pagamentos do Brasil* fue aprobada como “iniciador de pagos”. Sin embargo, *WhatsApp Pay* no logró consolidarse.

88. Según el folleto “Confira tudo o que você precisa saber sobre WhatsApp Pay (Descubre todo lo que necesitas saber sobre WhatsApp Pay)”, elaborado por Sebrae para comercios, la comisión establecida por WhatsApp Pay equivaldría al 3,99 % del importe recibido. El importe pagado por el cliente estaría disponible en la cuenta del comercio en dos días. Disponible en: <<https://sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/PE/Anexos/Confira%20tudo%20o%20que%20você%20precisa%20saber%20sobre%20WhatsApp%20Pay%20%281%29.pdf>>. Consultado el: 30 de agosto de 2025.

89. La nota emitida por el Banco Central está disponible en: <<https://www.bcb.gov.br/detalhenoticia/17108/nota>>. Consultado el: 3 de octubre de 2025.

90. Cabe destacar que Cade revocó la decisión cautelar poco después. Sin embargo, el servicio permaneció suspendido por orden del Banco Central de Brasil. Puede encontrar más información sobre la decisión de Cade y la demanda en: <<https://www.gov.br/cade/pt-br/assuntos/noticias/cade-revoga-suspensao-de-parceria-entre-facebook-e-cielo-para-pagamentos-por-whatsapp>>. Consultado el: 3 de agosto de 2025.

Big Techs y el sistema financiero brasileño

La entrada de *Big Techs* en el sistema financiero es una verdadera preocupación, ya que estas empresas tecnológicas comenzarían a recopilar una amplia gama de datos, que podrían combinar, por ejemplo, información personal, social, geográfica y financiera. Esto amplía aún más su poder, especialmente en lo que respecta a la minería de datos y su posible influencia en el comportamiento del consumidor.

La capacidad de las *Big Techs* para recopilar y agregar datos tan importantes a gran escala podría llevarlas a ganar una posición de mercado que dejaría sin margen a la competencia⁹¹. Esta concentración de poder podría, a corto plazo, convertirse en un monopolio, con el riesgo de prácticas abusivas.

Además, las *Big Techs* representan un desafío significativo para la supervisión y regulación, en particular por parte del Banco Central. Dado que operan en diferentes segmentos del mercado, las iniciativas regulatorias requerirían la integración de múltiples sectores, considerando las normas del sistema financiero, la protección de datos, la protección del consumidor y la competencia. La coordinación nacional e internacional también sería necesaria, dado el alcance de sus servicios. Las fuerzas económicas y políticas de estas corporaciones las colocan en una posición tan privilegiada que pueden desafiar estructuras legales y democráticas de los países en los que operan. Precisamente la concentración y el almacenamiento de datos tan significativos por parte de empresas extranjeras plantea la cuestión de la soberanía. En este caso: ¿la infraestructura de pagos brasileña debería ceder tanto espacio a empresas fuera de su regulación directa? ¿O este sistema debe ser tratado como infraestructura pública esencial, capaz de promover la inclusión social y la reducción de desigualdades?

Para que se logre una soberanía financiera digital en Brasil, será necesario estar atento tanto a la hegemonía tecnológica extranjera como al poder regulatorio del Estado brasileño, que debe ser reconocido como autónomo y respetado a través de sus instituciones. El consenso en torno a la importancia del control sobre activos estratégicos - digitales, judiciales, financieros y ecológicos - es cada vez más crucial como parte esencial del proyecto de soberanía.

91. Un artículo de la *UN Trade & Development*, menciona la creciente competencia entre los líderes del mercado digital. Disponible en: <<https://unctad.org/news/highly-concentrated-digital-markets-put-consumers-risk-heres-how-change-course?>>. Consultado el: 3 de octubre de 2025.

Consideraciones Finales

Inclusión financiera y digital para todos

Aunque las estadísticas del Pix confirman la adopción de la herramienta por la sociedad, es necesario prestar atención a la exclusión de una parte significativa de la población que posee un dominio limitado de las tecnologías digitales. Las personas menos familiarizadas con el entorno virtual pueden estar recurriendo a redes de apoyo informales para realizar transacciones vía Pix. Esta dependencia de algunos usuarios de la ayuda de familiares, amigos, vecinos o incluso desconocidos, si bien inicialmente facilita el acceso, expone a estos usuarios a riesgos considerables. La falta de autonomía en la gestión de aplicaciones digitales debilita a las personas, haciéndolas más susceptibles a la explotación financiera.

En este contexto, es crucial que los instrumentos de pago digitales, así como las aplicaciones bancarias, consideren los desafíos de los usuarios e incorporen las cuestiones de usabilidad. La interfaz y la arquitectura de la información deben diseñarse de forma intuitiva y accesible, considerando los distintos grados de habilidades digitales de los usuarios, así como su falta de ellas. Aunque sea un equilibrio difícil de alcanzar, es fundamental conjugar la facilidad de uso con la seguridad de las aplicaciones.

También conviene recordar que mitigar la brecha digital y financiera requiere una acción proactiva por parte de los agentes del sistema financiero y los organismos gubernamentales. Las alianzas público-privadas para el desarrollo y la promoción de estructuras educativas integrales son clave para combatir la exclusión. Las iniciativas de alfabetización digital y financiera, que abarcan desde los fundamentos de la seguridad en línea hasta el uso adecuado del Pix, son esenciales para empoderar a la población. Otra clave es la provisión de múltiples canales de atención al usuario que trasciendan el entorno digital e incluyan soporte presencial y telefónico accesible.

El Pix solo será una herramienta eficaz para la inclusión financiera si es accesible y segura para toda la población brasileña.

Además de las preocupaciones sobre la usabilidad, considerando las diversas características de la población y sus necesidades específicas, otro factor importante es la inclusión en sus diversos formatos. En el caso del Pix, la obligatoriedad del uso de smartphones y la conexión a internet son motivos importantes para la no adopción de la solución de pago o para una adopción limitada. Por lo tanto, mantener otros métodos de pago es esencial para garantizar que los usuarios siempre tengan opciones. La disponibilidad de diferentes métodos de pago para la población debe entenderse como un derecho, ya que garantiza la libertad de elección y la independencia. Reemplazar el efectivo físico por dinero digital puede traer muchas ventajas, pero esto no significa que todos se beneficien por igual.

Los billetes, por ejemplo, constituyen históricamente un medio de pago estable, seguro y capaz de garantizar privacidad. El efectivo es fácil de usar, no tiene comisiones y requiere conceptos numéricos simples. En general, es un medio de pago sin exclusiones. Las transacciones electrónicas, como el Pix, requieren requisitos como alfabetización, acceso a una cuenta bancaria, internet y *smartphones*, así como la necesidad de conocimiento e integración en un entorno digital. Una economía sin efectivo puede terminar abandonando a los ciudadanos menos integrados con la tecnología, como las personas mayores, las personas sin hogar, las personas con bajo nivel educativo o quienes viven en zonas con menor acceso a infraestructuras.

Garantizar que los establecimientos comerciales acepten diferentes formas de pago, sin distinción de importe, debe ser una prioridad para asegurar la inclusión de todos en la economía. Un país con desigualdades sociales y económicas tan significativas como Brasil necesita combinar el avance tecnológico con la garantía real de la integración de las personas.

Construcción de una confianza real

La creciente sofisticación de las tácticas de los ciberdelincuentes, impulsada por el uso de tecnologías avanzadas, permite el acceso remoto a sistemas institucionales y, en consecuencia, a información confidencial. La disponibilidad de datos personales filtrados en el país ha impulsado el desarrollo de estafas más complejas, exponiendo a riesgos a personas de diferentes edades y niveles educativos. Los casos recurrentes de fraude y estafas resaltan la necesidad de integrar la ciberseguridad como un pilar estratégico en las agendas de empresas, organizaciones y gobiernos.

El uso de datos personales reales para perpetrar estafas financieras a través del Pix está demostrando ser un factor crítico, ya que otorga legitimidad a los estafadores y dificulta la detección de actividades delictivas. Esta conexión

directa entre el robo de datos a gran escala y la puesta en práctica de estafas pone de relieve la intrincada cadena del cibercrimen, en la que la violación inicial de la privacidad facilita la ocurrencia de pérdidas financieras directas, subrayando la urgente necesidad de medidas eficaces de protección de datos y rendición de cuentas para mitigar este ciclo fraudulento.

Dada la complejidad del escenario, la protección individual del consumidor se vuelve cada vez más difícil. **Asignar al usuario la responsabilidad exclusiva de identificar estafas y fraudes es una tarea abrumadora, que a menudo excede sus capacidades y requiere un nivel desproporcionado de experiencia.** La creciente complejidad de las actividades delictivas dificulta su detección para el consumidor promedio, convirtiéndolo en el eslabón más vulnerable de la cadena.

Las instituciones financieras deben asumir la responsabilidad de la protección integral del consumidor, dada su experiencia en evaluación de riesgos y seguridad de la información. Sus responsabilidades también incluyen garantizar la integridad de sus sistemas y las transacciones realizadas por sus clientes, lo que implica adoptar medidas proactivas para detectar y bloquear actividades sospechosas, así como implementar sistemas de alerta eficaces. Esta responsabilidad también incluye brindar el apoyo y la asistencia adecuados en casos de fraude y estafas, asegurando que las inquietudes de los usuarios se aborden con cuidado y eficiencia.

Es fundamental que las personas cuenten con procedimientos de denuncia sencillos y accesibles, que garanticen la claridad sobre qué hacer si son víctimas de estafas y fraudes. Necesitan un servicio rápido, atento y estandarizado. Una política de compensación con criterios transparentes es crucial para mitigar la incertidumbre en este proceso. Además, son importantes las reformas legislativas que aclaran y refuerzan la responsabilidad de las instituciones financieras en casos de fraude y estafas, especialmente en el entorno digital. Al fin y al cabo, es deber de las empresas proteger a sus usuarios.

Cuando las personas encuentran dificultades para reportar una estafa, pasando por extensas investigaciones antes de obtener el reembolso, puede generar incomodidad y la revictimización de la parte afectada. Por lo tanto, es importante simplificar el acceso a los mecanismos de resolución de disputas, garantizando que las quejas de las víctimas se gestionen de forma justa y rápida.

Las comparaciones con experiencias internacionales pueden orientar el debate sobre la asignación de responsabilidad por pérdidas derivadas del fraude financiero. El Reino Unido, como se mencionó anteriormente, ha implementado nuevas regulaciones que proponen compartir la responsabilidad por las estafas

de APP (*Authorized Push Payment*) entre los bancos emisores y receptores⁹². En este sentido, se espera que los bancos reembolsen a las víctimas, excepto en casos de negligencia grave demostrada. Este cambio regulatorio, motivado por el aumento significativo de las estafas de APP, en las que se induce a los consumidores a autorizar pagos a los estafadores, representa un cambio significativo en el modelo de responsabilidad, trasladando una mayor carga a las instituciones financieras en la prevención y compensación de estos fraudes. El *Payment Systems Regulator* (PSR) del Reino Unido apoya esta medida como una forma de impulsar la inversión en seguridad y el intercambio de información para identificar y bloquear las cuentas de los estafadores.

La creación de índices y clasificaciones comparativos que informen sobre las mejores prácticas en seguridad de la información y apoyo a las víctimas en casos de estafas es una alternativa complementaria para que los consumidores comprendan a las empresas con las que interactúan y tomen decisiones basadas en criterios relevantes. La confianza es una construcción diaria, fundamentada en prácticas constantes de seguridad, soporte y justicia.

En resumen, la integración exitosa de los sistemas de pago electrónico en la sociedad depende de los esfuerzos para construir activamente la confianza. Esta confianza se basa en sistemas seguros y confiables y en el compromiso de las instituciones financieras de proteger y apoyar a sus usuarios.

Infraestructuras digitales como territorio de disputas

Finalmente, vale la pena señalar que el caso del Pix demuestra que la soberanía financiera de un país no se limita únicamente al control de la emisión monetaria, sino que también involucra la capacidad de desarrollar y gestionar las infraestructuras digitales que sostienen la circulación de valores. Al crear un sistema público, gratuito e interoperable, Brasil fortaleció su autonomía de los intereses privados y extranjeros, demostrando que el Estado puede brindar soluciones eficientes, seguras e inclusivas.

Sin embargo, los recientes episodios de tensiones diplomáticas y comerciales con Estados Unidos, así como la presión ejercida por las *Big Techs*, refuerzan la idea de que la soberanía no es un hecho, sino un proceso en constante disputa. En este contexto, el control sobre los datos, los estándares técnicos y los

92. Para más información sobre las normas de protección implementadas en el Reino Unido, consulte: <<https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/>>. Consultado el : 8 de octubre de 2025.

acuerdos de mercado se convierte en una decisión estratégica, directamente vinculada a la lucha por la autonomía digital y económica.

Para que esta soberanía se consolide efectivamente, se requiere avanzar en dos frentes complementarios. Institucionalmente, es fundamental fortalecer la gobernanza del Pix, aumentando la transparencia y, fundamentalmente, la participación de diferentes sectores de la sociedad civil y la academia en el Foro Pix. También es fundamental mejorar la coordinación entre el BCB, el CADE, la Autoridad Nacional de Protección de Datos (ANPD) y las agencias de protección al consumidor para abordar los riesgos de competencia y los abusos en la explotación de datos financieros. La soberanía financiera digital también depende de la capacidad de reducir las dependencias externas, lo que implica inversiones en el desarrollo nacional de tecnologías, estándares de seguridad e infraestructura de datos. Al mismo tiempo, la política exterior debe incorporar la dimensión de la diplomacia digital, consolidando alianzas regionales y multilaterales para proteger las infraestructuras públicas de pagos de las presiones comerciales externas.

En el ámbito social, consolidar el Pix como un bien público requiere la defensa inquebrantable de su carácter gratuito y accesible, con mecanismos de protección eficaces contra el fraude y el abuso. Asimismo, la educación financiera y digital debe ser una prioridad, garantizando que las poblaciones más vulnerables puedan utilizar los medios digitales de forma independiente y segura.

Referencias

ALFABETISMO FUNCIONAL. **Dados INAF 2024**. 2024. Disponible en: <<https://alfabetismo-funcional.org.br/dados-inaf-2024.pdf>>. Consultado el: 4 de octubre de 2025.

CENTRAL BANK OF BRAZIL **Circular BCB nº 3.100, de 28 de março de 2002**. Brasília, DF: BCB, 2002. Disponible en: https://www.bcb.gov.br/pre/normativos/circ/2002/pdf/circ_3100_v5_1.pdf. Consultado el: 4 de octubre de 2025.

_____. **Relatório de inclusão financeira**, n. 1. Brasília, DF: BCB, 2010.

_____. **Relatório de Vigilância do Sistema de Pagamentos Brasileiro 2013**. Divisão de Atendimento ao Cidadão, Deati/Diate. Brasília, DF: 2014. Disponible en: https://www.bcb.gov.br/content/estabilidadefinanceira/spb_docs/RELATORIO_DE_VIGILANCIA_SPB2013.pdf. Consultado el: 4 de octubre de 2025.

_____. **Agora é pra valer! Lançamento do Pix #AgoraéPix**. Youtube. 16 de novembro de 2020. Disponible en: <<https://www.youtube.com/watch?v=0Xkv-e46hJQ>>. Consultado el: 3 de octubre de 2025.

_____. **Relatório de Gestão do Pix**. Concepção e primeiros anos de funcionamento 2020-2022. Brasília, DF: 2023. Disponible en: <https://www.bcb.gov.br/content/estabilidadefinanceira/pix/relatorio_de_gestao_pix/relatorio_gestao_pix_2023.pdf>. Consultado el: 2 de octubre de 2025.

_____. **LiveBC celebra os quatro anos do Pix**. Brasília, DF, 2024a. Disponible en: <<https://www.bcb.gov.br/detalhenoticia/20425/noticia>>. Consultado el: 3 de enero de 2025.

_____. **O brasileiro e sua relação com o dinheiro**. Brasília, DF: 2024b. Disponible en: <https://www.bcb.gov.br/content/cedulasemoedas/pesquisabrasileirodinheiro/Apresentacao_brasileiro_relacao_dinheiro_2024.pdf>. Consultado el: 7 de enero de 2025.

_____. **SPB — Adendos**. [S. l.]: Banco Central do Brasil. Disponible en: <https://www.bcb.gov.br/estatisticas/spbadendos?ano=2024>. Consultado el: 2 de octubre de 2025.

BRASIL. **Pix se consolida como meio de pagamento mais usado pelos brasileiros**. Governo Federal, 22 nov. 2022. Disponible en: <<https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/11/pix-se-consolida-como-meio-de-pagamento-mais-usado-pelos-brasileiros>>. Consultado el: 2 de octubre de 2025.

BELLI, Luca. **Da soberania digital à soberania em IA**. Jota. 26 de fev. 2025a. Disponible en: <<https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/da-soberania-digital-a-soberania-em-ia>>. Consultado el: 2 de octubre de 2025.

_____. **Leveraging data economy across the BRICS' digital economy community** - CGETI webinar. MDIC Youtube. 18 mar. 2025b. Disponible en: <https://www.youtube.com/live/AATFcBhV6_A>. Consultado el: 20 de abril de 2025.

CORNELLI, Giulio; FROST, Jon; GAMBACORTA, Leonardo; SINHA, Sonalika; TOWNSEND, Robert M. **The organisation of digital payments in India – lessons from the Unified Payments Interface (UPI)**. In: BANK FOR INTERNATIONAL SETTLEMENTS (BIS). *Faster digital payments: global and regional perspectives*. Basel: Bank for International Settlements, 2024. (BIS Papers, n. 152).

FEBRABAN. **Relatório Anual 2009**. Federação Brasileira de Bancos, São Paulo: Sp, 2009. Disponível em: <https://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7IOaSDf9jyV/si-tefebraban/Febraban_completo.pdf>. Consultado em: 5 de outubro de 2025.

_____. **Pix foi o meio de pagamento mais usado no Brasil em 2024**; TED liderou em valores transacionados. Federação Brasileira de Bancos, São Paulo. Disponível em: <<https://portal.febraban.org.br/noticia/4290/pt-br/#:~:text=O%20Pix%20encerrou%20o%20ano,pa%-C3%ADs%20em%20um%20levantamento%20anual>>. Consultado em: 2 de outubro de 2025.

FEBRABAN/IPESPE. **Radar Febraban**. Pesquisa Trimestral. Março, 2025. Disponível em: <https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Relatório_Radar%20Febraban_Março_vf.pdf?_gl=1*ebin3a*_gcl_au*NTkzODIyOTc1LjE3NTQ4NjQzMdA.*_ga*NzA2NTQ1NjQyLjE3NTQ4NjQyOTI.*_ga_3W8FJ1CTT6*cze3NTk4ODQ2MDIkbzEzJ-GcwJHqXNzU5ODg0NjAyJGo2MCRsMCRoNDg2NTg1NTg0>. Consultado em: 6 de julho de 2025.

FERNANDES, Viviane. **Cuidando da Saúde Financeira**: uma etnografia sobre endividamento. 2019. 285 f. Tese (doutorado) – Universidade Federal do Rio de Janeiro, Museu Nacional. Programa de Pós-graduação em Antropologia social, 2019.

FOUILLET, Cyril; GUÉRIN, Isabelle; SERVET, Jean-Michel. Demonetization and digitalization: The Indian government's hidden agenda. **Telecommunications Policy**, v.45, n. 2, 2021.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2024. Disponível em: <https://publicacoes.forumseguranca.org.br/items/f62c4196-561d-452d-a2a8-9d33d1163af0>. Consultado em: 3 de outubro de 2025.

_____. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/123456789/279>. Consultado em: 3 de outubro de 2025.

FISERV. **Fiserv Insights: Pix e as Novas Modalidades Sob a Ótica do Cliente**, 2024. Disponível em: <<https://www.fiserv.com.br/pesquisa-pix-insights-2024-fiserv/>>. Consultado em: 6 de junho de 2025.

FREITAS, Neli. Compreendendo e abordando o impacto emocional da fraude financeira. **BioCatch blog channel**, 18 de junho, 2024. Disponível em: <<https://www.biocatch.com/pt-br/blog/lidando-com-o-impacto-emocional-da-fraude-financeira>>. Consultado em: 3 de agosto de 2025.

GASA. **Golpes Digitais no Brasil**. Global Anti-Scam Alliance: 2024. Disponible en: <<https://www.gasa.org/research>>. Consultado el: 7 de agosto de 2025.

GRAEBER, David. **Debt: The First 5000 Years**. New York: Melville House, 2011.

HART, Keith. Money Is Always Personal and Impersonal. **Anthropology Today**, Vol. 23, No. 5. oct., 2007, pp. 12-16.

IPEA. **Brasil: acesso a serviços financeiros**. Rio de Janeiro: IPEA; Washington, DC: Banco Mundial, 2004.

JAYO, Martin. **Correspondentes bancários como canal de distribuição de serviços financeiros: taxonomia, histórico, limites e potencialidades dos modelos de gestão de redes**. 2010. Tese (doutorado) em Administração de Empresas. Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas, São Paulo, 2010.

JIANG, M.; BELLI, L. **Digital Sovereignty in the BRICS Countries**. How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge: UK, Cambridge University Press & Assessment, 2025.

LAZARUS, Jeanne. Gouverner les conduites par l'éducation financière. L'ascension de la Financial Literacy. In: Dubuisson-Quellier, Sophie (ed.), **Gouverner les conduites**. Paris: Presses de Sciences Po., 2016a.

LIMA, H.; FRANCISCO, E. Revolução nos meios de pagamento digitais. **GV Executivo**, v. 20, n. 1, jan/mar 2021. Fundação Getúlio Vargas. Disponible en: <https://periodicos.fgv.br/gvexecutivo/article/view/83454/79217>. Consultado el: October 14, 2025.

MAURER, Bill. **How Would You Like to Pay? How Technology is Changing the Future of Money**. Durham: Duke University Press, 2015.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Lançamento da Aliança Nacional de Combate a Fraudes Bancárias Digitais**. [Vídeo ao vivo], 18 fev. 2025. Disponible en: <https://www.youtube.com/live/5noXkhsUqGY>. Consultado el: 4 de octubre de 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br); Comitê Gestor da Internet no Brasil (CGI.br). **TIC Domicílios 2024: pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros** [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil, 2025. Disponible en: https://cetic.br/media/docs/publicacoes/2/20250512120132/tic_domicilios_2024_livro_eletronico.pdf. Consultado el: 4 de octubre de 2025.

SENADO FEDERAL. **CTFC analisa medidas com o objetivo de coibir golpes via Pix**. Senado, 10 fev. 2025. Disponible en: <https://www12.senado.leg.br/radio/1/noticia/2025/02/10/ctfc-analisa-medidas-com-o-objetivo-de-coibir-golpes-via-pix>. Consultado el: 4 de octubre de 2025.

SCHAPIRO Mario; MOUALLEM, Pedro, DANTAS, Eric. Pix: desvendando uma Fintech estatal, **Brazilian Journal of Political Economy**. Center of Political Economy, vol. 43, n. 4, 2023, p. 874-892.

SERASA EXPERIAN. **Relatório de Identidade Digital e Fraude 2024**. Serasa, 2024. Disponível em: <<https://www.serasaexperian.com.br/conteudos/relatorio-de-fraude-2024-consumidores-estao-dispostos-a-pagar-mais-carro-por-seguranca/>>. Consultado em: August 1, 2024.

SILVERGUARD. **Estudo Golpes com Pix**. Um mapeamento inédito sobre golpes financeiros via Pix no Brasil. 2023.

_____. **Estudo Golpes com Pix**. 2024. Disponível em: <<https://www.silverguard.com.br/>>. Consultado em: 7 de septiembre de 2025.

TREVISAN, F.; GONZALEZ, L.; DINIZ, E. E; CERNEV, T. F.; GONZALEZ, L., DINIZ, E. e CERNEV, A. **Geografia do Pix: Como o Sistema de Pagamentos Instantâneos Redesenha o Mapa Financeiro do Brasil**. FGV, 2025. Disponível em: <<https://eaesp.fgv.br/producao-intelectual/geografia-pix-como-sistema-pagamentos-instantaneos-redesenha-mapa-financeiro>>.

ZELIZER, Viviana. **The Social Meaning of Money: Pin Money, Paychecks, Poor Relief, and Other Currencies**. Princeton: Princeton University Press, 1994.

GOV.BR

gov.br

Gov.br

el portal único del
Estado Brasileño





Introducción

La trayectoria brasileña hacia el desarrollo de las IPD se entrelaza con la historia del desarrollo de las tecnologías computacionales en el país. En los últimos 60 años, Brasil ha acumulado una experiencia significativa en el uso de computadoras digitales electrónicas para el tratamiento de los datos personales de sus ciudadanas y ciudadanos. La creación del Servicio Federal de Procesamiento de Datos (Serpro) en 1964 hizo posible el establecimiento de una infraestructura informacional basada en dicha tecnología y, en consecuencia, su utilización en la formulación de diferentes políticas públicas desde entonces (Serpro, 2025).

La aparición del Serpro tuvo lugar en un contexto de ruptura democrática, pocos meses después del Golpe Empresarial-Militar de 1964 (Serpro, 2009). Durante la dictadura empresarial-militar, se intensificó el uso de la información para mantener el orden y el funcionamiento del aparato represivo del gobierno dictatorial. Este uso autoritario de la información generó preocupaciones respecto a las prácticas de vigilancia ejercidas por el Estado, lo que culminó en los primeros debates sobre la protección de datos personales en Brasil y moldeó el enfoque teórico desarrollado por juristas de la época (Zanatta, 2023).

Además del Serpro, el Gobierno Federal instituyó en 1974 la Empresa de Tecnología e Informaciones de la Seguridad Social (Dataprev), ampliando la infraestructura que hizo posible el desarrollo, entre 1970 y 2000, de lo que llegaría a denominarse gobierno electrónico en Brasil (Filgueiras y Lui, 2023, p. 45), con la oferta de diversos servicios de recopilación, clasificación, almacenamiento, recuperación y difusión de datos.

Mientras el Serpro gestionaba la información del Ministerio de Hacienda, especialmente la relacionada con la declaración del Impuesto sobre la Renta de las Personas Físicas (IRPF), la Dataprev pasó a administrar la nómina del Instituto Nacional del Seguro Social (INSS), la mayor de América Latina y el Caribe (Eaves, Mazzucato y Pagliarini, 2024). De este modo, las agencias y departamentos del Gobierno Federal adoptaron esta infraestructura informacional, que se remonta al período de la dictadura empresarial-militar, centralizando las operaciones de tratamiento de datos mediante sistemas computacionales digitales electrónicos.

Investigadores del UCL *Institute for Innovation and Public Purpose* identifican en el surgimiento de estas dos empresas estatales de tecnología de la información (TI) el inicio de la primera etapa del proceso de transformación digital del Estado brasileño, conformado por cinco etapas posteriores (Eaves, Vasconcellos y Rao, 2024 *apud* Eaves, Mazzucato y Pagliarini, 2024, p. 7). A continuación, se presenta una reelaboración de la periodización propuesta.

Histórico

Línea de tiempo en seis etapas:⁹³

Etapa 1. Institución de las empresas estatales de TI (1960-1980)

El Registro de Persona Física (RPF), conforme a la **Ley n.º 4.862 del 29 de noviembre de 1965**, fue transformado en el Catastro de Personas Físicas (CPF) a partir del **Decreto-Ley n.º 401 del 30 de diciembre de 1968**. Este número registral fue fundamental para iniciar, en 1968, el procesamiento informatizado de las declaraciones de ingresos de las y los brasileños.

Actualmente, el CPF funciona como un “número único nacional” para la Cédula de Identidad Nacional (CIN). Las empresas estatales de TI, como Serpro y Dataprev, dotaron al sector público brasileño de una capacidad tecnológica de largo plazo, conformando una base para futuras IPD (Eaves, Mazzucato y Pagliarini, 2024, p. 8). La historia de las IPD en Brasil se entrelaza, así, con la historia de la automatización del impuesto sobre la renta y de la seguridad social llevada a cabo por estas empresas estatales de TI.

Etapa 2. Arquitectura de datos estructurales (1990)

El Sistema de Administración de Recursos de Información e Informática (SISP) fue instituido en 1994, por medio del **Decreto n.º 1.048**, con el objetivo de organizar la operación, el control, la supervisión y la coordinación de los recursos de TI de la administración directa, autárquica y fundacional del Poder Ejecutivo Federal (Brasil, 1994).

Más allá de la declaración del impuesto sobre la renta, el CPF se convirtió en un documento de identificación tan importante como el Registro General (RG). Dado que el RG - principal documento de identificación de las ciudadanas y los ciudadanos brasileños - es expedido por las unidades federativas (Estados y

93. Esta línea de tiempo reproduce y complementa la periodización mencionada anteriormente.

Distrito Federal), el CPF terminó desempeñando una función de identificación complementaria, convirtiéndose en el único registro nacional.

A finales de la década de 1990, hubo un intento de creación de un sistema único de identificación civil, denominado Registro de Identidad Civil (RIC), que reuniría diversos otros documentos que anteriormente se utilizaban como comprobación de identidad (Brasil, 1997; Bioni et al., 2022).

En 1995, se publicó la Orden Interministerial MCT/MC n.º 147, por la que se creaba el Comité Gestor de Internet en Brasil (CGI.br). Aunque fue instituido por una orden interministerial, el CGI.br es un comité de naturaleza sui generis y con participación multisectorial, por lo que no es un órgano vinculado al poder público. Desde entonces, las políticas públicas de TI pasaron de ser “(...) esfuerzos aislados a una estructuración de sistemas de datos más amplios” (Eaves, Mazzucato y Pagliarini, 2024, p. 8).

Etapas 3. Gobierno electrónico (2000-2014)

Los esfuerzos más amplios de transformación digital del Estado brasileño comenzaron a principios de la década de 2000 con la propuesta de la administración electrónica, prestando gran atención a la transparencia, la rendición de cuentas y la participación (Eaves, Mazzucato y Pagliarini, 2024). En 2004 se lanzó el Portal de Inclusión Digital y, en 2010, el Traductor de Lenguaje de Señas, innovaciones que representaron políticas públicas necesarias de accesibilidad.

Complementan estas iniciativas el programa E-gov, la Ley de Acceso a la Información (**Ley n.º 12.527, de 18 de noviembre de 2011**) y el Marco Civil de Internet (**Ley n.º 12.965, de 23 de abril de 2014**), que establecieron importantes bases políticas y legales. También se instituyeron mecanismos de coordinación como el Comité Ejecutivo de Gobierno Electrónico (CEGE), creado por **el Decreto de 18 de octubre de 2000**⁹⁴, y las normas de interoperabilidad (ePing), establecidas por la **Ordenanza n.º 92, de 24 de diciembre de 2014** (Brasil, 2014).

94. El Decreto del 18 de octubre de 2000 fue revocado por el Decreto n.º 8.638, de 15 de enero de 2016, y, posteriormente, por el Decreto n.º 10.332, de 28 de abril de 2000, que establece la Estrategia de Gobierno Digital para el período 2020-2022 en el ámbito de los órganos y entidades de la administración pública federal directa, autárquica y fundacional, y dispone otras medidas.

Etapa 4. Del gobierno electrónico al digital (2015-2018)

El Ministerio de Planificación lanzó la Estrategia de Gobernanza Digital (EGD) en 2015 y la implementó en 2016. La EGD se basó en tres pilares: 1) acceso a la información, 2) prestación de servicios y 3) participación social. Dicha estrategia estableció metas ambiciosas, incluyendo la expansión de los servicios digitales y el aumento del compromiso de las ciudadanas y los ciudadanos, rediseñando procesos internos e interfaces gráficas (Brasil, 2024). Un hito de ese año fue la creación de la Plataforma Gov.br, mediante el **Decreto n.º 8.936 del 19 de diciembre de 2016** (Brasil, 2016).

Tras el golpe parlamentario que culminó con la destitución de la presidenta Dilma Rousseff, su vicepresidente, Michel Temer, asumió la presidencia en 2016. En medio de una crisis fiscal, el gobierno interino enfatizó la eficiencia y la desburocratización como los principales impulsores de la transformación digital (Eaves, Mazzucato y Pagliarini, 2024).

La **Ley n.º 13.444 de 2017**, que creó la Identificación Civil Nacional (ICN), fue aprobada en ese contexto. Actualmente, la base de datos biométrica de la ICN constituye una de las tres bases biométricas de la plataforma Gov.br (Bioni et al., 2022). En complemento a los avances normativos, la **Ley n.º 13.709 del 14 de agosto de 2018**, conocida como Ley General de Protección de Datos Personales (LGPD), estableció las normas para el tratamiento computacional de los datos personales en el país.

Etapa 5. Plataformización del Estado (2019-2022)

Durante el gobierno de Jair Bolsonaro (2019-2022), el **Decreto n.º 9.745 del 8 de abril de 2019**, creó formalmente la Secretaría de Gobierno Digital⁹⁵, orientando sus atribuciones con énfasis en la eficiencia y la desburocratización del Estado. La Secretaría asumió, entre otras funciones, la supervisión de las iniciativas de la Red Gov.br (Brasil, 2019).

El **Decreto n.º 9.756 del 11 de abril de 2019**, instituyó el Portal [Gov.br](https://gov.br), que centralizó la información institucional, las noticias y los servicios públicos del Gobierno Federal. A diferencia de la Plataforma Gov.br, creada por el **Decreto**

95. El Decreto n.º 9.745 del 8 de abril de 2019 fue posteriormente derogado por el Decreto n.º 11.344 del 1.º de enero de 2023. En 2024, el Decreto n.º 11.344 del 1.º de enero de 2023 fue derogado por el Decreto n.º 11.907 del 30 de enero de 2024.

n.º 8.936 del 19 de diciembre de 2016, el Portal Gov.br unificó y amplió sus atribuciones para consolidar los servicios mencionados a lo largo de este informe.

En 2020, el 89% de los servicios federales habían sido digitalizados (Eaves, Mazzucato y Pagliarini, 2024). Durante la pandemia, la oferta de servicios como la cuenta Gov.br, la firma electrónica, así como el Pix y el programa Conecta Gov.br, impulsaron la transformación digital del Estado brasileño.

Para formalizar y orientar este proceso, se promulgó la **Ley n.º 14.129 del 29 de marzo de 2021** (Ley de Gobierno Digital), que instituyó principios, reglas e instrumentos para el Gobierno Digital. Con esta ley, se estableció el principio de «una sola vez» (*the once only principle*), según el cual los ciudadanos, las instituciones o las empresas que necesiten acceder a los servicios públicos solo deben introducir sus datos sensibles en el sistema una única vez.

En resumen, el desarrollo de la infraestructura pública digital brasileña se impulsó bajo la visión del Gobierno como Plataforma (*Government as a Platform* - GaaP)⁹⁶ (Eaves, Mazzucato y Pagliarini, 2024, p. 8).

Etapas 6. Infraestructuras públicas digitales y gobierno digital integrado (2023-presente)

Luís Inácio Lula da Silva, en su tercer mandato (2023-presente), creó el Ministerio de Gestión e Innovación en Servicios Públicos (MGI), que incorpora tanto la Secretaría de Gobierno Digital como Serpro y Dataprev (Brasil, 2023).⁹⁷

Estratégicamente posicionada en el MGI, la Secretaría de Gobierno Digital - instituida por la **Ordenanza n.º 23, de 4 de abril de 2019** - tiene como uno de sus pilares la integración federativa, cuyo objetivo consiste en la expansión e interiorización de la transformación digital del Estado brasileño, capacitando a los estados y municipios mediante la adhesión a la Red Nacional de Gobierno Digital (Rede Gov.br).

96. Para obtener más información sobre el concepto de Gobierno como Plataforma (GaaP), véase Cordella, Antonio y Paletti, Andrea. *Government as a platform, orchestration, and public value creation: the Italian case*. Londres: London School of Economics and Political Science, 2019. Disponible en: https://eprints.lse.ac.uk/102368/1/Cordella_Paletti_GIQ2019.pdf. Consultado el: 23 de septiembre de 2025.

97. Ambas empresas estatales de TI fueron incluidas en el Programa Nacional de Privatización (PND) durante el gobierno de Jair Bolsonaro (2019-2022), convirtiéndose en objeto de un proceso de privatización que generó un intenso debate sobre la soberanía y la seguridad digitales del país (Brasil, 2023).

La Red Gov.br se creó con el fin de promover la colaboración, el intercambio, la articulación y la creación de iniciativas innovadoras relacionadas con la temática del Gobierno Digital en el sector público. Debido a su naturaleza colaborativa, está formada por estados y municipios que han solicitado su adhesión.⁹⁸

Prevista en la Ley de Gobierno Digital mencionada anteriormente, la Estrategia Nacional de Gobierno Digital (EGD) fue elaborada por la Secretaría de Gobierno Digital a partir de un proceso participativo con actores municipales, estatales, distritales y socios del gobierno federal.⁹⁹ En esta etapa surgieron nuevas preocupaciones: el fortalecimiento de las IPD brasileñas, la defensa de la soberanía digital y la garantía de la inclusión digital y la universalización del acceso a los servicios públicos prestados (Eaves, Mazzucato y Pagliarini, 2024).

El **Decreto n.º 12.069, de 21 de junio de 2024**, formalizó esta nueva estrategia y la **Ordenanza SGD/MGI n.º 4.248, de 26 de junio de 2024**, estableció recomendaciones para el período 2024-2027. Otras iniciativas importantes son la Nueva Tarjeta Nacional de Identidad (CIN), el programa de Infraestructura Nacional de Datos (IND), el Plan Brasileño de Inteligencia Artificial (PBIA), el Centro Integrado de Seguridad Cibernética del Gobierno Digital (CISC Gov.br) y el Centro de Excelencia en Privacidad y Seguridad (CEPS).

98. En mayo de 2025, el número de municipios adheridos a la iniciativa alcanzó los 1800, lo que representa aproximadamente el 32% de los municipios brasileños (Brasil, 2025). Para obtener más información, visite: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/rede-nacional-de-governo-digital>.

99. A partir de abril de 2025, el Instituto de Defensa del Consumidor formará parte del Comité Asesor de la Estrategia Nacional de Gobierno Digital (CC-ENGD), establecido por la **Ordenanza MGI N.º 9.682, del 23 de diciembre de 2024**. El Comité tiene como objetivo servir de órgano asesor para la gobernanza de la Red Gov.br, así como para el seguimiento y la propuesta de desarrollos relacionados con la Estrategia Nacional de Gobierno Digital.

Servicios

Como se detalló anteriormente, la creación del portal Gov.br marca la Etapa 5 - de plataformización - en la trayectoria de transformación digital del Estado brasileño. Su establecimiento, sin embargo, es el resultado de una serie de iniciativas que caracterizan otras etapas de dicha trayectoria, especialmente la Etapa 2, marcada por el desarrollo del programa de Gobierno Electrónico.

Al observar las medidas adoptadas por los gobiernos de Fernando Henrique Cardoso (1995-2003), Luiz Inácio Lula da Silva (2003-2011), Dilma Rousseff (2011-2016), Michel Temer (2016-2018), Jair Bolsonaro (2019-2022) y por el actual gobierno de Lula (2023-presente), se evidencia que los orígenes del Gov.br se remontan a la política pública de gobierno electrónico y/o digital que, a lo largo de diferentes mandatos, tiene como objetivo optimizar la relación entre el Estado y la ciudadanía mediante el uso de la tecnología de la información (TI).

En la transición del gobierno electrónico hacia la transformación digital del Estado, el debate gira en torno al uso de sistemas computacionales con el fin de hacer que los servicios públicos sean más accesibles y transparentes para la población, bajo el argumento de promover la eficiencia en la prestación de dichos servicios.

La política de gobierno digital bajo el gobierno de Bolsonaro

El consenso entre gestores y académicos identifica un desmantelamiento generalizado de las políticas públicas (PP) durante el mandato de Jair Bolsonaro, al menos en el ámbito federal (Faria y Lima, 2024).

Pero ¿habría sido este el caso de la política de gobierno electrónico y/o de gobernanza digital, que con características propias atravesó cinco presidentes (siete mandatos) y hoy continúa desarrollándose bajo el actual gobierno de Luiz Inácio Lula da Silva (2023-presente)? ¿Habría sido esta política pública desmantelada por el gobierno Bolsonaro, como ocurrió con las políticas de fiscalización de la deforestación en la Amazonia Legal, de asistencia social o de derechos humanos? ¿O habría encontrado cierta resiliencia gracias a la actuación de la propia burocracia estatal? Las respuestas a estas preguntas exceden los límites de este informe, pero esperamos que su formulación inspire nuevas investigaciones en el futuro.

El Gov.br fue instituido con ese propósito. Se trata de un portal mediante el cual 155 millones de personas registradas pueden acceder gratuitamente, siempre que cuenten con conexión a Internet¹⁰⁰, a más de cinco mil servicios públicos digitales (5.309), además de noticias e información confiable del Poder Ejecutivo Federal, como se observa en la Figura 19.

Todo ello permanece disponible en un mismo entorno digital cuyo diseño sigue el principio de «una sola vez» (*the once only principle*). El portal permite un acceso unificado a la Cartilla de Trabajo Digital, a la Factura de Servicios Electrónica (NFSe), a la Escrituración Digital de las Obligaciones Fiscales, Previsionales y Laborales (e-Social) y al Fondo de Garantía por Tiempo de Servicio Digital (FGTS digital, aún en fase de prueba), entre otros servicios disponibles para las ciudadanas y los ciudadanos registrados en Gov.br.

Entre los servicios disponibles, los más utilizados, según una noticia publicada por el Ministerio de Gestión e Innovación en los Servicios Públicos (MGI) en mayo de 2025, son: Firma Electrónica, Mi INSS, Mi SUS Digital, Enem, Fies, Cartilla de Trabajo Digital y Cartilla Digital de Tránsito (MGI, 2025).

Figura 19. Reproducción del Panel de Monitoreo de los Servicios Digitales¹⁰¹



Fuente: Gov.br (2025)

100. El Idec considera que la banda ancha es un servicio esencial para los ciudadanos, por lo que lucha por su universalización desde la campaña «La banda ancha es un derecho de todos». Más adelante discutiremos los problemas de la exclusión digital en Brasil relacionados con el gobierno digital y la forma en que estos han sido mitigados por el gobierno actual.

101. Estas cifras datan del 05/09/2025. La consulta se realizó en el portal el 06/09/2025.

En la plataforma Gov.br es posible realizar diversas transacciones, como llenar formularios, firmar documentos, programar consultas médicas, acceder a la cartera de vacunación en el Sistema Único de Salud (SUS), inscribirse en el Examen Nacional de Educación Media (ENEM) o en el Concurso Nacional Unificado (CNU), acceder a la Licencia Nacional de Conducir (CNH), simular la jubilación, entre otros servicios. Los costos del portal Gov.br se dividen entre las diferentes entidades federativas, lo que garantiza la gratuidad del propio portal (Brasil, 2025).

En 2024, el portal Gov.br figuraba entre las aplicaciones más descargadas del país, a veces por delante de redes sociales como Instagram y TikTok¹⁰². En la categoría de gobierno, en marzo de 2024, el portal se convirtió en la plataforma pública más visitada del mundo, con más de 150 millones de usuarios y usuarias¹⁰³.

Gov.br no solo sirve para la certificación de identidad. El portal también ofrece servicios de firma electrónica, que registraron más de 75 millones de usos entre enero y mayo de 2025 (Brasil, 2025). A través de este servicio es posible firmar gratuitamente documentos con validez jurídica, respaldados por la **Ley n.º 14.063, de 23 de septiembre de 2020**. Dicha validez jurídica distingue estas firmas de las demás firmas pagadas, que requieren certificación digital, lo que representa un factor de inclusión de la sociedad en el entorno digital (Benelli et al., 2024).

El acceso unificado a esta plataforma digital se realiza a través de la cuenta Gov.br. Cada ciudadano puede acceder, con una contraseña única, a todos los servicios públicos, noticias e información integrados en esta cuenta, que tiene tres niveles de seguridad: bronce, plata y oro. Cada uno de estos niveles corresponde a la forma en que se creó y validó la cuenta Gov.br.

Los diferentes niveles de acceso validan un mayor o menor grado de seguridad, ampliando o restringiendo el acceso a los servicios disponibles, como se detallará más adelante. Los niveles de acceso más altos están

102. Las clasificaciones completas están disponibles en: <<https://www.poder360.com.br/poder-tech/gov-br-lidera-downloads-na-play-store-em-2024-veja-ranking/>>. Consultado el: 3 de octubre de 2025.

103. Disponible en: <<https://www.gov.br/gestao/pt-br/assuntos/noticias/2024/marco/gov-br-e-a-pagina-de-governo-mais-acessada-do-mundo>>. Consultado el: 3 de octubre de 2025.

vinculados a la autenticación del usuario mediante datos biométricos, como el reconocimiento facial, lo que, en términos de protección de datos personales, revela un mayor grado de riesgo para el titular de los datos.

Al optar por un modelo de autenticación basado en el reconocimiento facial, el gobierno federal asume el riesgo de producir resultados derivados del llamado racismo algorítmico, en el que las personas negras, por ejemplo, se ven afectadas negativamente por el funcionamiento de estas herramientas de reconocimiento facial (Kremer, 2023; Silva, 2022). Son numerosos los casos que denuncian este tipo de violencia.

Como ejemplo de este tipo de violencia, cabe destacar el caso en el que un trabajador de la plataforma de reparto IFood, identificado como hombre negro, fue impedido de realizar su trabajo debido a un fallo del sistema de reconocimiento facial adoptado por la empresa. El trabajador presentó una demanda ante el Tribunal Laboral, que, en su sentencia, reconoció el fallo como racista y condenó a la empresa¹⁰⁴.

Como se mencionó anteriormente, los niveles de acceso al Portal Gov.br dan permiso a diferentes servicios y políticas públicas digitalizadas. Sin embargo, es necesario que el gobierno federal adopte medidas para facilitar el acceso a estos servicios y políticas sin renunciar a las mejores prácticas de seguridad.

Un ejemplo de ello es el programa Desenrola Brasil, creado para facilitar la renegociación de deudas y dirigido a personas con ingresos brutos mensuales de hasta dos salarios mínimos o que estén inscritas en el Registro Único para Programas Sociales del Gobierno Federal (CadÚnico) (Ministerio de Hacienda, 2025). Para acceder a este programa, el usuario debería poseer cuentas con nivel plata u oro. Sin embargo, el Ministerio de Hacienda identificó que cerca del 44% de los beneficiarios del Desenrola Brasil no poseían tales niveles de acceso en Gov.br, y el 13% ni siquiera poseía cuenta Gov.br con nivel bronce. El éxito de un programa importante para contener el sobreendeudamiento de la población podría verse comprometido por barreras de acceso a la plataforma Gov.br.











En este sentido, buscando superar esta barrera de entrada en un programa social, el Gobierno Federal pasó a autorizar, en enero de 2024, que personas con cuenta Gov.br de nivel bronce pudieran renegociar sus deudas¹⁰⁵.

A continuación, es posible visualizar una tabla comparativa de los niveles de seguridad de la cuenta Gov.br.

104. Disponible en: <<https://g1.globo.com/df/distrito-federal/noticia/2025/06/30/justica-condena-ifood-a-indenizar-entregador-do-df-por-danos-morais-apos-falha-racista-em-reconhecimento-facial-entenda.ghtml>>. Consultado el: 3 de octubre de 2025.

105. Disponible en: <<https://g1.globo.com/economia/noticia/2024/01/29/desenrola-brasil-governo-permite-parcelamento-para-pessoas-com-conta-bronze-do-govbr.ghtml>>. Consultado el: 3 de octubre de 2025.

Figura 20. Tabla comparativa de los niveles de seguridad de la cuenta Gov.br

	 BRONCE	 PLATA	 ORO
Una única cuenta para acceder a diversos servicios digitales.			
Hacer el login en cualquier servicio gov.br sin necesidad de contraseña, usando solo la biometría del celular			
Gestionar las autorizaciones de uso de sus datos			
Realizar la prueba de vida utilizando el reconocimiento facial			
Visualizar y compartir sus datos y documentos digitales			
Utilizar servicios gratuitos de firma electrónica en el sitio assinador.iti.br			
Acceder a servicios públicos que exigen el mayor grado de confiabilidad de la cuenta gov.br			
Habilitar la autenticación en dos pasos para tener más seguridad en el uso de su cuenta			
Nivel máximo de seguridad de la cuenta gov.br	Básico	Alto	Máximo

Fuente: Adaptado de Gov.br (2024)

Gov.br también permite el desarrollo de interfaces de programación de aplicaciones (API) que posibilitan el intercambio automático y seguro de datos entre los sistemas informáticos del Poder Ejecutivo Federal. Esto significa que, si el Estado ya dispone de determinados datos de identificación registrados, los ciudadanos pueden solicitar que estos se pongan a disposición de otros servicios sin necesidad de presentarlos de nuevo.

Cabe recordar que este derecho ya está garantizado por la Ley de Sello de Desburocratización y Simplificación (**Ley N.º 13.726, del 8 de octubre de 2018**) y la Ley de Gobierno Digital mencionada anteriormente. Esta solución desarrollada a partir del portal integra datos y facilita la oferta de servicios públicos digitales. En otras palabras, se produce la interoperabilidad de los datos, lo que facilita el acceso a los servicios y, al mismo tiempo, a los derechos (Benelli et al., 2024).

Creación de una cuenta Gov.br

A continuación, se presenta la descripción del paso a paso para abrir una cuenta Gov.br, utilizando datos disponibles en el *Frequently Asked Questions* (FAQ) de la cuenta Gov.br¹⁰⁶.

Acceder al sitio web o aplicación de Gov.br

1. **Desde el computador:** Acceda al sitio web oficial de Gov.br: <https://www.gov.br/>
2. **Desde el celular:** Descargue la aplicación “Gov.br” en la tienda de aplicaciones de su celular (Google Play Store para Android o Apple App Store para iOS). El proceso es bastante similar en ambos casos.



Paso 2: Iniciar el Registro

1. En el sitio web o aplicación, haga clic en “**Crear su cuenta Gov.b**” o “**Ingresar con Gov.br**” y, a continuación, en la opción para crear cuenta.
2. Se le solicitará que informe su **CPF**. Escribalo y haga clic en “Continuar”.



106. Para obtener más información, visite el sitio web: <https://acesso.gov.br/faq/>

Paso 3: Validar sus Datos Personales

El sistema intentará validar sus datos automáticamente a partir de bases de datos gubernamentales (como CPF, Título de Elector, CNH, etc.).

1. Se le presentarán algunas **preguntas sobre sus datos personales** (como año de nacimiento, nombre de la madre, fecha de expedición de la CNH, etc.). Respóndalas correctamente.
2. Después de responder las preguntas, deberá elegir cómo desea recibir **código de verificación**: por correo electrónico (e-mail) o por SMS (teléfono celular). Elija la opción de su preferencia.
3. Escriba el código de verificación recibido en el campo indicado.

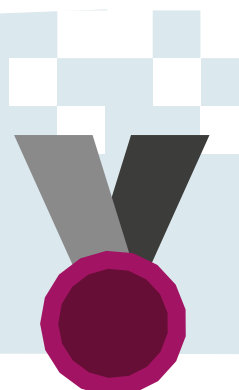


Paso 4: Crear su Contraseña

1. Tras la validación del código, será dirigido a la pantalla de creación de contraseña.
2. Cree una contraseña fuerte, que contenga letras mayúsculas y minúsculas, números y caracteres especiales. Guárdela en un lugar seguro.
3. Confirme la contraseña y haga clic en “Crear cuenta”.



Paso 5: Completar el Registro y Aumentar el Nivel de la Cuenta (Opcional)



Al finalizar los pasos anteriores, el usuario tendrá una cuenta de **nivel Bronce**, que permite acceder a los servicios descritos en la Figura 20. Para acceder a más servicios y mayor seguridad, es necesario aumentar el nivel a Plata u Oro.

Para aumentar al Nivel Plata:

- **Validación facial mediante la aplicación Gov.br:**

1. Descargue la aplicación Gov.br en su teléfono móvil.
2. Inicie sesión con su CPF y contraseña.
3. Acceda a «Aumentar nivel» o «Privacidad».
4. Siga las instrucciones para completar la validación facial, que generalmente implica escanear su rostro utilizando la foto de su Licencia Nacional de Conducir (CNH) o los datos biométricos faciales de su TSE (Tarjeta de Registro de Votantes).

- **Validación Bancaria:**

1. Inicie sesión en Gov.br.
2. Seleccione la opción de validación por banco.
3. El sistema le dirigirá al sitio web o la aplicación de uno de los bancos asociados (Banco do Brasil, Caixa, entre otros).
4. Inicie sesión de forma segura en su banco para que Gov.br pueda validar su identidad.

- **Certificado de Vacunación:**

1. En la aplicación Gov.br, puede aumentar el nivel a Plata si tiene el certificado de vacunación contra la COVID-19 validado.

Para aumentar el nivel de seguridad a Oro:

- **Validación Facial por la Justicia Electoral (TSE):** Utilice la aplicación Gov.br para realizar el reconocimiento facial comparando su foto con la base de datos de la Justicia Electoral.
- **Validación por Certificado Digital:** utilice un certificado digital (e-CPF) para validar su cuenta.



GOV.BR

Lentes de Análisis

Inclusión Digital



Para que las IPD como Gov.br puedan ser utilizadas por el mayor número posible de personas, el Estado aún debe enfrentar y resolver el problema de la exclusión digital en Brasil en sus múltiples dimensiones sociales. La prestación de servicios públicos a través de las IPD puede facilitar la vida de la población, que ya accede a Internet para consumir diversos servicios privados: comercio electrónico, transporte individual, pedidos de comidas, entre otros. Sin embargo, las desigualdades sociales representan un desafío que debe tenerse en cuenta en la oferta de servicios públicos a través de Internet (Falcão et al., 2023).

La adopción de las IPD no se produce al margen de las desigualdades existentes. Una de sus manifestaciones más evidentes está relacionada con la cuestión del acceso a las tecnologías de la información y la comunicación (TIC) en Brasil, especialmente a Internet. Los ciudadanos eligen la forma de interactuar con el Estado en función de las condiciones objetivas y subjetivas en las que se encuentran.

Es precisamente en este sentido que el problema de la exclusión digital no puede ignorarse en el debate sobre las IPD. Al fin y al cabo, este problema constituye un fenómeno social complementario que restringe las oportunidades que las personas pueden obtener con el uso de Internet en general y de las IPD en particular.

Es importante investigar la adopción de las TIC y las IPD desde una perspectiva tecnológica. Sin embargo, como citan Falcão et al. (2023), también es necesario analizar los aspectos sociales, políticos y sociodemográficos de los usuarios. Ciertas clases o grupos sociales enfrentan más dificultades o barreras de acceso en el uso de estas tecnologías que otros, quedando, a menudo, al margen de lo que se ofrece de forma digital y electrónica. Un ejemplo es el grupo social de personas mayores (IdeC, 2025), representado por individuos de 60 años o más.

Durante la pandemia de la COVID-19, se produjo una expansión en la prestación de servicios públicos digitales a través de Internet. En este momento, las personas mayores sufrieron aún más la exclusión digital, ya que, en muchos casos, no podían utilizar los servicios disponibles a través de las plataformas digitales (Seifert, 2021).

Para comprender los aspectos que llevan a este y otros grupos sociales a utilizar menos –o incluso no utilizar– las tecnologías digitales en Brasil, debemos observar los datos sociodemográficos sobre el acceso a Internet y las habilidades digitales.

Para crear una estrategia de transformación digital del Estado alineada con las políticas de lucha contra la exclusión y fomento de la inclusión digital,

*(...) es necesario que los fenómenos sociales se consideren complementarios y que las políticas públicas sean más amplias en el sentido de incluir el acceso, la educación y la identificación de las necesidades individuales de los usuarios»
(Falcão et al., 2023, p. 1).*

Por lo tanto, es necesario comprender el perfil y el comportamiento de los consumidores de Internet más vulnerables (Al-Hujran et al., 2015; Phang et al., 2006).

La edición de 2025 de la encuesta TIC Domicilios, realizada por el Centro Regional de Estudios para el Desarrollo de la Sociedad de la Información (Cetic.br), señaló que, entre 2023 y 2024, se redujo la proporción de usuarios de Internet mayores de 16 años que utilizaron servicios públicos digitales o de administración electrónica, con una disminución significativa del 73 % al 61 % de los usuarios de Internet (NIC.br, 2025).

Según la encuesta, el tipo de servicio público que sufrió una mayor variación en el acceso en relación con 2023 fue el relacionado con los derechos de los trabajadores y la seguridad social, con una reducción de ocho puntos porcentuales (NIC.br, 2025). Los datos sugieren, además, que el mayor uso de la administración electrónica por parte de los usuarios de Internet mayores de 16 años está asociado a un mayor nivel de instrucción: el 83 % de las personas con estudios superiores utilizan este tipo de servicio, mientras que solo el 39 % de las personas con estudios primarios acceden a los servicios públicos digitales (NIC.br, 2025).

Otro aspecto a destacar es el hecho de que los mayores porcentajes de acceso a los servicios públicos digitales están asociados a los mayores niveles de conectividad significativa (CS): «(...) mientras que el 88 % de los usuarios de Internet con el nivel más alto de CS utilizaron este tipo de servicio, la proporción fue del 38 % para el grupo con menor CS. Las personas de las clases D y E (43 %), de 60 años o más (38 %) y con un salario mínimo (42 %) se encontraban entre las que menos utilizaban los servicios públicos en línea» (NIC.br, 2025, p. 80).

Los datos de la encuesta indican que, entre 2021 y 2023, hubo un aumento en la proporción de ciudadanos que no salieron de casa para pagar impuestos y tasas gubernamentales, prefiriendo hacerlo de forma remota, a través de Internet. En cuanto a otras actividades, como asuntos relacionados con la

seguridad pública, documentos personales o derechos de los trabajadores, no hubo variaciones en las proporciones.

La encuesta destaca que no hubo variación en los motivos por los que una parte de los usuarios no utiliza los servicios públicos digitales, siendo la preferencia por el contacto cara a cara la razón más mencionada (NIC.br, 2025). Los grupos que más señalaron este motivo se encuentran entre aquellos con educación primaria y mayores de 60 años.

Entre los usuarios que no utilizan los servicios públicos digitales, el 53 % no lo hizo porque consideraba que los servicios eran complicados o porque tenían algún riesgo para la seguridad y la privacidad de los datos personales. A pesar de la difusión de las IPD en Brasil, estos datos indican que aún es necesario garantizar una mayor inclusión de los ciudadanos en cuanto a su uso efectivo (NIC.br, 2025).

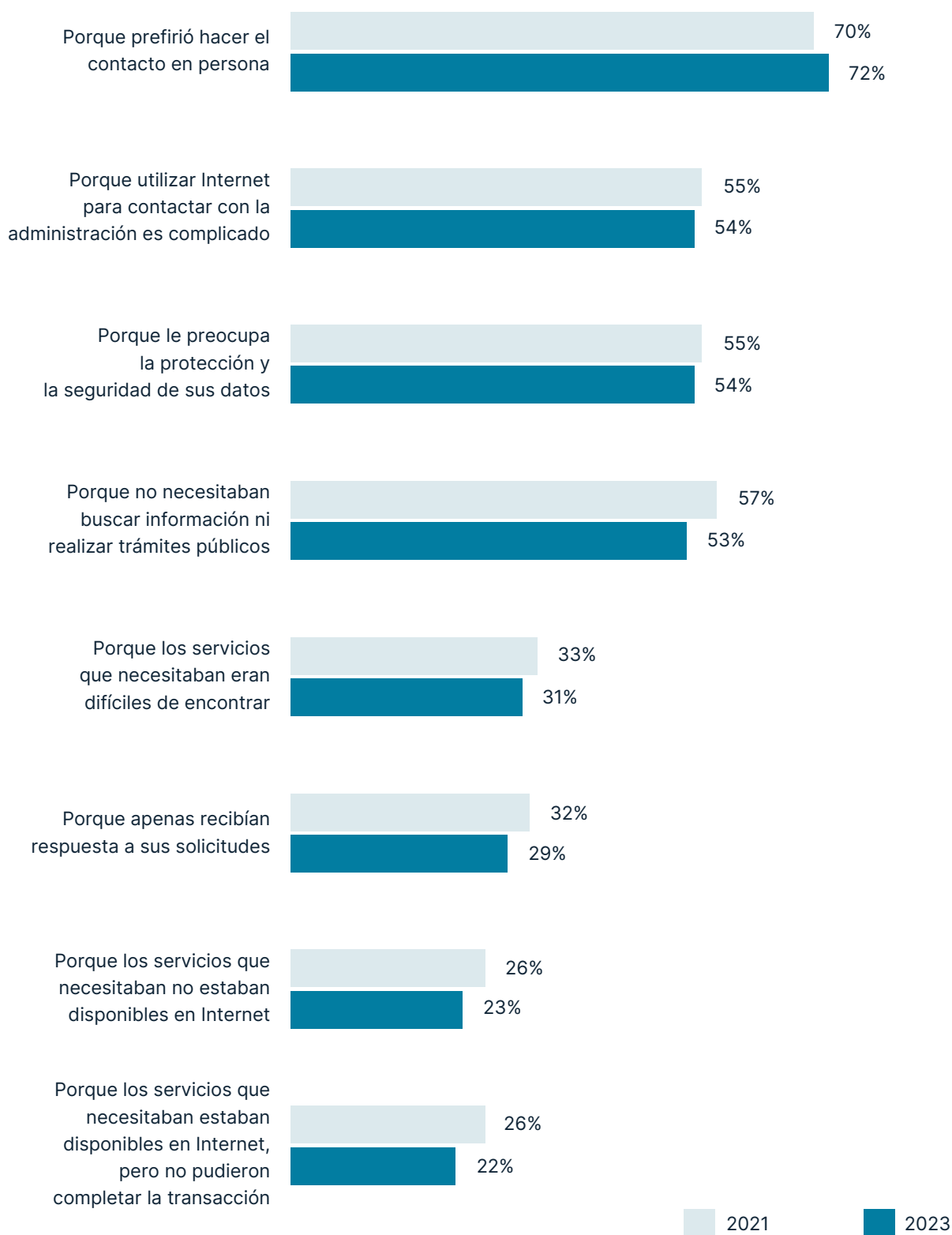
Los datos revelan, además, un aspecto que requiere atención en cuanto al posible desajuste entre las formas de contacto entre los ciudadanos y el gobierno, a nivel federal, estatal y municipal. Se ha identificado un bajo nivel de participación de los ciudadanos en los mecanismos digitales de participación popular, como votaciones, encuestas y consultas públicas, además del escaso uso de los canales de comunicación digitales establecidos por el gobierno en sus diferentes esferas.

Este posible desajuste se debe al contraste entre la baja adhesión de ustedes a los mecanismos mencionados anteriormente y el aumento de las formas de contacto ofrecidas por los gobiernos en los ámbitos municipal, estatal y federal, que han abierto perfiles en plataformas de redes sociales como Instagram o TikTok y de mensajería instantánea como WhatsApp o Telegram (CGI.br, 2022). Como se puede observar en la Figura 21, este desajuste puede indicar la existencia de otras barreras y limitaciones en el acceso a Internet que han impedido a los consumidores ponerse en contacto con el gobierno a través de estos canales digitales.

Figura 21. Personas consumidoras de Internet que no utilizaron servicios electrónicos en los últimos 12 meses (2015-2023)

USUARIOS DE INTERNET QUE NO HAN UTILIZADO LOS SERVICIOS DE GOBERNANZA ELECTRÓNICA EN LOS ÚLTIMOS 12 MESES, POR MOTIVO DE NO UTILIZACIÓN (2021-2023)

Total de usuarios de Internet mayores de 16 años que no han utilizado servicios de administración electrónica en los últimos 12 meses (%)



Fuente: Reproducción. NIC.br (2023).

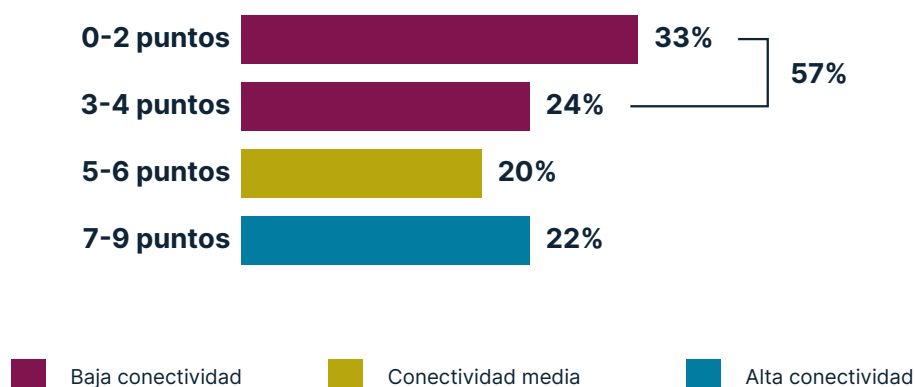
En este sentido, la promoción de la inclusión digital exige el enfrentamiento, en palabras de Renata Mielli (2024, p.20), coordinadora del CGI.br, de los “desafíos relacionados con la provisión de una conectividad de calidad, con velocidad adecuada y sin barreras que limiten el uso de Internet, como la imposición de un límite o franquicia de datos, por ejemplo”. Además, para que ciudadanas y ciudadanos accedan plenamente a las IPDs, es necesario comprender no solo sus usos y habilidades digitales, sino también la seguridad y la privacidad en el entorno digital.

En el estudio inédito “Conectividad Significativa: propuestas para la medición y el retrato de la población en Brasil”, lanzado en 2024, se elaboró una definición de conectividad más amplia en términos de calidad. Según esta definición, la conexión significativa debería permitir el uso satisfactorio de varios servicios disponibles en Internet, posibilitando el aprovechamiento efectivo de las oportunidades creadas en el entorno digital. La conectividad significativa fue medida en una escala de cero a nueve, basada en nueve indicadores agrupados en cuatro dimensiones (NIC.br, 2024):



A pesar de que Brasil ha avanzado considerablemente en los índices de acceso a Internet - el 84% de su población con 10 años o más accede a Internet - el estudio mostró que este acceso se caracteriza por una baja conectividad significativa (NIC.br, 2024).

Figura 22. Distribución de la Conectividad Significativa en Brasil—2024
Porcentajes de brasileños según rango de puntuación y características geográficas



Fuente: Adaptado de NIC.br (2024)

Las regiones Norte y Nordeste tienen los peores índices de conectividad significativa, con solo el 11 % y el 10 % de la población, respectivamente, en el rango de 7 a 9 puntos. En el otro extremo de la escala, entre 0 y 2 puntos, estas regiones presentaron un 44 % y un 48 %, recordando que la media nacional es del 33 % (NIC.br, 2024).

Por su parte, las regiones Sur y Sudeste registraron los mejores índices, 27 % y 31 %, siendo las únicas en las que el número de habitantes en el rango más alto es superior al del rango más bajo (NIC.BR, 2024, p. 106).

Cuanto más grandes son las ciudades, mejores son los índices de conectividad significativa (NIC.br, 2024, p. 107). En aquellas con hasta 50 000 habitantes, el 44 % se encuentra en el peor rango de la escala. En las ciudades con más de 500 000 habitantes, la proporción negativa se reduce casi a la mitad (24 %) (NIC.br, 2024, p. 107). Mientras que el 30 % de los habitantes de las zonas urbanas se encuentran en el peor rango (hasta 2 puntos), el 54 % de los que viven en zonas rurales se encuentran en el peor rango (NIC.br, 2024, p. 107).

Este estudio también confirmó la mayor vulnerabilidad a la exclusión digital de las personas mayores mencionada anteriormente: el 61 % de los brasileños de 60 años o más se encuentran en una situación de conectividad significativamente baja (en el rango de hasta 2 puntos), una proporción muy superior a la observada en general (33 %) (NIC.br, 2024, p. 112).

Solo el 16 % de las personas de entre 10 y 15 años y el 24 % de las de entre 16 y 24 años se encuentran en el rango más alto (entre 7 y 9 puntos) (NIC.br, 2024, p. 113). Los niveles más altos de conectividad significativa no se dan entre las personas más jóvenes, contrariamente a lo que sugiere el sentido común, sino entre los grupos de edad presentes en el mercado laboral (entre 25 y 44 años) (NIC.br, 2024, p. 113).

La proporción en el rango más alto (entre 7 y 9 puntos) es considerablemente mayor entre los hombres (28 %) que entre las mujeres (17 %), una diferencia de

11 puntos porcentuales. Esta desigualdad merece atención en la formulación de políticas públicas de inclusión digital.

El análisis de los datos basado en la autodeclaración de color o raza refleja el escenario de exclusión de grupos ya vulnerabilizados socialmente. Existe un claro desequilibrio entre individuos blancos, por un lado, y negros y mestizos (pardos), por el otro. Entre los autodeclarados blancos, el 32% se encuentra en el grupo con mejor desempeño (entre 7 y 9) y el 27% presenta los peores índices de conectividad significativa (entre 0 y 2) (NIC.br, 2024, p. 114).

Entre negros y mestizos (pardos), solo el 18% está en el rango más alto y el 34% está en el rango más bajo (NIC.br, 2024, p. 115). La diferencia entre blancos, negros y mestizos (pardos) asciende, por lo tanto, a 14 puntos porcentuales, considerando el rango con los índices más altos (NIC.br, 2024, p. 115). Políticas públicas centradas en la reducción de las desigualdades de acceso y de uso de las TICs en estos grupos más vulnerables son imprescindibles para la universalización de la conectividad significativa en Brasil.

El estudio también mostró una relación entre escolaridad y conectividad significativa. Cuanto mayor es el nivel de escolaridad, menor es la proporción de individuos con puntuación entre 0 y 2 y mayor es la proporción de individuos con puntuación entre 7 y 9 (NIC.br, 2024, p. 117). Entre los individuos con hasta la enseñanza primaria I, el 68% se encuentra en el peor rango de puntuación y solo el 3% en el mejor. Entre los individuos con enseñanza superior, la situación se invierte: solo el 7% se encuentra en el peor rango de puntuación y el 59% en el mejor (NIC.br, 2024, p. 117).

Llama la atención también la relación entre clase socioeconómica y conectividad significativa. Entre los individuos de la clase A, el 83% se encuentra en el mejor rango de puntuación y solo el 1%, en el peor. Entre aquellos de las clases D y E, la situación se invierte: solo el 1% está en el mejor rango de puntuación y el 64% en el peor (NIC.br, 2024, p. 117).

Entre las personas beneficiarias de programas sociales, más vulnerables en términos socioeconómicos, el 43% presenta una puntuación entre 0 y 2, y solo el 9% entre 7 y 9. Entre los individuos que no son beneficiarios, el 28% tiene una puntuación entre 0 y 2, y el 29% entre 7 y 9. Cabe destacar que estos números son superiores a los presentados por el conjunto de la población brasileña, que tiene el 33% de individuos en el peor rango de puntuación y el 22% en el mejor (NIC.br, 2024, p. 117).

Los resultados muestran que, entre las personas con trabajo remunerado, el 20 % se encuentra en el rango de 0 a 2 y el 34 % entre 7 y 9. En los otros tres grupos considerados por la investigación, esta situación no se repite: en ellos, la proporción de individuos en el rango más bajo de conectividad significativa es superior a la proporción de individuos en el rango más alto:

Entre las personas económicamente inactivas, que ni trabajan ni buscan empleo, la diferencia es notable: el 48 % obtiene una puntuación entre 0 y 2, y solo el 10 % entre 7 y 9. La diferencia entre los desempleados (aquellos que buscan empleo)

y los que tienen un trabajo remunerado alcanza los 19 puntos porcentuales (NIC.br, 2024, págs. 117-118).

Las barreras históricas para la inclusión productiva, como mayores ingresos y cualificación, se ven reforzadas por la falta de acceso a una Internet de calidad. Las personas con menor nivel educativo, de las clases socioeconómicas más vulnerables, beneficiarias de programas sociales y fuera de la fuerza laboral o en busca de empleo son precisamente las que tienen los peores índices de conectividad significativa (NIC.br, 2024, p. 118).

La categoría de análisis «conectividad significativa» parte de la idea de que, para aprovechar eficazmente las oportunidades que ofrece el uso de Internet, es necesario garantizar unas condiciones de acceso suficientemente adecuadas. Así, una vez identificados los factores que caracterizan los mejores y peores índices de conectividad (como las características demográficas y económicas), aún es necesario comprender la relación entre dichos índices y los diferentes tipos de actividades realizadas en el entorno digital (NIC.br, 2024).

Los indicadores que se refieren a las denominadas «actividades transaccionales» son los que más nos interesan en este contexto, ya que implican el intercambio de información, bienes o servicios entre consumidoras, consumidores y empresas, así como entre ciudadanas, ciudadanos y el Estado (en las esferas municipal, estatal y federal), como se puede observar en la Figura 23.

Figura 23. Indicadores de actividades transaccionales derivados y preguntas de origen

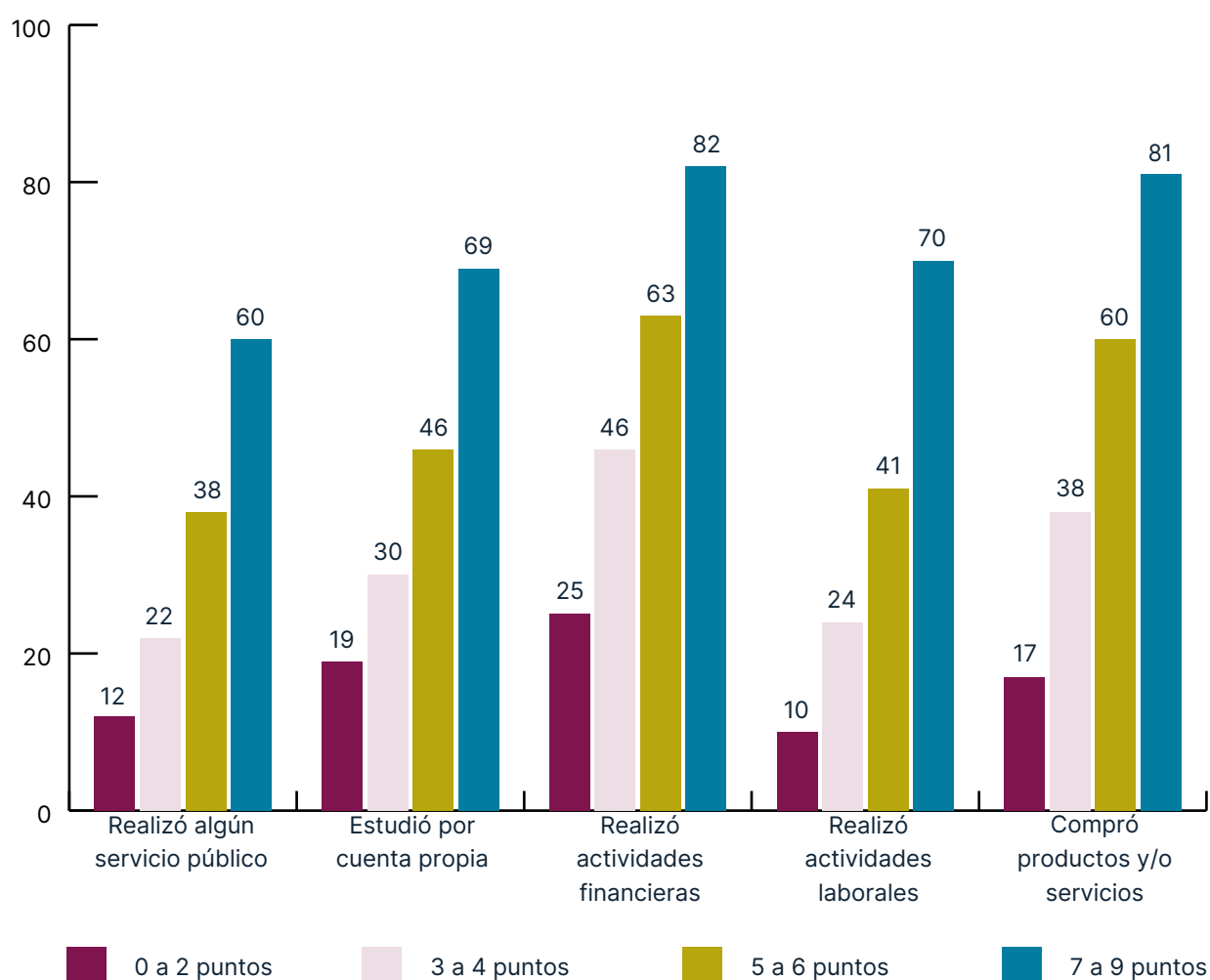
ACTIVIDADES TRANSACCIONALES	Realizó algún servicio público	¿Cuál de las siguientes actividades realizó en Internet en los últimos 3 meses?	¿Realizó algún servicio público, por ejemplo: emitir documentos por Internet, completar y enviar formularios en línea o pagar tasas e impuestos por Internet?
	Realizó actividades financieras		¿Hizo consultas, pagos u otras transacciones financieras?
	Realizó actividades laborales		¿Realizó actividades laborales?
	Estudió por cuenta propia		¿Estudió por cuenta propia a través de Internet?
	Compró productos y/o servicios	¿Usted compró o encargó productos o servicios por Internet en los últimos 12 meses, aunque el pago no se haya realizado por Internet?	

Fuente: NIC.br (2024)

Los indicadores de actividades transaccionales evidencian importantes cuellos de botella entre los diferentes niveles de conectividad significativa. El uso de Internet para servicios públicos presenta una correlación directa con la calidad de la conectividad: mientras que el 60 % de las personas con una puntuación entre 7 y 9 realizaron algún servicio en línea, esta proporción se reduce al 38 % entre aquellos con una puntuación de 5 a 6, al 22 % en el grupo de 3 a 4 puntos y alcanza solo el 12 % entre los usuarios con conectividad más precaria (0 a 2). Se observa una relación lineal similar en las demás actividades transaccionales (NIC.br, 2024, págs. 127-128).

Entre las actividades transaccionales, la amplitud de la disparidad entre los grupos extremos es de 48 a 64 puntos porcentuales, alcanzando su punto máximo en la compra de productos y servicios por Internet (NIC.br, 2024, p. 132), como se muestra en la Figura 24.

Figura 24. Niveles de conectividad significativa por actividades transaccionales realizadas en Internet (2023) - Total de usuarios de Internet (%)



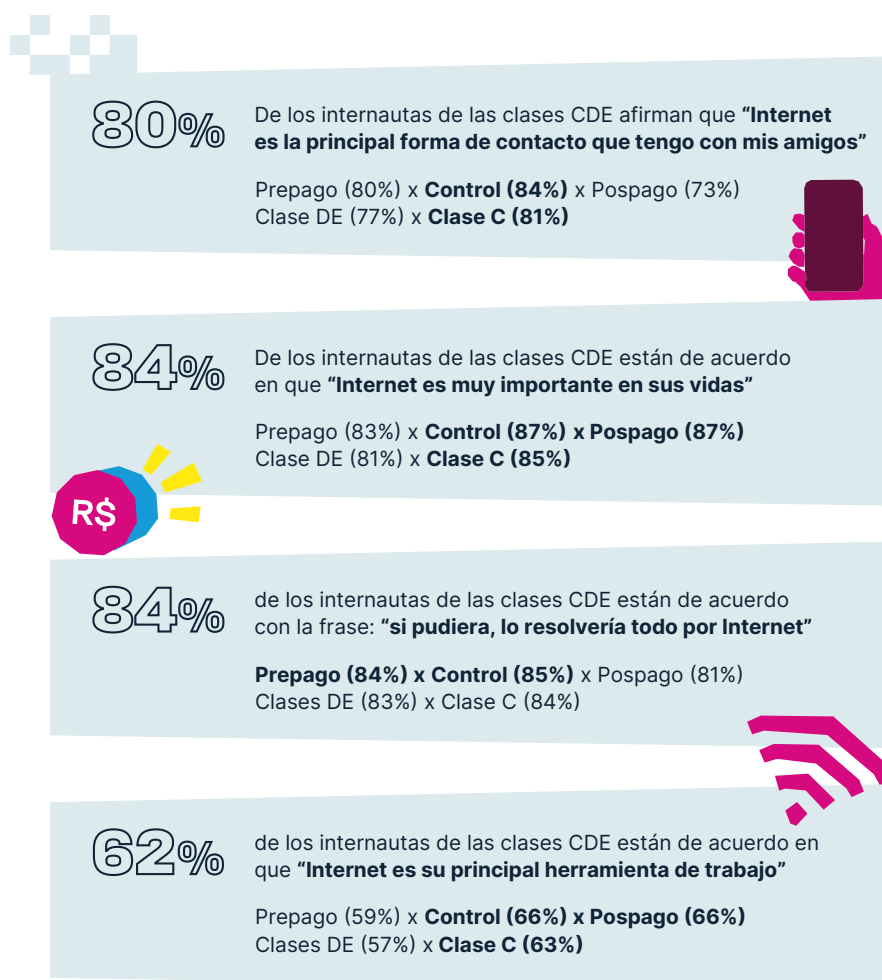
Fuente: Reproducción. NIC.br (2024).

Perfil de los usuarios de IPD y desigualdad de acceso

Las IPD se concentran predominantemente entre usuarios con una conectividad significativa. Este grupo se caracteriza por un perfil demográfico específico: mayoritariamente hombres blancos, pertenecientes a las clases A y B, con un nivel educativo superior (Nic.br, 2024; Anatel, 2025).

Paradójicamente, aunque las clases C y D presentan los índices más bajos de conectividad significativa, estas poblaciones reconocen Internet como un recurso esencial. Una investigación realizada por Idec e Instituto Locomotiva (2021) revela que el 84 % de estos usuarios y usuarias consideran que Internet es muy importante para sus vidas, la misma proporción que afirma que «si pudiera, resolvería todo por Internet» (Idec e Instituto Locomotiva, 2021, p. 4). Entre estos consumidores, el 62 % identifica Internet como su principal herramienta de trabajo (Idec e Instituto Locomotiva, 2021, p. 4).

Figura 25. Relevancia de Internet para los consumidores de las clases C, D y E

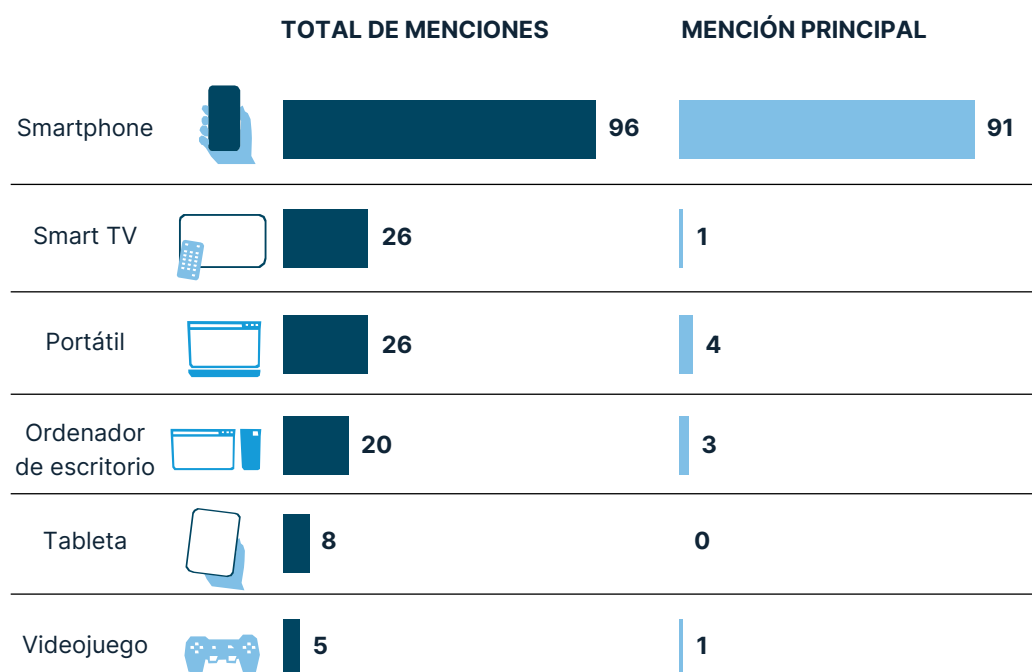


Fuente: Idec e Instituto Locomotiva, 2021

La intensidad de uso confirma esta centralidad: nueve de cada diez personas de las clases C, D y E acceden a Internet a diario. La telefonía móvil destaca como vía predominante de acceso, ya que el 91 % utiliza smartphones como dispositivo principal y solo el 4 % dispone de computadoras portátiles, el 3 % de computadoras de escritorio y el 0,3 % de tabletas (Idec e Instituto Locomotiva, 2021).

Cuando se les preguntó sobre las seis principales formas de acceso a Internet, solo el 26 % mencionó las computadoras portátiles y el 20 % las computadoras de escritorio, lo que refuerza la dependencia exclusiva de la telefonía móvil para una parte significativa de estos consumidores (Idec e Instituto Locomotiva, 2021), como se muestra en la Figura 26.

Figura 26. Dispositivos digitales más utilizados



Fuente: Idec e Instituto Locomotiva, 2021

Franquicia de datos y exclusión del acceso a los servicios públicos

La escasez de franquicia de datos constituye una barrera para el acceso a los servicios públicos digitales. Entre los consumidores de las clases C, D y E, el 39 % dejó de beneficiarse de las políticas públicas por falta de acceso a Internet 3G/4G en sus smartphones (Idec e Instituto Locomotiva, 2021, p. 12). Este impedimento ha tenido un impacto directo en el ejercicio de sus derechos: el 33 % no ha podido realizar algún servicio público y el 28 % ha dejado de recibir prestaciones sociales (Idec e Instituto Locomotiva, 2021, p. 12).

Entre los usuarios de planes restringidos a unas pocas aplicaciones, la privación se intensifica: el 52 % sufrió limitaciones en el acceso a las políticas públicas. Además, al 34 % se les bloqueó el acceso a Internet, perdiendo así el acceso a prestaciones sociales, mientras que el 45 % dejó de utilizar los servicios públicos digitales debido a bloqueos que les restringían, mediante la práctica de tarifa cero o *zero rating*¹⁰⁷, el uso de aplicaciones específicas (Idec e Instituto Locomotiva, 2021).

Datos recientes de Anatel (2025), elaborados en colaboración con Idec, confirmaron y profundizaron este diagnóstico: el 63,8 % de las personas dejaron de acceder a servicios bancarios o financieros; el 56,5 % interrumpieron el uso de servicios gubernamentales; el 55,2 % abandonaron sus estudios y el 52,3 % no acudieron a servicios de salud.

Programa Balcão Gov.br: inclusión digital presencial

Las iniciativas para promover la inclusión digital y simplificar el acceso a los públicos digitales resultan fundamentales para democratizar el uso de las IPD. El programa Balcão Gov.br es un ejemplo de este enfoque. Creado por la Secretaría de Gobierno Digital del MGI en el actual gobierno de Luiz Inácio Lula da Silva (2023-presente), establece un servicio presencial en colaboración con unidades acreditadas, ofreciendo asistencia humanizada a las usuarias y usuarios de la cuenta Gov.br.

En 2025, Balcão Gov.br recibió el premio GovTech Prize en la categoría de mejor servicio gubernamental del mundo centrado en el ciudadano, un reconocimiento internacional que acredita su relevancia (Brasil, 2025).

Aunque el programa representa un avance reciente en la promoción de la inclusión digital, existe un problema significativo relacionado con el acceso seguro y autónomo a los servicios públicos digitales. En este sentido, el programa busca responder a una situación persistente: muchas personas, al enfrentar dificultades en la plataforma Gov.br, dependen de agentes externos para obtener ayuda, como contadores¹⁰⁸ and cybercafé employees, a situation that exposes them to information security vulnerabilities.

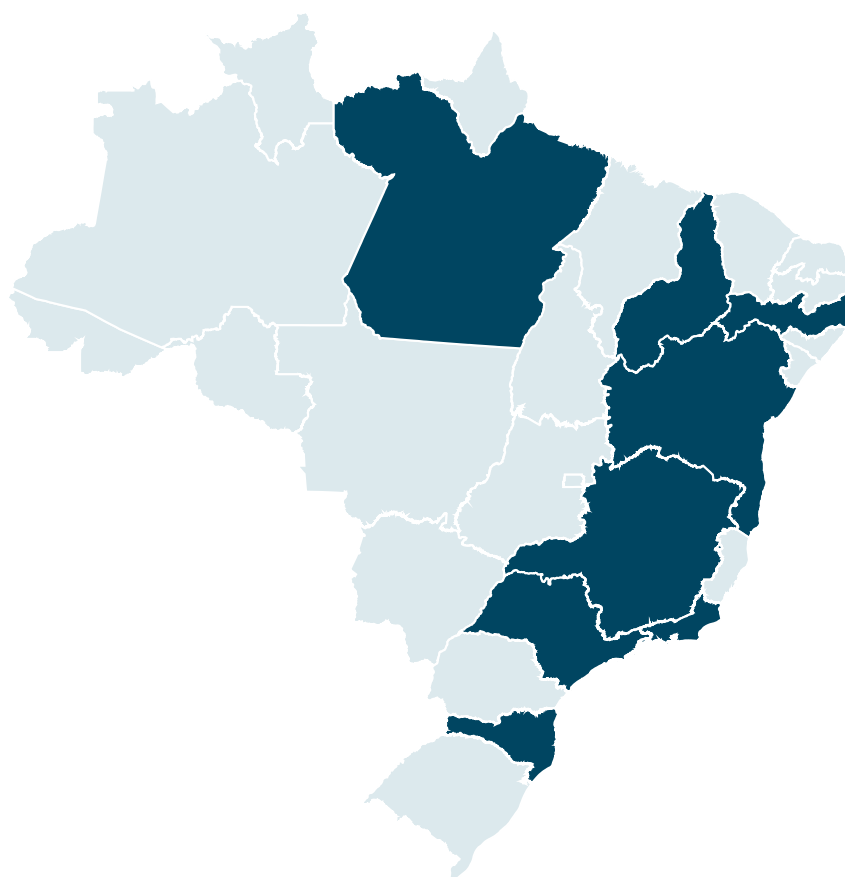
107. Práctica según la cual las operadoras de telecomunicaciones permiten a los clientes, incluso después de haber agotado su franquicia de datos, seguir utilizando determinados servicios o aplicaciones sin costos adicionales.

108. A pesar de la práctica frecuente de compartir credenciales personales con terceros, la plataforma Gov.br cuenta con una funcionalidad de poder digital que permite al ciudadano (otorgante) autorizar a otra persona (apoderado), como un contador, a representarlo en el uso de los servicios digitales de la Secretaría de Hacienda, como el e-CAC, sin necesidad de compartir contraseñas personales. Este poder puede ser registrado directamente en el portal Gov.br por usuarios con cuenta de nivel plata u oro, con validación automática e inmediata, lo que garantiza la seguridad y la practicidad en el acceso delegado.

El público objetivo comprende a las ciudadanas y los ciudadanos que necesitan apoyo con la cuenta Gov.br, especialmente las personas mayores, sin acceso a Internet o con baja alfabetización digital. En fase de expansión, el programa cuenta actualmente con 82 unidades de atención distribuidas en 66 municipios de 9¹⁰⁹ estados, según la Figura 27 (Brasil, 2025).

La relevancia del programa Balcão Gov.br se hace aún más evidente en situaciones en las que el acceso precario a Internet - o el propio mal funcionamiento de la plataforma - dificulta o impide el acceso a derechos constitucionales. Un caso emblemático está siendo investigado por el Ministerio Público Federal, en el que pacientes renales en Roraima no pudieron programar consultas en la plataforma y temían, por lo tanto, perder el acceso al Tratamiento Fuera del Domicilio (TFD)¹¹⁰.

Figura 27. Presencia de Balcão Gov.br en Brasil



Fuente: Atención Presencial Gov.br (2025).

109. Estos datos corresponden al 6 de septiembre de 2025, fecha de la última consulta.

110. Disponible en: <<https://g1.globo.com/rr/roraima/noticia/2025/01/11/pacientes-renais-nao-conseguem-marcas-consultas-por-aplicativo-em-roraima-e-temem-perder-tfd.ghtml>>. Consultado el: 3 de octubre de 2025.

El Programa Balcão Gov.br se estructura en cinco ejes estratégicos¹¹¹:

- 1. Habilidades digitales:** los asistentes ayudan y orientan a las personas sobre cómo acceder de forma autónoma a los servicios públicos digitales disponibles en línea.
- 2. Acceso a Internet:** el programa ofrece conexión gratuita a Internet en las unidades participantes, lo que facilita el acceso a los servicios públicos digitales.
- 3. Uso seguro de la cuenta Gov.br:** con un enfoque en la seguridad digital preventiva, los asistentes ayudan y orientan a las personas que tienen dificultades para acceder a la cuenta Gov.br de forma segura.
- 4. Inclusión digital:** garantiza que todas las personas puedan ejercer plenamente su ciudadanía digital, utilizando los servicios públicos en línea a través de la cuenta Gov.br, independientemente de sus condiciones socioeconómicas o su nivel de familiaridad con la tecnología.
- 5. Confianza y beneficios digitales:** a través de servicios informativos, los equipos explican las ventajas de las plataformas digitales del gobierno, promoviendo una mayor confianza, adhesión y compromiso de la población.

¹¹¹. Para más información, visite el sitio web del [Programa Balcão Gov.br](https://www.gov.br/balcao)

Resultados y expansión

Entre mayo y agosto de 2024, el proyecto piloto del Balcão Gov.br operó con 53 puntos de atención presencial, atendiendo a 25 000 personas (Gov.br, 2025) Según una encuesta de satisfacción, durante este periodo de prueba, el 95 % de los usuarios vieron resueltos sus problemas y la mitad adquirió los conocimientos y la confianza necesarios para utilizar la plataforma de forma autónoma (Gov.br, 2025).

El programa cuenta actualmente con 140 mil brasileños y brasileñas. El objetivo del gobierno federal para diciembre de 2025 es alcanzar los 250 puestos distribuidos por los estados brasileños, ampliando progresivamente esta cobertura (Gov.br, 2025).

La adhesión de poblaciones anteriormente excluidas a la cuenta Gov.br, así como la instalación de la aplicación en sus dispositivos móviles, indica un proceso de democratización del acceso a las herramientas digitales del Estado. Según el gobierno federal, este movimiento va acompañado de una alfabetización digital funcional, suficiente para la navegación y el uso básico de los servicios disponibles en la plataforma unificada (Gov.br, 2025).

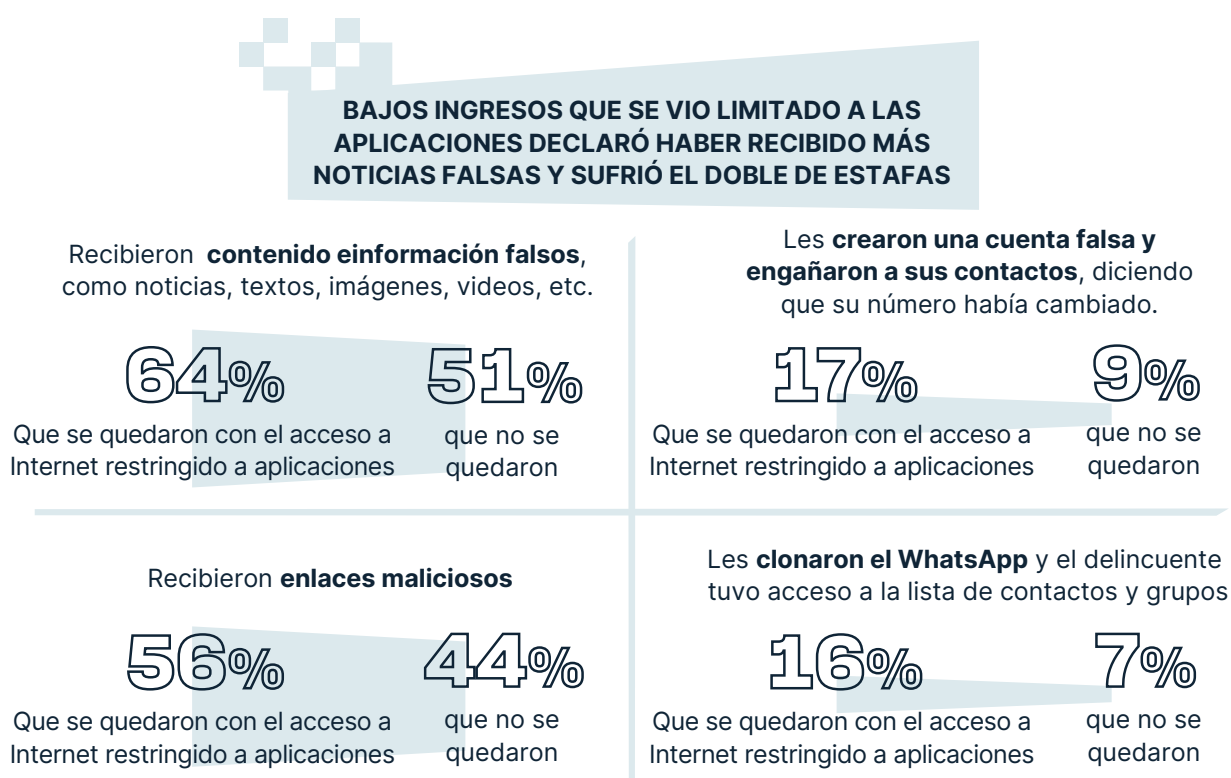
Seguridad



Cualquier persona con acceso a Internet está potencialmente expuesta a la desinformación, el fraude y las estafas. Sin embargo, esta exposición se produce de forma desigual. Los consumidores de las clases C, D y E se enfrentan a niveles más elevados de vulnerabilidad digital, una situación agravada por los paquetes de datos que restringen el acceso a Internet a las aplicaciones patrocinadas.

Una investigación realizada por el IDEC y el Instituto Locomotiva (2021, p.19) revela que el 56% de las personas entrevistadas ya han recibido noticias falsas y el 49% informaron haber recibido enlaces maliciosos. La diferencia entre las personas con acceso restringido e irrestricto a Internet también es significativa: entre aquellas con acceso irrestricto, el 51% declaró haber recibido contenidos falsos; entre quienes tienen acceso limitado, ese número aumenta al 64%.

Figura 28. Desinformación en las clases C, D y E



Fuente: IDEC e Instituto Locomotiva, 2021.

La práctica de no descontar el consumo de aplicaciones patrocinadas - especialmente por grandes empresas tecnológicas - en los planes de datos vendidos por los operadores de telecomunicaciones puede parecer beneficiosa para los consumidores de las clases C, D y E, pero, en realidad, sesga los usos de Internet y viola la neutralidad de la red, garantizada por el Marco Civil de Internet.

En el modelo de tarifa cero, el tráfico de datos a través de determinadas aplicaciones no se contabiliza durante la vigencia de la franquicia. Cuando se agota la franquicia, solo sigue estando disponible el acceso a las aplicaciones patrocinadas.

Una investigación de Anatel (2025), realizada con el apoyo del IDEC, indica que más de un tercio de la población brasileña se quedó sin acceso a Internet móvil por falta de franquicia de datos. Entre aquellos con ingresos de hasta un salario mínimo, el 11,6 % permaneció más de 15 días sin conexión móvil, mientras que tres de cada diez personas de las clases más pobres posponen el acceso a Internet hasta encontrar una red Wi-Fi para ahorrar franquicia.

En cuanto a las estafas, el número de usuarios que tuvieron cuentas falsas creadas y contactos engañados casi se duplicó: 9 % entre las personas con Internet sin restricciones y 17 % con Internet restringido. Las estafas relacionadas con la clonación de WhatsApp, la principal aplicación de mensajería instantánea utilizada en Brasil, con acceso directo a la lista de contactos y grupos, afectaron dos veces más al grupo con Internet restringido: el 16 % de los encuestados afirmó haber sufrido alguna estafa, frente al 7 % de los que tenían acceso ilimitado a Internet (Idec e Instituto Locomotiva, 2021, p. 20).

Vulnerabilidad de las IPD y casos recientes de fraude

La creciente digitalización de los servicios públicos y la centralización de información confidencial en plataformas como Gov.br han aumentado significativamente los riesgos de exposición al fraude, especialmente para los usuarios con menor alfabetización digital o con acceso restringido a Internet.

En diciembre de 2024, se reveló la actuación de una organización criminal especializada en la invasión de cuentas de Gov.br para realizar préstamos y poderes fraudulentos, utilizando datos personales obtenidos ilícitamente (G1, 2024). Las víctimas denunciaron la clonación de cuentas, con cambios de correo electrónico y número de teléfono, lo que permitió al grupo acceder a documentos como la tarjeta de trabajo, la identidad digital y la licencia de conducir, a menudo para realizar transacciones de alto valor.

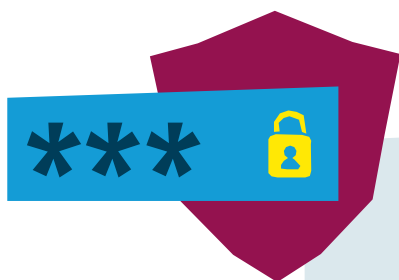
En mayo de 2025, la Policía Federal reveló la sospecha de que alrededor de 3000 cuentas de Gov.br habían sido fraudulentas a través de la biometría facial, utilizando imágenes de personas fallecidas para acceder a beneficios financieros o contratar préstamos consignados (UOL, 2025). El grupo logró

burlar el sistema de liveness, que tiene como objetivo garantizar que el usuario sea una persona viva y real, demostrando tanto el alto dominio técnico para defraudar los mecanismos de seguridad basados en el reconocimiento facial como las limitaciones de la actual infraestructura de seguridad digital del Estado.

A continuación, presentamos algunas modalidades de estafas relacionadas con Gov.br¹¹²:

Phishing

Cómo funciona: El estafador envía correos electrónicos, SMS, mensajes de WhatsApp o enlaces falsos que imitan las comunicaciones oficiales de Gov.br, de organismos gubernamentales (Servicio de Impuestos Federales, INSS) o de bancos. Estos mensajes suelen contener un enlace que dirige a la víctima a una página falsa idéntica al sitio oficial de Gov.br o al de un banco.



Objetivo: Capturar credenciales de acceso (CPF y contraseña de Gov.br), datos bancarios, información personal y, en algunos casos, instalar software malicioso.

Ejemplo: Un correo falso informando sobre un supuesto beneficio a recibir o una pendiente en la declaración del impuesto sobre la renta, solicitando hacer clic en un enlace para “regularizar la situación”.



¹¹². Los golpes enumerados se basan en investigaciones y materiales previos elaborados por Idec. Para más información, consulte: <https://idec.org.br/era-dos-golpes>.

Estafas de “actualización de registro” o “validación de datos”

Cómo funciona: La víctima recibe un mensaje (correo, SMS, WhatsApp) solicitando una “actualización urgente” o “validación de registro” en Gov.br, bajo amenaza de bloqueo de la cuenta o pérdida de acceso a servicios. El enlace proporcionado dirige a un sitio web falso.



Objetivo: Robar datos de acceso u otra información personal.

Boletos y comprobantes falsos

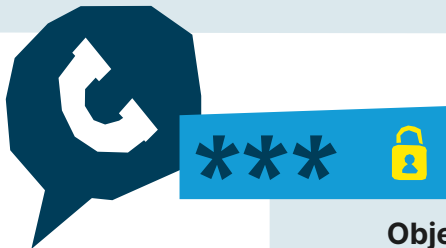
Cómo funciona: Los estafadores crean boletos falsos o comprobantes de pagos/recepciones que supuestamente provienen de servicios accesibles por Gov.br (como FGTS, devolución de IR, tasas gubernamentales). Estos documentos falsos suelen enviarse por correo electrónico o SMS.



Objetivo: Lograr que la víctima pague una cantidad indebida o proporcione sus datos bancarios.

Ingeniería Social (Llamada/Contacto Directo)

Cómo funciona: El estafador contacta a la víctima por teléfono, fingiendo ser de un organismo gubernamental, del soporte de Gov.br o de un banco. Utiliza tácticas de persuasión para obtener información confidencial o inducir a la víctima a realizar alguna acción (como instalar una aplicación, facilitar un código de seguridad o transferir dinero).



Objetivo: Robar dinero, datos o obtener acceso remoto al dispositivo de la víctima.

Oferta de beneficios falsos

Cómo funciona: Mensajes o anuncios prometen acceso a beneficios sociales, ayudas, préstamos o programas gubernamentales inexistentes o a los que la víctima no tiene derecho. Para “liberar” el beneficio, solicitan información personal o bancaria, o incluso el pago de tasas.



Objetivo: Robar datos y/o extorsionar dinero.

Aplicaciones falsas de Gov.br o de Servicios Públicos

Cómo funciona: Los estafadores crean aplicaciones fraudulentas que imitan a las oficiales de Gov.br o de servicios públicos (por ejemplo: «Consulta FGTS Fácil», «Mi INSS Rápido»). Se difunden fuera de las tiendas oficiales (Google Play Store o Apple App Store) o mediante *enlaces* maliciosos.



Objetivo: Instalar *malware*, robar información de inicio de sesión u otra información personal.

Ante el aumento de las estafas destinadas a obtener acceso indebido a la cuenta Gov.br para prácticas ilícitas, la seguridad de las IPD constituye un elemento fundamental. La seguridad puede entenderse desde una doble dimensión: i) la mejora individual por parte del propio usuario; y ii) la mejora a nivel de infraestructura, es decir, en el diseño de las IPD.

En cuanto a la primera dimensión, existen alternativas que el propio usuario puede aplicar para hacer más segura su cuenta Gov.br, como la autenticación de dos factores (2FA). Con esta técnica, se añade una capa adicional de seguridad a la cuenta; una vez activada la 2FA, el usuario deberá introducir un código temporal generado por la aplicación¹¹³.

Para activar la autenticación de dos factores, el usuario debe tener una cuenta Gov.br de nivel plata u oro¹¹⁴ e instalar la aplicación Gov.br en un dispositivo móvil. Cabe destacar que cada dispositivo móvil solo puede vincularse a una cuenta Gov.br, lo que imposibilita compartir un mismo dispositivo entre varios usuarios.

113. Para obtener más información sobre la autenticación de dos factores en la cuenta Gov.br, visite: <https://www.gov.br/governodigital/pt-br/acessibilidade-e-usuario/atendimento-gov.br/duvidas-na-conta-gov.br/ativar-a-verificacao-em-duas-etapas>.

114. En un comunicado oficial, el Ministerio de Gestión e Innovación en Servicios Públicos anunció, en julio de 2025, que todos los usuarios que tengan cuentas Gov.br de nivel oro serán orientados a activar la 2FA. La medida busca mejorar la ciberseguridad de los 72 millones de personas que tienen cuentas de este nivel (MGI, 2025).

Otra medida en favor de la seguridad consiste en el uso de contraseñas fuertes y complejas, que combinen caracteres alfanuméricos (letras mayúsculas, minúsculas y números) y caracteres especiales (como signos de exclamación, signos de dólar, entre otros). El uso de contraseñas seguras reduciría las posibilidades de intrusión por ataque de fuerza bruta, es decir, por ensayo y error o cualquier otra técnica utilizada por los intrusos. Además de las contraseñas seguras, es importante evitar la repetición de las mismas contraseñas para diferentes cuentas y servicios *en línea*.

En cuanto a la segunda dimensión de la seguridad de una IPD, es importante destacar que, además de las posibilidades de mejora individual, es fundamental que la seguridad se considere, desde el diseño de una IPD, como un elemento crítico de su desarrollo. Esta atención a la construcción de una infraestructura segura, como elemento crítico del proyecto, se debe al hecho de que plataformas como Gov.br se alimentan de un gran volumen de datos personales.

Arquitectura de la información y bases de datos biométricas

En términos de arquitectura informacional, el Gov.br opera actualmente con tres bases de datos biométricos: i) la Cédula de Identidad Nacional (CIN), mantenida por los institutos de identificación del Distrito Federal y de los estados; ii) la Identificación Civil Nacional (ICN), administrada por el Tribunal Superior Electoral (TSE); y iii) la Licencia Nacional de Conducción (CNH), gestionada por la Secretaría Nacional de Tránsito (Senatran) (MGI, s.f.).

Una investigación realizada por la organización Data Privacy Brasil demuestra que la Ley 13.444/2017 optó por una estructura de datos centralizada, en la que una sola base —la ICN— reuniría principalmente la base de datos biométricos de la Justicia Electoral, la base de información del Sistema Nacional de Información del Registro Civil (SIRC) y la base de datos del Registro Civil Nacional (CRC Nacional). Según la investigación, la elección de un modelo centralizado puede debilitar la arquitectura informacional y, en consecuencia, la seguridad e integridad de la información contenida en dichas bases (Bioni et al., 2022). Además, surgen cuestiones relativas a la calidad de los datos

personales, dado que un mismo ciudadano puede tener sus datos biométricos registrados en todas las bases actualmente utilizadas por Gov.br. La elección por la interoperabilidad de los datos debe mantenerse y promoverse, con el objetivo de reducir el uso de bases centralizadas.

Accountability, transparencia y gobernanza participativa

Más allá de los aspectos de *diseño*, debe garantizarse a la población la posibilidad de acompañar el desarrollo de las infraestructuras públicas digitales. Así, el principio de *accountability* - traducido como responsabilidad y rendición de cuentas- presente en la Ley General de Protección de Datos Personales (LGPD), junto con el principio constitucional de transparencia, se vuelven esenciales para dicho monitoreo.

De estos principios derivan herramientas como el Informe de Impacto a la Protección de Datos Personales (RIPD)¹¹⁵, fundamentales para la evaluación de riesgos. La realización y publicación periódica de estos informes constituyen no solo buenas prácticas, sino una obligación del poder público, que somete la política pública al escrutinio de la sociedad y posibilita la creación de mecanismos de gobernanza participativa (Bioni et al., 2022).

115. Puede encontrar más información sobre el RIPD en: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>. Consultado el: 3 de octubre de 2025.

El caso de la “degustación” de datos del Gov.br

En 2022, se firmaron acuerdos de cooperación técnica entre la Secretaría de Gobierno Digital, vinculada al Ministerio de Economía, y asociaciones representativas del sector bancario brasileño, como la Federación Brasileña de Bancos (Febraban) y la Asociación Brasileña de Bancos (ABBC). Dichos acuerdos permitían la “degustación experimental” por un período de 12 meses de los datos biométricos y biográficos de millones de brasileños registrados en Gov.br y en la base de la Identificación Civil Nacional (ICN). La justificación oficial era el uso temporal y controlado con fines de validación y mejora de servicios; sin embargo, los términos eran tan genéricos que generaban dudas sobre las bases legales, la finalidad pública legítima y los procedimientos de control y consentimiento de los titulares de los datos.

El Ministerio Público Federal (MPF), a partir de un procedimiento iniciado tras una denuncia del diputado Carlos Veras (PT/PE), comenzó a investigar las posibles irregularidades de estos acuerdos, cuestionando la legalidad del intercambio de datos, la amplitud del acceso concedido, los mecanismos de seguridad para evitar filtraciones o usos indebidos, y la conformidad con los principios de la LGPD, como finalidad, transparencia, responsabilidad y rendición de cuentas.

La reacción de la sociedad civil organizada, especialmente de la Coalizão Direitos na Rede, del Idec y de Data Privacy Brasil, fue inmediata, cuestionando la transparencia de los acuerdos y la posible violación de la LGPD. Se destacó que el compartir datos sensibles con instituciones financieras privadas, sin el consentimiento claro y detallado de los titulares, además de poner en riesgo la privacidad y los derechos fundamentales de los ciudadanos, podría sentar precedentes peligrosos para la protección de datos en el sector público.

La repercusión fue tal que el Ministerio de Economía suspendió temporalmente las pruebas en curso, evidenciando la necesidad de cautela en los proyectos que involucren datos personales sensibles a gran escala.

Soberanía



Según la Organización de las Naciones Unidas (ONU), la soberanía nacional figura entre los principios fundamentales del derecho internacional, con el objetivo de afirmar la independencia y la autoridad de los Estados-nación para gobernar dentro de los límites de su jurisdicción interna, sujetos a las obligaciones del derecho internacional y de los tratados de los que son signatarios (ONU, s.f.).

En el contexto brasileño, la soberanía está prevista como principio en todas las constituciones nacionales, ya sea de forma explícita o implícita (Oliveira, 2000). La Constitución de 1988 consagra la soberanía como el primer fundamento de la República, tal y como se establece en su artículo 1 (Oliveira, 2020).

Este concepto convencional de soberanía se ha visto influido por las transformaciones políticas, económicas, sociales y culturales vividas por la comunidad internacional a lo largo de la historia. Más allá de la expresión soberanía nacional, hoy en día se debate la soberanía digital, un concepto poco común hace décadas, dado que el desarrollo de las TIC, en especial de Internet, ha desafiado la noción clásica de soberanía (Silveira y Xiong, 2025).

Sin embargo, este concepto sigue siendo objeto de controversia no solo en la burocracia estatal, ya que cada funcionario público lo interpreta a su manera, sino también entre los demás sectores de la sociedad, dado que algunos agentes privados han capturado la noción de soberanía en el desarrollo de infraestructuras digitales.

Las diferentes interpretaciones sobre la soberanía digital surgen en medio de una difusión de perspectivas que van desde la seguridad nacional hasta los aspectos legales, desde la autodeterminación económica (incluido el desarrollo tecnológico y científico) hasta la protección de los derechos, pasando por la capacitación de los ciudadanos y las comunidades tradicionales. No es posible identificar un significado único para este concepto, ya que surgen diferentes significados según quién enuncia e interpreta la noción de soberanía digital (Camelo et al., 2024, p. 14).

Sin embargo, se puede afirmar que dicho concepto se originó a partir del de “soberanía tecnológica” empleado en 1967 por el Consejo de Ciencia de Canadá como política pública indispensable para el desarrollo nacional (Globerman, 1978). Desde entonces, han surgido nuevas interpretaciones, sobre todo basadas en las transformaciones provocadas por la difusión de las tecnologías cibernéticas de la información y la comunicación (Schiavi y Silveira, 2022).

En una investigación reciente, Sérgio Amadeu da Silveira y Jeff Xiong (2025) señalaron diferentes perspectivas de soberanía digital que van desde una

conceptualización aproximada y analógica hasta la soberanía alimentaria — noción que representaría más que un concepto jurídico, indicando la autonomía de las comunidades para elegir qué comer, qué y cómo plantar, sin estar sujetas a las imposiciones de las grandes corporaciones— hasta una noción de soberanía digital que describe la capacidad de las comunidades y los Estados para ejercer tanto el control como la gobernanza sobre sus infraestructuras tecnológicas.

Soberanía de datos y el sector público

Actualmente, el sector privado ha empleado la expresión soberanía de datos en lugar de soberanía digital. Las empresas transnacionales de TI abordan el tema cuando se discuten las diferencias regulatorias entre países en los contratos o cuando pretenden vender productos y servicios de tratamiento remoto de datos o computación en la nube que podrían mitigar los riesgos para la soberanía nacional en el ámbito digital.

International Business Machines Corporation (IBM), por ejemplo, no solo define la “soberanía de datos”, sino que la distingue de la “residencia de datos”. Para esta empresa estadounidense, la soberanía de datos sería el principio de que las naciones tienen autoridad reguladora, es decir, legal, sobre los datos generados o tratados computacionalmente dentro de sus fronteras nacionales, mientras que la residencia de datos se refiere a la ubicación geográfica de estos datos, es decir, el espacio físico donde se encuentran los centros de tratamiento computacional de datos (centros de datos), servidores u otros sistemas que los almacenan. (Kosinski, 2025).

Con la denominada transformación digital del Estado, la soberanía digital y la soberanía de los datos surgen como cuestiones centrales para la administración pública. Después de todo, con la intensa digitalización de las infraestructuras públicas, también se intensifica la dependencia del Estado respecto a las empresas transnacionales de TI (Lablivi, 2024). Para los administradores y administradoras públicos de Brasil, es fundamental comprender estos conceptos y adoptar prácticas que garanticen el control y la independencia en el tratamiento computacional de los datos de la población y de las infraestructuras públicas digitales.

El gobierno de Luís Inácio Lula da Silva (2023-presente) ha invertido hasta ahora 1200 millones de reales en la construcción de su nube gubernamental²⁵, justificando esta iniciativa como una medida de soberanía digital y ciberseguridad para Brasil.

116. Para obtener más información y una definición del término “nube gubernamental”, visite el sitio web: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ambiente-tecnologico/nuvem/nuvem-de-governo>

Figura 29. Propaganda no website do Serpro*



Fuente: Serpro (2025)

***Soberanía para los datos del poder público**

Infraestructura en la nube de gestión 100 % nacional, alojada en los centros de datos de Serpro, con garantía de soberanía y privacidad de los datos, incluidos los confidenciales y secretos.

La nube gubernamental y la cuestión de la soberanía digital

El proyecto, que forma parte del Plan Brasileño de Inteligencia Artificial (PBIA), tiene como objetivo mantener los datos de la población bajo jurisdicción nacional, utilizando infraestructuras informáticas remotas gestionadas por las empresas estatales Serpro y Dataprev. Según Rogério Mascarenhas, secretario de gobierno digital del MGI, la medida pretende repatriar los datos públicos transferidos a proveedores extranjeros durante la administración del expresidente Jair Bolsonaro (2019-2022) (Teixeira, 2025).

La nube gubernamental – o nube soberana, como se denomina en las publicaciones oficiales – utiliza servicios de tratamiento de datos de grandes empresas transnacionales como Google, Huawei, Amazon, Microsoft, IBM, Oracle y Tencent. Sin embargo, establece como condición que todos los datos se almacenen y permanezcan en territorio brasileño (Teixeira, 2025), lo que se aproxima a la noción de localización de datos (*data localisation*), concepto que describe las prácticas de almacenamiento y procesamiento de datos en

una determinada ubicación geográfica o jurisdicción (Del Giovane, Ferencz, González, 2023).

Como se muestra en la Figura 30, la nube gubernamental tiende a promover asociaciones entre empresas tecnológicas internacionales, como Amazon (Brasil, 2020).

En 2019, Serpro realizó una convocatoria pública para identificar proveedores de servicios en la nube en las modalidades de infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y *software* como servicio (SaaS) interesados en ofrecer dichos servicios en una plataforma multinube. En marzo de 2020, la empresa estatal estableció su primera asociación público-privada (APP) derivada de esta convocatoria con *Amazon Web Services* (AWS) por un valor de 71,2 millones de reales.

Figura 30. Extracto de la asociación público-privada (APP)*



*** BOLETÍN OFICIAL DEL ESTADO**

Publicado el 23/03/2020 | Edición 56 | Sección 31 | Página 28

Órgano: Ministerio de Economía / Servicio Federal de Procesamiento de Datos

EXTRACTO DE CONTRATO DE ASOCIACIÓN N.º 76 043/2020 - UASG 806030

Expediente N.º: 00232-2020. Contratante: SERVICIO FEDERAL DE PROCESAMIENTO DE DATOS (SERPRO). Contratada: AMAZON WEB SERVICES, INC. Objeto: Asociación comercial con un proveedor de servicios en la nube en las modalidades de Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Fundamento Jurídico: Artículo 28, §3, inciso II y §4 de la Ley 13.303/2016. Vigencia: del 02/03/2020 al 01/03/2025. Valor: R\$ 71.200.910,03. Fecha de la firma: 02/03/2020. Nota de compromiso: 2020NE000302.

Fuente: Ministerio de Economía (2020).

El dispositivo jurídico que permitió al Serpro justificar la contratación de Amazon Web Services fue el **Artículo 28 de la Ley 13.303/2016**, conocida como Ley de las Empresas Estatales:

Art. 28. Los contratos con terceros destinados a la prestación de servicios a las empresas públicas y sociedades de economía mixta incluidos los de ingeniería y publicidad, a la adquisición y arrendamiento de bienes, a la enajenación de bienes y activos integrantes del respectivo patrimonio o a la ejecución de obras que pasen a formar parte de dicho patrimonio, así como a la implementación de gravámenes reales sobre tales bienes, deberán ser precedidos de licitación conforme a los términos de esta Ley, salvo en los casos previstos en los arts. 29 y 30. [...]

*§ 3 Las empresas públicas y sociedades de economía mixta **quedan exentas** del cumplimiento de las disposiciones de este Capítulo en las siguientes situaciones: [...]*

II - en los casos en que la elección del socio esté asociada a sus características particulares, vinculada a oportunidades de negocio definidas y específicas, debidamente justificada la inviabilidad de un procedimiento competitivo. (Brasil, 2016, énfasis nuestro).

Desde la promulgación de la Ley 13.303/2016, se han establecido otras PPPs que siguen este modelo, el cual dispensa la licitación en situaciones específicas, como contrataciones entre empresas estatales y sus subsidiarias, siempre que los precios sean compatibles con los del mercado. Hasta 2022, se totalizaron 198,6 millones de reales en contratos con grandes empresas transnacionales de tecnología de la información.

En 2021, se firmó la segunda asociación de servicios en la nube con la empresa china Huawei, por un valor de 23 millones de reales. Ese mismo año se firmaron contratos con Microsoft (22,6 millones) y con Oracle (41,5 millones). En 2022, se celebró un acuerdo con IBM por 40,3 millones de reales (Cassino, 2025).

Originalmente, la idea de estas asociaciones consistía en que el Serpro ofreciera los productos y servicios de esas transnacionales a sus propios clientes (estados y municipios). A partir de 2023, hubo un cambio de estrategia: el Serpro volvió a priorizar sus propios centros computacionales de procesamiento de datos, aunque utilizando las soluciones de nube gubernamental o “soberana”

ofrecidas por socios privados, empresas transnacionales de TI, en su mayoría con sede en Estados Unidos.

Según explica Cassino (2025), fue en ese momento cuando el Serpro cambió su orientación. Si antes los servicios contratados por los clientes de la estatal podían permanecer en los centros de procesamiento de las grandes transnacionales de TI, ahora los servicios deben permanecer dentro de sus propios centros. La empresa estatal pionera en el procesamiento computacional de datos de la población brasileña construyó entonces su infraestructura pública digital propia, adquiriendo componentes físicos (*hardware*) y lógicos (*software*) de grandes empresas transnacionales de TI. Sin embargo, como se verá más adelante, este cambio de orientación aún no es suficiente para garantizar la plena soberanía digital de Brasil.

Dependencia tecnológica y vulnerabilidades jurídicas

Aunque la nube gubernamental de Serpro se ofrece como un servicio de soberanía de datos, sigue dependiendo de proveedores extranjeros y de una infraestructura híbrida formada por socios públicos y privados. Según Cassino (2025, p. 144), persiste “la posibilidad de transferir datos sin la autorización de las autoridades brasileñas”.

El marco jurídico-legal de los Estados Unidos, país donde tienen su sede la mayoría de estas empresas privadas de TI, tiene una gran capacidad para hacer que colaboren con sus agencias gubernamentales.

A modo de ejemplo, los Estados Unidos, mediante la Ley N.º 103-414 de 1994, promulgaron la *Communications Assistance for Law Enforcement Act* (CALEA), que exige que las empresas de tecnología y los proveedores de servicios incorporen en sus productos y redes la capacidad técnica necesaria para que agencias gubernamentales, como el FBI, puedan realizar interceptaciones electrónicas legalmente autorizadas. Esta ley obliga a las empresas a diseñar sus infraestructuras digitales de manera que el acceso gubernamental para fines de vigilancia sea posible en caso de existir una orden judicial.

Otra normativa estadounidense a considerar es la *Clarifying Lawful Overseas Use of Data* (CLOUD) Act de 2018, que exige que las empresas tecnológicas estadounidenses, como Google y Microsoft, proporcionen datos de usuarios a las autoridades de los Estados Unidos, sin importar dónde se encuentren almacenados dichos datos. Esto significa que, incluso si los datos se encuentran en servidores ubicados en Brasil, las empresas de ese país pueden estar legalmente obligadas a entregarlos a su gobierno.

El análisis de los contratos entre el Serpro y las empresas transnacionales de tecnología de la información revela la subordinación digital de Brasil a tales legislaciones extranjeras, más allá de las cuestiones de espionaje. Por razones contractuales, este servicio remoto puede ser interrumpido en cualquier momento. Además, no existe posibilidad de transferencia de tecnología, ya que la propiedad de los sistemas ni siquiera puede ser garantizada: estos deben ser destruidos o dejar de utilizarse al finalizar los contratos.

Los sistemas son cerrados y no auditables, con riesgo de introducción de códigos que podrían actuar como un *kill switch*,¹¹⁷ inutilizando el funcionamiento de dichas soluciones computacionales.

Ejemplo: Caso de le Tribunal Penal Internacional y reacciones europeas

El impacto práctico de estas situaciones se evidenció en el caso que involucró a Microsoft y al Tribunal Penal Internacional (TPI). Tras la emisión de una orden de arresto contra el primer ministro israelí Benjamin Netanyahu, el gobierno de los Estados Unidos impuso sanciones al TPI, con sede en La Haya, Países Bajos. Según *Associated Press*, como consecuencia, el gobierno estadounidense obligó a *Microsoft* a bloquear la cuenta de correo electrónico oficial de Karim Khan, fiscal jefe del Tribunal¹¹⁸. El episodio, posteriormente negado por la empresa¹¹⁹, generó una fuerte reacción en el gobierno neerlandés, que comenzó a reevaluar críticamente su dependencia de infraestructuras digitales controladas por empresas extranjeras, especialmente estadounidenses. Las autoridades del país han advertido sobre los riesgos estratégicos que conlleva mantener datos sensibles bajo jurisdicción extranjera, incluso en instituciones como el banco central, cuyo sistema de pagos nacional (iDEAL) depende en gran medida de empresas estadounidenses.

Bart Groothuis, miembro liberal holandés del Parlamento Europeo, solicitó la creación de una nube europea, citando el incidente del TPI. Los legisladores neerlandeses han solicitado al gobierno que, para 2029, el 30 % del uso de servicios en la nube provenga de los Países Bajos o Europa, además de otras medidas para reducir la dependencia de servicios estadounidenses, como los de Microsoft.

117. En informática, la expresión *kill switch* se refiere a un mecanismo diseñado para desactivar (o apagar) de inmediato un sistema, dispositivo o software en caso de emergencia o compromiso de seguridad.

118. Disponible en: <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>. Consultado el: 3 de octubre de 2025

119. Disponible en: <https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/> Consultado el: 3 de octubre de 2025

Recientemente, el estado de Schleswig-Holstein, en Alemania, anunció la sustitución de *Microsoft Teams* y la suite *Office* por soluciones de código abierto, como LibreOffice y el proveedor de correo electrónico *OpenXchange*, afectando a aproximadamente 60.000 empleados públicos¹²⁰. Esta medida, que se implementará en los próximos meses, también prevé la adopción del sistema operativo *Linux* en los próximos años.

Según Dirk Schrödter¹²¹, Ministro de Digitalización del Estado, el objetivo es recuperar el control sobre los datos públicos y garantizar la soberanía digital de la administración pública local, reduciendo la dependencia de proveedores privados y reforzando la autonomía para auditar y personalizar sistemas, así como alojarlos en su propia infraestructura. Iniciativas como esta reflejan una tendencia creciente en Europa, donde países como Dinamarca también han promovido la migración a *software* de código abierto como forma de reducir costes y proteger los datos gubernamentales.

Preocupaciones nacionales con respecto a la IA generativa

Las filtraciones de datos a través de sistemas de inteligencia artificial (IA) también han sido motivo de preocupación para los gestores públicos nacionales. El 20 de marzo de 2025, el Consejo de Control de Actividades Financieras (COAF), organismo del Gobierno Federal vinculado al Banco Central de Brasil, expresó su desconfianza ante el uso indebido de la IA generativa al publicar en el Boletín Oficial de la Unión la Ordenanza COAF n.º 4.

El artículo 2 de la Ordenanza prohíbe *“el tratamiento de datos e información sujetos a regímenes jurídicos propios de confidencialidad, como los relacionados con la producción de inteligencia financiera, la supervisión de personas obligadas y la protección de datos personales sensibles en plataformas externas de IAG”*.

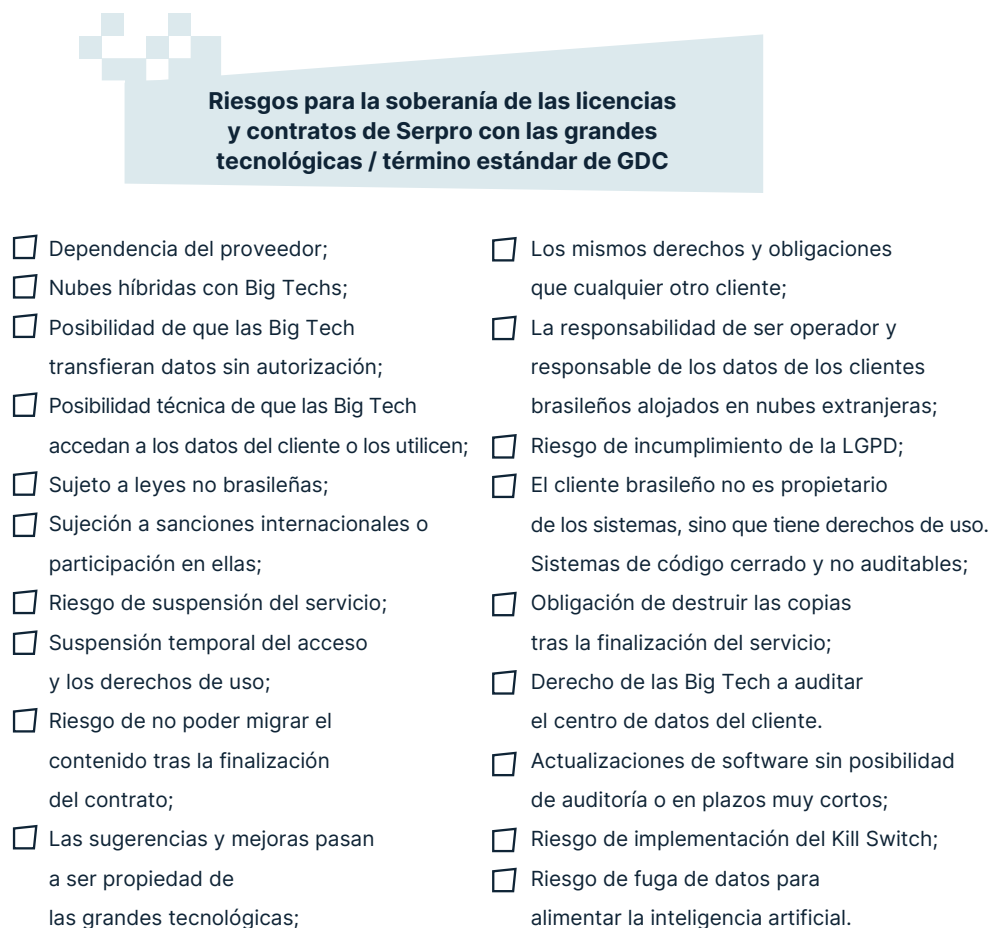
Esta prohibición también se aplica a la plataforma Microsoft Copilot, cuyo contrato de prestación de servicios está vigente con el COAF. Por lo tanto, cualquier herramienta de IA generativa deberá ser evaluada previamente por los funcionarios públicos responsables de la TI del organismo antes de ser utilizada.

120. Disponible en: <https://www.france24.com/en/live-news/20250613-we-re-done-with-teams-german-state-hits-uninstall-on-microsoft>. Consultado el: 3 de octubre de 2025.

121. La cita de Dirk Schrödter fue extraída del artículo “Soberanía digital: Esbozo de un proyecto para Brasil”, publicado por James Görden (2025) en el sitio web Otras Palabras. Disponible en: <https://outraspalavras.net/tecnologiaemdisputa/soberania-digital-esboco-para-um-projeto-para-o-brasil/>. Consultado el: 3 de octubre de 2025.

Cassino (2025) identifica una serie de riesgos para la soberanía digital de Brasil al analizar los contratos entre Serpro y grandes empresas transnacionales de TI, como se muestra en la Figura 31.

Figura 31. Risks to sovereignty in licenses and contracts between Serpro and transnational IT companies



Fuente: Cassino (2025).

En el actual gobierno de Luí Inácio Lula da Silva (2023-presente), el Ministerio de Gestión e Innovación en Servicios Públicos (MGI) se ha hecho responsable de las normas de los procesos internos de la administración federal. La Secretaría de Gobierno Digital (SGD) de este ministerio, responsable de la digitalización de los servicios públicos, ha elaborado documentos y creado servicios como la Estrategia Nacional de Gobierno Digital, la nueva Tarjeta de Identidad Nacional, el portal Gov.br, el Estándar Digital de Gobierno y la Infraestructura Nacional de Datos (IND).

La **Ordenanza SGD/MGI n.º 5.950, de 26 de octubre de 2023**, estableció un modelo de contratación de software y servicios de computación en la nube para la administración pública federal. Es a través de esta ordenanza que las empresas estatales Serpro y Dataprev están estructurando la nube del gobierno (Brasil, 2023).

En su *sitio web*, la SGD utiliza la palabra “soberanía” para explicar la importancia de este servicio público. Según la secretaria, con “una nube propia”, el gobierno garantizaría que los datos se “almacenaran en territorio nacional”, algo importante para cuestiones de soberanía e independencia tecnológica (Brasil, 2025). Sin embargo, el gobierno parece confundir “soberanía” con “ubicación de datos”, es decir, con el almacenamiento de datos dentro de un territorio determinado. However, the government seems to confuse “sovereignty” with “data localisation,” that is, with the storage of data within a specific territory.

Desafíos a la soberanía

En el tratamiento computacional remoto de datos, la simple localización de los datos no basta para garantizar la soberanía y la independencia tecnológica. Dependiendo de la arquitectura de la red que almacena y procesa los datos, así como de los equipos y componentes lógicos utilizados en dichas redes, los proveedores de las soluciones pueden acceder a información confidencial, que debería estar protegida en infraestructuras sometidas a un mayor escrutinio público.

La actual política de transformación digital del Estado brasileño aún no ha superado los retos relacionados con la pérdida de soberanía digital y el riesgo de fuga de datos. El análisis detallado del marco jurídico y el diseño de las tecnologías utilizadas revela que Brasil sigue siendo vulnerable, lo que lo hace dependiente de proveedores extranjeros. En la práctica, la contratación de servicios de computación en la nube ofrecidos por empresas transnacionales de tecnología acaba profundizando esta subordinación digital, lo que dificulta la plena garantía de la soberanía digital nacional.

Existe un claro contraste entre el discurso público en defensa de la soberanía digital y la práctica presupuestaria de Brasil, que sigue invirtiendo miles de millones de reales en contratos con grandes empresas tecnológicas extranjeras, como Google, Microsoft y Oracle. En solo un año (de junio de 2024 a junio de 2025), el gasto superó los 10 000 millones de reales, distribuidos entre los gobiernos federal (4600 millones), estatales y municipales (5400 millones), lo que demuestra una dependencia estructural que atraviesa todas las esferas gubernamentales.

Este patrón de contratación no solo refuerza la subordinación digital del país, sino que también expone los servicios públicos esenciales y los datos sensibles a riesgos de interferencia y control externo. La falta de inversiones sólidas en el desarrollo de la industria nacional de software y en soluciones tecnológicas propias contribuye a perpetuar esta dependencia, comprometiendo la autonomía del Estado y su capacidad para garantizar la seguridad y la continuidad de los servicios públicos.

Consideraciones finales

Como se destacó al inicio de este informe, Brasil tiene una larga tradición en el tratamiento computacional de los datos personales de sus ciudadanos. La creación de Serpro a mediados de la década de 1960 y de Dataprev a mediados de la década de 1970 generó una infraestructura pública que permitió el desarrollo de lo que hoy se conoce como gobierno electrónico y/o digital.

Incluidas en el Programa Nacional de Desestatización (PND) durante el gobierno de Jair Bolsonaro (2019-2022), instituido por la Ley n.º 9.491, de 9 de septiembre de 1997, estas empresas estatales de TI han demostrado ser, por diferentes razones, fundamentales para la inclusión, la seguridad y la soberanía digital del país.

El proceso de privatización de ambas, ya revertido en el gobierno de Luiz Inácio Lula da Silva (2023-presente), ignoraba por completo los riesgos para la protección de datos. En 2021, el Ministerio Público Federal (MPF) remitió una nota técnica al Ministerio de Economía advirtiendo que la privatización de Serpro amenazaría la soberanía nacional (Queiroz, 2021; Ministerio Público Federal, 2021).

Dicha Nota Técnica, elaborada por el Grupo de Trabajo de Tecnología de la Información y la Comunicación de la Cámara de Consumo y Orden Económico de la MPF, destacó que la venta de Serpro, la mayor empresa estatal de TI del mundo, entraba en contradicción con la Ley General de Protección de Datos Personales (LGPD), según la cual solo las empresas públicas pueden tratar datos personales relacionados con la seguridad pública (Torres, 2025)

En este documento, los servicios de Serpro se describieron como “esenciales” para la “seguridad nacional” y el “mantenimiento de la soberanía” del Estado brasileño, ya que “tienen por objeto garantizar la inviolabilidad de los datos gubernamentales y son de gran interés colectivo” (Torres, 2025).

La Sociedad Brasileña de Computación (SBC), una de las entidades de ciencia y tecnología más importantes del país, también publicó un manifiesto en el que expresaba su gran preocupación por la privatización de Serpro y Dataprev. La publicación, firmada por varias instituciones, alertaba sobre el riesgo de transferir estas empresas al sector privado, ya que los datos de los ciudadanos, las empresas y la administración pública deben ser conservados y protegidos por el Estado brasileño, responsable de “garantizar su privacidad, integridad, disponibilidad y autenticidad” (Torres, 2025).

Considerado un “mercado estratégico” para la instalación de centros de tratamiento computacional de datos debido a su matriz energética limpia, Brasil ha sufrido “apagones” tras la progresiva privatización de su sector eléctrico. Los expertos alertan sobre los impactos nocivos para el medio ambiente y la necesidad de priorizar la descarbonización de la industria brasileña.

El sector de las telecomunicaciones, igualmente privatizado, ha alcanzado una casi universalización en términos de conexión a Internet, pero con niveles de conectividad significativos aún bajos e insatisfactorios, como se ha demostrado anteriormente.

Aunque lidera la instalación de centros de tratamiento computacional de datos en América Latina, las cifras siguen siendo pequeñas para el tamaño y el potencial del país, además de la concentración regional en el Sudeste.

Con la creación del Centro Nacional de Tecnología Electrónica Avanzada (Ceitec), Brasil buscó ingresar al mercado internacional de semiconductores, pero la empresa enfrentó un intento de liquidación durante el gobierno de Jair Bolsonaro. En 2023, el gobierno revirtió esta decisión, retirando a Ceitec del programa de privatización y garantizando su continuidad. En 2024, se anunció una inversión de 220 millones de reales para modernizar la producción de semiconductores, especialmente de carburo de silicio, con el fin de fortalecer la cadena tecnológica nacional. A pesar de los avances, Ceitec aún enfrenta desafíos financieros y depende de inversiones continuas para garantizar su sostenibilidad y crecimiento.

El desarrollo de componentes lógicos libres (software libre) o de código abierto en Brasil fue una referencia mundial a principios de la década de 2000, pero esta política pública digital fue abandonada y el país aún sufre de escasez de mano de obra calificada en el área. El desarrollo de aplicaciones en Brasil está impulsado principalmente por empresas privadas y startups, cuya capacidad de exportación de software sigue siendo limitada, a pesar de que el país ocupa el décimo lugar en el ranking mundial del mercado de las TIC.

Las empresas transnacionales de TI están interesadas en explotar económicamente las vastas bases de datos del Estado brasileño para mejorar sus sistemas de IA. La ministra Luciana Santos reconoció el reto al afirmar que “Brasil tiene muchos datos que son codiciados por [...] las big techs” y que necesitamos “tener sus datos”, aunque todavía no existe “una integración”, “con una nube propia, soberana” y “con lenguaje brasileño” (Brasil, 2024).

Las empresas de TI de Estados Unidos constituyen una base estratégica para el ejercicio de su poder global (Fiori, 2007). La República Popular China, con sus propias características, ha desarrollado tecnologías similares que la sitúan hoy en día en una posición de independencia frente a ese poder. Brasil, al igual que el resto de países, se ha convertido en un mero consumidor, más o menos dependiente de estas tecnologías.

Al asumir la presidencia de los Estados Unidos por segunda vez en 2025, Donald Trump se acercó a Rusia, amenazó con salir de la Organización del Tratado del Atlántico Norte (OTAN) y declaró su intención de anexar Groenlandia a los Estados Unidos, poniendo en riesgo la soberanía territorial de Dinamarca. Ante este escenario geopolítico convulso, las naciones que integran la Unión Europea mostraron su malestar y elaboraron una propuesta de inversión en IPD, inspirada

en el modelo indio y conocida como “Eurostack” (Eurostack, 2025, p. 8).

Los expertos sugieren que Brasil se inspire en esta iniciativa para reducir su dependencia tecnológica. Sin embargo, otros análisis destacan las particularidades del país y advierten de los riesgos de adoptar una política industrial como esta sin las debidas adaptaciones regionales o locales. Independientemente de la inspiración efectiva, vale la pena examinar la iniciativa, ya que su objetivo es reducir la subordinación total de Europa a las empresas transnacionales de TI no europeas para los servicios prestados a la población, las empresas y los propios organismos públicos europeos, aumentando la seguridad, creando redundancia y resiliencia, así como mejorando las oportunidades de innovación y competitividad digital, al tiempo que se establecen normas de gobernanza europeas (Eurostack, 2025).

En una carta abierta firmada por más de 200 empresas europeas de TI, la iniciativa identificó los siguientes objetivos inmediatos:

1. Crear un mercado regional en el que los proveedores europeos puedan competir legítimamente y la inversión sea justificable. Esto significa que el Estado deberá “comprar europeo” (*to buy European*), es decir, satisfacer sus necesidades a partir de soluciones lideradas y montadas en Europa (reconociendo que estas pueden contar con complejas cadenas de valor de producción). El sector privado necesitará incentivos adecuados para orientar parte de su demanda hacia los proveedores europeos, permitiendo soluciones soberanas.

2. Apoyar un enfoque “federado” y normas industriales comunes que puedan proporcionar alternativas europeas de “escalabilidad”, en colaboración con la industria. Esto implica apoyar las soluciones de código abierto y la interoperabilidad (tanto técnica como comercial). Los proyectos de infraestructura digital basados en la autonomía de los componentes físicos (*hardware*) y las nubes soberanas deben tener prioridad. En el escenario actual, en el que empresas no europeas extraen valor y concentran poder a través de tecnologías propietarias, la apertura (ciencia abierta, estándares y datos abiertos) debe ser uno de los pilares de la estrategia de soberanía digital europea.

3. Desarrollar una propuesta de certificación para que los clientes de nubes públicas o privadas puedan adherirse voluntariamente a servicios de nube soberana para sus datos sensibles. Para que esta adopción tenga éxito, debe garantizar que sus datos más sensibles estén protegidos contra el acceso o la interrupción operativa derivados de leyes extraterritoriales no europeas. Esto debe abordarse a nivel regional y el *End User Computing Software* y el *European Cybersecurity Certification Scheme for Cloud Services* (EUCS) deben aumentarse a criterios *High+* o deben pausarse hasta que se encuentre una solución alternativa adecuada.

4. Revisar y/o reajustar los planes existentes en el marco de la iniciativa “Década Digital” (*Digital Decade*) con el fin de (re)asignar fondos cuando sea apropiado, dando prioridad a proyectos tangibles, relevantes para el mercado y orientados a resultados.

5. Crear un fondo de infraestructura digital soberana para apoyar las inversiones públicas, en particular en las cadenas de valor intensivas en capital (como la computación cuántica y los chips), “con un compromiso adicional significativo de fondos asignados y/o garantizados por el Banco Europeo de Inversiones (BEI) y los organismos nacionales de financiación pública”. Complementar las iniciativas ya existentes (como el sello STEP) consultando a capitales de riesgo filantrópicos, instituciones nacionales de innovación y financiación, así como fondos soberanos nacionales, para crear un sentido coordinado de propósito y desarrollo y no solo de innovación. Considerar la creación de un fondo que contemple otros fondos de “dinamismo europeo.

El desarrollo de las IPD requiere la integración de tres dimensiones fundamentales. En primer lugar, la soberanía digital debe guiar todas las etapas, desde el desarrollo hasta el mantenimiento y la gobernanza, garantizando la autonomía tecnológica y el control estatal sobre las infraestructuras críticas. En segundo lugar, la seguridad de la información y la protección de los datos personales requieren modelos basados en las mejores prácticas, con mecanismos transparentes de identificación, mitigación y supervisión de riesgos sujetos al escrutinio público. En tercer lugar, la gobernanza participativa debe involucrar de manera sustantiva a los diversos sectores de la sociedad, en especial a la sociedad civil organizada, garantizando la legitimidad democrática de las decisiones técnicas.

La inclusión digital es una condición *sine qua non* para el éxito de estas iniciativas. En un contexto en el que la digitalización del Estado digitaliza progresivamente el acceso a las políticas públicas y los beneficios sociales, las medidas de inclusión digital se vuelven imperativas. La universalización del acceso debe contemplar precisamente a aquellos grupos históricamente excluidos, so pena de profundizar las desigualdades estructurales mediante la transposición de las barreras del mundo físico al entorno digital.

Si la base del desarrollo de las IPD, como Gov.br, reside en la desburocratización y la eficiencia en la prestación de servicios públicos, la accesibilidad de la población con acceso precario o limitado a Internet no puede quedar relegada a un segundo plano, sino que constituye, por el contrario, el indicador primordial de éxito. El éxito de una IPD no se mide por el número de servicios públicos digitalizados, sino por la capacidad de incluir a segmentos que siempre han estado marginados, incluso antes de la digitalización.

Por lo tanto, es necesario fortalecer las estrategias de inclusión digital, como el Programa Balcão Gov.br, junto con el desarrollo de modalidades alternativas de acceso, como la disponibilidad de servicios offline. Solo mediante un enfoque que combine la soberanía tecnológica, la seguridad sólida, la gobernanza participativa y la inclusión digital será posible construir infraestructuras públicas digitales que sirvan eficazmente al interés público y fortalezcan la ciudadanía democrática.

Referencias bibliográficas

AL-HUJRAN, Omar et al. *The imperative of influencing citizen attitude toward e-government adoption and use*. **Computers in Human Behavior**, [S. l.], v. 53, p. 189–203, 2015. Disponible en: <https://doi.org/10.1016/j.chb.2015.06.015>. Consultado el 20 de septiembre de 2025.

ANATEL, Idec. **Pesquisa de conectividade significativa**. Superintendência de Relações com Consumidores, 2025. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD-26Q9Xx5QNDbqZUQ5y5j6h2yvy7aYmCm-1Mu-qUgXUpnTgbbGy-Xr2hDZz2dxAx3Axq-vxAyuwr6onoLCKa82vajrfdkOdWk5CwV. Consultado el: 3 de octubre de 2025.

Bioni et al. **Entre a visibilidade e a exclusão**: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma Gov.br. São Paulo, 2022. Disponible en: <https://www.dataprivacybr.org/documentos/policy-paper-entre-a-visibilidade-e-a-exclusao-um-mapeamento-dos-riscos-da-identificacao-civil-nacional/?idProject=320>. Consultado el: 24 de septiembre de 2025.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponible en: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Consultado el: 19 de septiembre de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital (SGD/MGI). **Portaria SGD/MGI n. 5.950, de 26 de outubro de 2023**. Estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal. Brasília, DF: Diário Oficial da União, 2023. Disponible en: <https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/vigentes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023#:~:text=Estabelece%20modelo%20de%20contrata%C3%A7%C3%A3o%20de,SISF%20do%20Poder%20Executivo%20Federal>. Consultado el: 17 de junio de 2025.

_____. **Decreto nº 8.936, de 14 de december de 2016**. Institui a Plataforma de Cidadania Digital e dispõe sobre a simplificação do atendimento aos usuários dos serviços públicos. Brasília, DF: Presidência da República, 2016. Disponible en: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8936.htm. Consultado el: 19 de junio de 2025

_____. **Decreto nº 9.745, de 8 de abril de 2019**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Economia, remaneja cargos em comissão e funções de confiança, transforma Funções Comissionadas do Poder Executivo - FCPE e extingue cargos em comissão. Brasília, DF: Presidência da República, 2019. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9745.htm. Consultado el: 19 de junio de 2025

_____. **Decreto nº 9.756, de 11 de abril de 2019**. Altera o Decreto nº 9.203, de 22 de novembro de 2017, para dispor sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF: Presidência da República, 2019. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9756.htm. Consultado el: 19 de junio de 2025

_____. **Decreto nº 1.048, de 21 de janeiro de 1994.** Dispõe sobre o Sistema de Administração de Recursos de Informação e Informática (SISP) da Administração Pública Federal e dá outras providências. Diário Oficial da União, Brasília, DF, 24 jan. 1994, p. 950. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D1048.htm. Consultado em: 19 de junho de 2025

_____. **Lei nº 13.303, de 30 de junho de 2016.** Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias [...]. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm. Consultado em: 17 de junho de 2025.

_____. **Lei nº 9.454, de 7 de abril de 1997.** Institui o número único de Registro de Identidade Civil. Brasília, DF: Presidência da República, 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9454.htm. Consultado em: 19 de junho de 2025.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Consultado em:

_____. Ministério da Gestão e da Inovação em Serviços Públicos. **Estratégia de Governança Digital. Do eletrônico ao digital.** Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2024. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>. Consultado em: 19 de junho de 2025.

_____. Presidência da República. **“Um marco neste país”, diz Lula ao receber proposta de Plano Brasileiro de Inteligência Artificial.** Brasília, DF: Portal Planalto, 30 jul. 2024. Disponível em: <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2024/07/201cum-marco-neste-pais201d-diz-lula-ao-receber-proposta-de-plano-brasileiro-de-inteligencia-artificial>. Consultado em: 19 de junho de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. **Atendimento Presencial Balcão GOV.BR.** Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/identidade/identidade-digital-para-gestores-publicos/programa-balcao-gov.br>. Consultado em: 19 de junho de 2025.

_____. Ministério da Economia. Serviço Federal de Processamento de Dados. **Extrato de Contrato de Parceria nº 76.043/2020 - UASG 806030.** Diário Oficial da União, Brasília, DF, 23 mar. 2020, Seção 3. Disponível em: <https://www.in.gov.br/en/web/dou/-/extrato-de-contrato-de-parceria-n-76.043/2020-uasg-806030-249306681>. Consultado em: 17 de junho de 2025.

_____. Ministério das Comunicações. **Portaria Interministerial nº 14, de 16 de janeiro de 1995.** Dispõe sobre o Sistema de Administração de Recursos de Informação e Informática (SISP) da Administração Pública Federal e dá outras providências. Diário Oficial da União, Brasília, DF, 17 jan. 1995, Seção 1, p. 770. Disponível em: <https://www.in.gov.br/en/web/dou/-/PORTARIA-INTERMINISTERIAL-N-14-DE-16-DE-JANEIRO-DE-1995-36453952>. Consultado em: 19 de junho de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. **Segurança e Proteção de Dados.** Brasília, DF. Disponível em: <https://www.gov.br/governodigital/pt-br/conta-gov-br/seguranca>. Consultado em: 19 de junho de 2025

_____. Ministério da Ciência, Tecnologia e Inovação. **Portaria Interministerial nº 92, de 24 de dezembro de 2014.** Dispõe sobre o Sistema de Administração de Recursos de Tecnologia da Informação (SISP). Diário Oficial da União, Brasília, DF, 26 dez. 2014, Seção 1, p. 120. Disponível em: <https://www.in.gov.br/web/dou/-/PORTARIA-INTERMINISTERIAL-N-92-DE-24-DE-DECEMBER-DE-2014-16292398>. Consultado em: 19 de junho de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. **Governo exclui estatais do Programa de Desestatização, entre elas a BRASIL Dataprev.** Brasília, DF, 7 abr. 2023. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/abril/governo-exclui-estatais-do-programa-de-desestatizacao-entre-elas-a-dataprev>. Consultado el: 19 de junio de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. **Rede GOV.BR alcança 1.800 municípios e fortalece a transformação digital em todos os níveis de governo.** Brasília, DF, 09 abril 2025. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/maio/rede-gov-br-alcanca-1-800-municipios-e-fortalece-a-transformacao-digital-em-todos-os-niveis-de-governo>. Consultado el: 19 de junio de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. Infraestrutura Nacional de Dados: ambiente tecnológico. **Nuvem de Governo.** Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ambiente-tecnologico/nuvem/nuvem-de-governo>. Consultado el: 19 de septiembre de 2025.

_____. Gabinete de Segurança Institucional. Centro de Tratamento e Resposta a Incidentes de Cibersegurança de Governo. **Apresentação.** Brasília, DF: CTIR Gov, 2025. Disponível em: <https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/apresentacao>. Consultado el: 19 de septiembre de 2025.

_____. Secretaria de Comunicação Social. **Polícia Federal investiga fraudes em contas vinculadas à plataforma gov.br.** Brasília, DF: Secretaria de Comunicação Social, maio 2025. Disponível em: <https://www.gov.br/secom/pt-br/assuntos/noticias/2025/05/policia-federal-investiga-fraudes-em-contas-vinculadas-a-plataforma-gov.br>. Consultado el: 19 de septiembre de 2025.

_____. **Lei nº 10.741, de 1º de outubro de 2003.** Dispõe sobre o Estatuto do Idoso e dá outras providências. Brasília, DF: Presidência da República, 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/10/10.741.htm. Consultado el: 19 de septiembre de 2025.

_____. **Lei nº 12.527, de 18 de novembro de 2011.** Lei de acesso à informação. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Consultado el: 03 de octubre de 2025.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Marco Civil da Internet. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Consultado el: 03 de octubre de 2025.

_____. **Lei nº 13.444, de 2017.** Lei que dispõe sobre a Identificação Civil Nacional (ICN). Brasília, DF: Portal Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/113444.htm. Consultado el: 03 de octubre de 2025.

_____. **Lei nº 13.726, de 8 de outubro de 2018.** Institui o Selo de Desburocratização e Simplificação. Brasília, DF: Portal Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113726.htm. Consultado el: 03 de octubre de 2025.

_____. **Lei nº 14.129, de 29 de março de 2021.** Lei que dispõe sobre princípios, regras e instrumentos no Governo Digital. Brasília, DF: Portal Planalto. Disponível: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114129.htm. Consultado el: 03 de octubre de 2025.

_____. **Lei nº 14.063, de 23 de setembro de 2020.** Lei que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos. Brasília, DF: Portal Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114063.htm. Consultado el: 03 de octubre de 2025.

_____. Ministério de Minas e Energia. **Quem é Quem - MGI**. Brasília, DF: Ministério de Minas e Energia, 2025. Disponível em: <https://www.gov.br/mme/pt-br/assuntos/secretarias/sntep/quem-e-quem/setor-publico-1/mgi>. Consultado el: 19 de septiembre de 2025.

_____. Ministério da Gestão e da Inovação em Serviços Públicos. **Assinatura GOV.BR ultrapassa 75 milhões de usos e registra alta de 92 % em 2025**. Brasília, 28 maio 2025. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/maio/assinatura-gov-br-ultrapassa-75-milhoes-de-usos-e-registra-alta-de-92-em-2025>

_____. Estratégia Nacional de Governo Digital para o período de 2024 a 2027. **Portaria SGD/MGI nº 4.248, de 26 de junho de 2024**. Brasília, DF: Portal Planalto. Disponível em: https://asespropr.org.br/wp-content/uploads/2024/07/PORTARIA-SGD_MGI-No-4.248-DE-26-DE-JUNHO-DE-2024.pdf. Consultado el: 03 de octubre de 2025.

_____. Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital - Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027. **Decreto nº 12.069, de 21 de junho de 2024**. Brasília, DF: Portal Planalto. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2024/decreto-12069-21-junho-2024-795831-publicacaooriginal-172182-pe.html>. Consultado el: 03 de octubre de 2025.

_____. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências. **Decreto de 18, de outubro de 2000**. Brasília, DF: Portal Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/dnn/dnn9067.htm. Consultado el: 03 de octubre de 2025.

_____. Dispõe sobre diretrizes, competências e condições para adesão à Rede Nacional de Governo Digital. **Portaria nº 23, de 4 de abril de 2019**. Brasília, DF: Portal Planalto. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_SGD_ME_n_23_de_04042019.html. Consultado el: 03 de octubre de 2025.

CAMELO, Ana Paula et al. **Soberania digital: para quê e para quem? Análise conceitual e política do conceito a partir do contexto brasileiro**. São Paulo: CEPI FGV DIREITO SP; ISOC Brasil, 2024.

CASSINO, João Francisco. **Soberania fatiada: controle das infraestruturas e subordinação da autoridade pública no mundo digital**. 2025. Dissertação (Mestrado em Ciências Humanas e Sociais) – Universidade Federal do ABC, São Bernardo do Campo, 2025.

CERT.BR. **Página inicial**. São Paulo: NIC.br, 2025. Disponível em: <https://www.cert.br/>. Consultado el: 19 de septiembre de 2025.

DEL GIOVANE, Chiara; FERENCZ, Janos; LÓPEZ GONZÁLEZ, Javier. The Nature, Evolution and Potential Implications of Data Localisation Measures. Paris: OECD Publishing, 2023. **OECD Trade Policy Papers**, n. 278. DOI: 10.1787/179f718a-en. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf. Consultado el: 20 de septiembre de 2025.

DIAS, Daniella S. Governança da internet: um novo modelo de gestão para o ciberespaço? **Revista de Informação Legislativa**, Brasília, a. 48, n. 192, p. 19-35, out./dez. 2011. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/242929/000936209.pdf?sequence=3&isAllowed=y>. Consultado el: 19 de septiembre de 2025. p. 58.

DIGITAL Watch Observatory. **Digital Public Infrastructure: An innovative outcome of India's G20 leadership**. [S. l.], 4 set. 2024. Disponível em: <https://dig.watch/updates/digital-public-infrastructure-an-innovative-outcome-of-indias-g20-leadership>. Consultado el: 20 de septiembre de 2025.

EAVES, D.; MAZZUCATO, M.; PAGLIARINI, G. **Leveraging digital public infrastructures for the common good to promote inclusive and sustainable economic development in Brazil**. UCL Institute for Innovation and Public Purpose, Working Paper Series, IIPP WP 2024-19, 2024. ISSN 2635-0122.

EUROSTACK. **A pitch**. [S. l.]: EuroStack, 10 jan. 2025. Disponible en: <https://euro-stack.eu/a-pitch-paper/>. Consultado el: 19 de junio de 2025.

EUROSTACK. **[Sem título]**. [S. l.], 14 mar. 2025. Disponible en: https://euro-stackletter.eu/wp-content/uploads/2025/03/EuroStack_Initiative_Letter_14-March-.pdf. Consultado el: April 09, 2025.

ESTADOS UNIDOS. Department of Justice. **CLOUD Act ReFuentes**. Washington, D.C.: Department of Justice, [2018]. Disponible en: <https://www.justice.gov/criminal/cloud-act-reFuentes>. Consultado el: 19 de septiembre de 2025.

ESTADOS UNIDOS. **Communications Assistance for Law Enforcement Act**. Pub. L. No. 103-414, de 25 de outubro de 1994. Codificada em 47 U.S.C. §§ 1001-1010 Disponible en: <https://www.fcc.gov/calea>. Consultado el: 19 de septiembre de 2025.

FALCÃO, L. C. et al. Uso de governo eletrônico e exclusão digital: perfil e desafios no contexto da terceira idade. In: SEMINÁRIOS EM ADMINISTRAÇÃO – SEMEAD, 26., 2023, São Paulo. **Anais eletrônicos...** São Paulo: SEMEAD, 2023. Disponible en: <https://login.semead.com.br/26semead/anais/arquivos/147.pdf>. Consultado el: 17 de junio de 2025.

FARIA, Carlos Aurélio Pimenta de; LIMA, Luciana Leite (org.). **As políticas públicas do governo Bolsonaro: desmonte, resiliência e refundação**. Porto Alegre: Jacarta Produções, 2024.

FILGUEIRAS, Fernando; LUI, Lizandro. Designing data governance in Brazil: an institutional analysis. **Policy Design and Practice**, v. 6, n. 1, p. 41-56, 2023. DOI: <https://doi.org/10.1080/25741292.2022.2065065>.

FIORI, José Luís. **O poder global e a nova geopolítica das nações**. São Paulo: Boitempo, 2007.

G1. **Desenrola Brasil: governo permite parcelamento para pessoas com conta bronze do gov.br**. 29 jan. 2024. Disponible en: <https://g1.globo.com/economia/noticia/2024/01/29/desenrola-brasil-governo-permite-parcelamento-para-pessoas-com-conta-bronze-do-gov-br.ghtml>. Consultado el: 24 de septiembre de 2025.

_____. **Justiça condena iFood a indenizar entregador do DF por danos morais após falha racista em reconhecimento facial**; entenda. Brasília, 30 jun. 2025. Disponible en: <https://g1.globo.com/df/distrito-federal/noticia/2025/06/30/justica-condena-ifood-a-indenizar-entregador-do-df-por-danos-morais-apos-falha-racista-em-reconhecimento-facial-entenda.ghtml>. Consultado el: 24 de septiembre de 2025.

_____. **Polícia investiga organização criminosa que aplica golpes por aplicativo do governo federal**. Fantástico, 22 dez. 2024. Disponible en: <https://g1.globo.com/fantastico/noticia/2024/12/22/policia-investiga-organizacao-criminosa-que-aplica-golpes-por-aplicativo-do-governo-federal.ghtml>

_____. **Pacientes renais não conseguem marcar consultas por aplicativo em Roraima e temem perder TFD**. Boa Vista, 11 jan. 2025. Disponible en: <https://g1.globo.com/rr/roraima/noticia/2025/01/11/pacientes-renais-nao-conseguem-marcar-consultas-por-aplicativo-em-roraima-e-temem-perder-tfd.ghtml>. Consultado el: 24 de septiembre de 2025.

GORGEN, James. **Soberania Digital: Esboço para um projeto para o Brasil. Outras palavras**. 03 de outubro de 2025. Disponible en: <https://outraspalavras.net/tecnologiaemdisputa/soberania-digital-esboco-para-um-projeto-para-o-brasil/> . Consultado el: 20 de septiembre de 2025.

GUEDES, R. D. **Digital public infrastructures & digital public goods for combating climate change: the Brazil case study**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2024/11/20241104-Relatorio-IPD-BPD-1.pdf>. Consultado el: 20 de septiembre de 2025.

GLOBERMAN, S. Canadian science policy and technological sovereignty. **Canadian Public Policy/Analyse De Politiques**, v. 4, n. 1, p. 34-45, 1978.

GOVERNMENT OF INDIA, Ministry of External Affairs. **G20 New Delhi Leaders' Declaration**. Nova Delhi, 9-10 set. 2023. Disponível em: <https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf>. Consultado el: 20 de septiembre de 2025.

IDEC; INSTITUTO LOCOMOTIVA. **Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E**. [S. l.]: IDEC; Instituto Locomotiva, 2021. Disponível em: https://idec.org.br/arquivos/pesquisas-acesso-internet/idec_pesquisa_internet-mo-vel-pelas-classes-cde.pdf. Consultado el: 17 de junio de 2025.

KREMER, Bianca. **Racismo algorítmico** [livro eletrônico] / Bianca Kremer, Pablo Nunes, Thallita G. L. Lima. – Rio de Janeiro: CESeC, 2023.

KOSINSKI, Matthew. **Soberania de dados e residência de dados: Qual a diferença?** [S. l.]: IBM, 17 jan. 2025. Disponível em: <https://www.ibm.com/br-pt/think/topics/data-sovereignty-vs-data-residency>. Consultado el: 17 de junio de 2025.

LABLIVRE – LABORATÓRIO DE TECNOLOGIAS LIVRES. **Guia rápido sobre soberania digital e soberania de dados para gestores públicos municipais do Brasil**. Universidade Federal do ABC, 2024. Disponível em: <https://lablivre.pesquisa.ufabc.edu.br/wp-content/uploads/2024/10/GUIASOBERANIA-DIGITAL-PARA-GESTORES-MUNICIPAIS.pdf>. Consultado el: 17 de junio de 2025.

MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital Public Infrastructure and Public Value: **What is 'public' about DPI?** London: UCL Institute for Innovation and Public Purpose, 2024. Working Paper Series (IIPP WP 2024-05). Disponível em: <https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi>. Consultado el: 20 de septiembre de 2025.

MIELLI, Renata; NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Conectividade significativa: propostas para medição e o retrato da população no Brasil**. São Paulo: NIC.br, 2024. Disponível em: <https://cetic.br/media/docs/publicacoes/7/20240415183307/estudos-setoriais-conectividade-significativa.pdf>. Consultado el: 17 de junio de 2025.

MINISTÉRIO PÚBLICO FEDERAL. **Nota Técnica nº 2/2021/GTTIC/3ªCCR**. Análise sobre eventual privatização do Serviço Federal de Processamento de Dados – SERPRO, incluído no Programa Nacional de Desestatização – PND por meio do Decreto nº 10.206, de 22 de janeiro de 2020. Brasília, 19 jan. 2021. Disponível em: <https://static.poder360.com.br/2021/02/NotaTecnicaMPSerpro-25.fev.2021.pdf>. Consultado el: 20 de septiembre de 2025.

MINISTÉRIO DA FAZENDA. **Negociar dívidas da Faixa I com o programa Desenrola Brasil**. Brasília, 19 ago. 2025. Disponível em: <https://www.gov.br/pt-br/servicos/negociar-dividas-da-faixa-i-com-o-programa-desenrola-brasil>. Consultado el: 24 de septiembre de 2025.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). **Usuários do GOV. BR com conta Ouro serão orientados a utilizar a Verificação em Duas Etapas**. Brasília, 25 jul. 2025. Disponível em: <https://www.gov.br/governodigital/pt-br/noticias/usuarios-do-gov-br-com-conta-ouro-serao-orientados-a-utilizar-a-verificacao-em-duas-etapas>. Consultado el: 24 de septiembre de 2025.

_____. **Dúvidas sobre as bases biométricas faciais.** Brasília, [s.d.]. Disponible en: <https://www.gov.br/governodigital/pt-br/acesibilidad-e-usuario/atendimento-gov.br/duvidas-no-aplicativo-gov.br/duvidas-no-reconhecimento-facial/bases-biometricas-faciais>. Consultado el: 24 de septiembre de 2025.

_____. **Iniciativas do MGI fortalecem a soberania digital, ampliam o acesso a serviços públicos e modernizam o Estado brasileiro.** Brasília, 22 jul. 2025. Disponible en: <https://www.gov.br/governodigital/pt-br/noticias/iniciativas-do-mgi-fortalecem-a-soberania-digital-ampliam-o-acesso-a-servicos-publicos-e-modernizam-o-estado-brasileiro>. Consultado el: 24 de septiembre de 2025.

NOGUEIRA JÚNIOR, D. A.; VALLE, V. C. L. L.; BENELLI, A. C. Direitos dos usuários de serviços públicos no ambiente do governo eletrônico e da administração pública digital. **Revista de Direito Administrativo**, v. 283, n. 1, p. 93–130, 2024. Disponible en: <https://doi.org/10.12660/rda.v283.2024.90691>. Consultado el: 17 de junio de 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). **Conectividade significativa** [livro eletrônico]: propostas para medição e o retrato da população no Brasil. Tradução Ana Zuleika Pinheiro Machado. São Paulo: NIC.br, 2024. Disponible en: https://cetic.br/media/docs/publicacoes/7/20240415183307/estudos_setoriais-conectividade_significativa.pdf. Consultado el: 19 de junio de 2025.

_____. **TIC Domicílios: Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – 2023.** São Paulo: NIC.br, 2024. Disponible en: https://cetic.br/media/docs/publicacoes/2/20241104102822/tic_domicilios_2023_livro_eletronico.pdf. Consultado el: 17 de junio de 2025.

O GLOBO. **Desenrola: preocupação do governo é que 57% das pessoas elegíveis ao programa não têm acesso à plataforma.** 09 out. 2023. Disponible en: <https://oglobo.globo.com/economia/noticia/2023/10/09/desenrola-preocupacao-do-governo-e-57percent-das-pessoas-elegiveis-ao-programa-nao-tem-acesso-a-plataforma.ghtml>. Consultado el: 24 de septiembre de 2025.

OLIVEIRA, Raul José de Galaad. O preceito da soberania nas constituições e na jurisprudência brasileira. **Revista de Informação Legislativa**, Brasília, v. 37, n. 146, p. 153–173, abr./jun. 2000. Disponible en: <https://www2.senado.leg.br/bdsf/item/id/587>. Consultado el: 20 de septiembre de 2025.

ONU. Network on Migration. **Termo de taxonomia 742.** [S. l.], [S.d.]. Disponible en: <https://migrationnetwork.un.org/taxonomy/term/742>. Consultado el: 20 de septiembre de 2025.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **The nature, evolution and potential implications of data localisation measures.** Paris: OECD Publishing, 2023. 116 p. Disponible en: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf. Consultado el: 19 de septiembre de 2025.

PHANG, Chee Wei *et al.* Senior citizens' acceptance of information systems: a study in the context of e-government services. **IEEE Transactions on Engineering Management**, [S. l.], v. 53, n. 4, p. 555–569, nov. 2006. Disponible en: <https://doi.org/10.1109/TEM.2006.883710>. Consultado el: 20 de septiembre de 2025.

QUEIROZ, Luiz. MPF questiona venda do Serpro sob a ótica da LGPD e da segurança nacional. **Capital Digital**, 25 abr. 2025. Disponible en: <https://capitaldigital.com.br/mpf-questiona-venda-do-serpro-sob-a-otica-da-lgpd-e-a-da-seguranca-nacional/>. Consultado el: 20 de septiembre de 2025.

SCHIAVI, Iara; SILVEIRA, Sérgio Amadeu da. A cidade neoliberal e a soberania de dados: mapeamento do cenário dos dispositivos de dataficação em São Paulo. **urbe. Revista Brasileira de Gestão Urbana**, v. 14, e20210145, 2022.

SEIFERT, Alexander. The digital exclusion of older adults during the COVID-19 pandemic. **Journal of Gerontological Social Work**, [S. l.], v. 63, n. 6–7, p. 674–676, 2020. DOI: <https://doi.org/10.1080/01634372.2020.1764687>. Disponível em: <https://doi.org/10.1080/01634372.2020.1764687>. Consultado el: 20 de septiembre de 2025.

SERPRO. **Serpro celebra 45 anos com homenagem aos empregados**. Brasília, 1 dez. 2009. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-antigas/serpro-celebra-45-anos-com-homenagem-aos-empregados>

_____. **Seis décadas de muita inovação e muitas realizações**. Serpro, 2024. Disponível em: <https://www.serpro.gov.br/menu/noticias/Tema-edicao-239/seis-decadas-de-muita-inovacao-e-muitas-realizacoes>. Consultado el: 19 de junio de 2025.

SILVA, Tarcizio da, 2022. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. [livro eletrônico]. São Paulo: Edições Sesc SP.

SILVEIRA, Sergio Amadeu da; XIONG, Jeff. Índice de Soberania Digital: o caso do Brasil. **Liinc em Revista**, Rio de Janeiro, v. 21, n. 1, p. 1–15, jan./jun. 2025. DOI: 10.18617/liinc.v21i1.7451. Disponível em: <https://revista.ibict.br/liinc/article/view/7451>. Consultado el: 20 de septiembre de 2025.

TEIXEIRA, Pedro. Governo Lula já gastou R\$ 1,2 bi para repatriar dados de brasileiros e construir nuvem soberana. **Folha de S.Paulo**, São Paulo, 10 jun. 2025. Disponível em: <https://www1.folha.uol.com.br/tec/2025/06/governo-lula-ja-gastou-r-12-bi-para-repatriar-dados-de-brasileiros-e-construir-nuvem-soberana.shtml>. Consultado el: 17 de junio de 2025.

UNITED NATIONS DEVELOPMENT PROGRAMME (UNDP). **Accelerating the SDGs Through Digital Public Infrastructure**: A Compendium of the Potential of Digital Public Infrastructure. Nova Iorque, 21 ago. 2023. Disponível em: <https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure>. Consultado el: 20 de septiembre de 2025.

UOL. **PF suspeita que 3.000 contas do Gov.br tenham sido fraudadas com biometria**. UOL Notícias, 13 maio 2025. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2025/05/13/pf-suspeita-de-fraudes-de-reconhecimento-facial-em-3-mil-contas-do-govbr.htm>

ZANATTA, Rafael Augusto Ferreira. **A proteção coletiva dos dados pessoais no Brasil: a defesa de direitos entre autoritarismo e democracia**. Tese (Doutorado) — Instituto de Energia e Ambiente, Universidade de São Paulo, São Paulo, 2023.

ZUCKERMAN, Ethan. **What Is Digital Public Infrastructure?** [S. l.]: Center for Journalism & Liberty, nov. 2020. Disponível em: <https://static1.squarespace.com/static/5efcb64b1cf16e4c487b2f61/t/5fb41b6aac578321b0c50717/1605639019414/zuckerman-digital-infrastructure-cjl-nov2020.pdf>. Consultado el: 20 de septiembre de 2025.

Nuestras principales recomendaciones ➔

A continuación, presentamos las recomendaciones de Idec para mejorar las IPD brasileñas (Gov.br y Pix), organizadas según los ejes temáticos de Inclusión digital; Seguridad; Soberanía y Gobernanza.

RECOMENDACIONES DE INCLUSIÓN DIGITAL:



SUPUESTO 🔍

Aunque existe legislación que prohíbe a los comercios rechazar efectivo (incluso el Banco Central y Procon ya han advertido sobre esta práctica abusiva), con el uso generalizado del Pix en los últimos años, es necesario asegurar que los usuarios tengan una variedad de métodos de pago a su disposición.

RECOMENDACIÓN 💡

Se recomienda fortalecer las regulaciones y prácticas **que incentiven a los establecimientos comerciales a aceptar, sin distinción, diferentes formas de pago, asegurando la plena inclusión y accesibilidad para todos los usuarios.** Pix es una alternativa relevante, pero no puede usarse para rechazar otros métodos de pago, especialmente efectivo.



SUPUESTO 🔍

A los usuarios que carecen de acceso a internet o dispositivos digitales se les impide usar las IPD. Más de 20 millones de brasileños aún carecen de acceso a internet, según datos del IBGE (2025). Existen desafíos importantes relacionados con la conectividad para la población brasileña que no deben impedir el avance en la inclusión financiera.

RECOMENDACIÓN 💡

Para ampliar y facilitar el acceso a los usuarios que experimentan dificultades de conexión, **recomendamos priorizar Pix Offline en la agenda evolutiva del Pix**, como una medida esencial para garantizar la accesibilidad digital completa.



SUPUESTO

Los usuarios todavía enfrentan barreras para acceder a Gov.br, ya sea por falta de equipos compatibles con biometría, por el posible no reconocimiento de rostros racializados y de personas trans, por limitaciones de conectividad o por baja competencia digital. El mostrador de Gov.br existe en 66 ciudades (según los propios datos del sitio web a septiembre de 2025), pero los planes de expansión aún no están claros.

- ➔ **Publicación periódica de informes de transparencia con el plan de expansión del Balcão Gov.br**, incluyendo información sobre los órganos que no formen parte de la red tradicional de atención presencial al ciudadano vinculada a órganos o entidades públicas.
- ➔ Definir un protocolo de seguridad para la atención presencial.

El **Balcão Gov.br** es una iniciativa de atención presencial diseñada para brindar soporte a los usuarios de Gov.br. Está dirigida a los ciudadanos que enfrentan desafíos tecnológicos, ofreciendo un enfoque de asistencia más centrado en las personas.

SUPUESTO

El acceso a los servicios públicos digitales debe garantizarse incluso en contextos de **conectividad limitada o inexistente**.



RECOMENDACIÓN

Para garantizar el acceso completo de la población a los servicios públicos digitales ofrecidos en línea por la plataforma Gov.br, es esencial que el Estado habilite el **acceso offline a estos servicios**.



Hoy en día, acceder a los servicios digitales requiere cada vez más verificar y autenticar su identidad digital. En este contexto, es necesario que los usuarios conozcan formas de proteger esta identidad y que existan mecanismos educativos que sean didácticos respecto al tema.

RECOMENDACIÓN

Promover campañas educativas, con guías prácticas, para sensibilizar al público objetivo y facilitar su comprensión del uso de los servicios gubernamentales en línea, incluyendo orientación para acceder a ellos únicamente a través de los medios previamente declarados, como forma de garantizar una mayor seguridad para la población.

RECOMENDACIONES SEGURIDAD Y PROTECCIÓN DE DATOS:



Directrices para el monitoreo de los Manuales Pix

SUPUESTO

Los casos de fraude son **tratados de manera desigual**, dependiendo de las acciones de las instituciones Pix. A pesar de la existencia del Manual de Seguridad del Pix, no hay evidencia de mecanismos de supervisión implementados por el Banco Central, ni de su implementación efectiva por las instituciones financieras.

RECOMENDACIÓN

Supervisar la adopción de **directrices de comunicación entre las instituciones y los consumidores** en casos de fraudes en el Pix (a través de Autoatención de MED y MED 2.0).

Mejora en la prevención y represión de fraudes en Gov.br

SUPUESTO

La confianza de la población en las plataformas digitales del gobierno depende de la **percepción de seguridad** y de la **capacidad de respuesta ante incidentes**. No existe un **canal de soporte o resolución de fraude dedicado para los usuarios de Gov.br**, ni un canal de transparencia que informe el volumen de fraude.

RECOMENDACIÓN

1. Campañas de prevención: El gobierno debe realizar campañas sistemáticas contra el fraude en Gov.br y emitir advertencias para prevenir prácticas riesgosas.

2. Detección de movimientos atípicos: Detección de movimientos atípicos: Priorizar el desarrollo de herramientas para mapear movimientos atípicos/biometría de comportamiento que identifiquen patrones de comportamiento sospechosos, alertando a los usuarios sobre riesgos potenciales y fortaleciendo así la seguridad del acceso a Gov.br. **Estas tecnologías deben implementarse con salvaguardas de privacidad de los ciudadanos y deben generar inteligencia para la elaboración de informes que permitan identificar patrones comunes de estafas y fraudes.**

3. Apoyo: Crear un canal exclusivo para que los usuarios resuelvan problemas relacionados con estafas y fraudes.

4. Represión: mejora de los mecanismos de fiscalización y represión del fraude en el Gov.br.

Mejoras en la operación Pix: Pix incorrecto

SUPUESTO

En caso de un **Pix incorrecto**, no existe una vía institucional para que el consumidor recupere el dinero.

RECOMENDACIÓN

- ➔ Diseñar un **proceso que las instituciones adopten como estándar para resolver los errores de los usuarios** al realizar un Pix.
- ➔ Proporcionar orientación a las instituciones sobre qué datos se pueden proporcionar para identificar al destinatario.

Mejoras al MED (Mecanismo Especial de Reembolso)

SUPUESTO

La **seguridad debe garantizarse desde el diseño de la tecnología del Pix**, con requisitos estandarizados de resolución de problemas para facilitar la comprensión del usuario. Actualmente, no existe un estándar que garantice el reembolso completo en casos de estafa, incluso cuando se utiliza el MED (Mecanismo Especial de Reembolso), lo que debilita la protección del consumidor.

RECOMENDACIONES

- ➔ Garantizar la **ampliación de los reembolsos de MED 2.0 a todos los importes**, ya que el mínimo actual es de R\$200, pero el 75% de las transacciones Pix son inferiores a este importe.
- ➔ Crear un Comité de Seguimiento de MED 2.0.
- ➔ Monitoreo de transacciones de MED (Instrumentos Médicos) con montos inferiores a R\$200 (reales brasileños) para generar evidencia que respalde la reducción de este límite al aplicar MED 2.0.
- ➔ Si se confirma una estafa, se debe garantizar la restitución íntegra de las cantidades a las víctimas, de acuerdo con el modelo de reembolso adoptado en el Reino Unido, donde se reembolsan en un plazo de cinco días hábiles. En este modelo, el reembolso se divide entre las instituciones involucradas en el fraude: el 50 % corre a cargo de la institución financiera receptora y el otro 50 % a cargo de la institución pagadora.
- ➔ Se debe evaluar la posibilidad de ajustar la nomenclatura de MED-Fraude para que la funcionalidad sea más fácil de entender para los consumidores.

Es un mecanismo del Pix creado para recibir y registrar casos de fraude, así como fallas operativas. Una vez que se genera un ticket en el sistema MED, las instituciones financieras involucradas comienzan a implementar los procedimientos adecuados destinados a reembolsar a los reclamantes.

Datos recientes muestran que el número de solicitudes de reembolso a través del MED casi se duplicó en 2024 en comparación con 2023, pasando de aproximadamente 2,5 millones a cerca de 4,95 millones de solicitudes. Sin embargo, solo alrededor del 9 % de ellas fueron aceptadas, total o parcialmente, principalmente porque la versión actual del mecanismo solo puede rastrear y bloquear fondos que permanecen en la primera cuenta receptora. En la mayoría de los casos, el dinero robado ya ha sido transferido o retirado, dejando sin saldo disponible para su recuperación. Entre enero y julio de 2024, el Banco Central reembolsó aproximadamente 63 millones de dólares por casos de fraude y cerca de 6,6 millones de dólares por fallas operativas.



Autenticación de Gov.br

SUPUESTO

Los mecanismos de autenticación deben ser seguros, accesibles y **respetuosos con la diversidad de identidades** y circunstancias de la población.

RECOMENDACIÓN

- 1. Alternativas al reconocimiento facial:** Garantizar el acceso inicial, la validación y mecanismos de mayor seguridad que no impliquen reconocimiento facial, ofreciendo alternativas a los ciudadanos.
- 2.** Fomentar y desarrollar campañas para aumentar la autenticación de dos factores al usar Gov.br, promoviendo una mayor seguridad para los usuarios.
- 3.** Crear una estructura de gobernanza central para revisar y aprobar el nivel de autenticación requerido por cada servicio, en función del riesgo y la sensibilidad de los datos o transacciones involucradas, evitando excesos y asegurando la consistencia.

SUPUESTO

Existe una falta de **transparencia** con respecto a las instituciones con **altas tasas de fraude**, lo que dificulta la acción preventiva y la toma de decisiones informada por parte de los usuarios. Nombrar y divulgar estas instituciones puede generar incentivos para mejorar la tasa de resolución. Información que ayudaría a los consumidores a elegir qué institución contratar para usar el Pix.

RECOMENDACIÓN

Establecer un Ranking de Instituciones Financieras con Altos Índices de Cuentas Fraudulentas. El Registro debe incluir índices como los establecidos en MED 2.0:

- a. Índice de fraude confirmada** por transacciones;
- b. Índice de sospecha de fraude**, considerando la relación entre notificaciones de infracción analizadas y el volumen de transacciones recibidas.
- c. Índice de rechazo** de notificaciones de infracción, lo que indica un uso ineficaz de MED por parte de la institución receptora;
- d. Participación en fraudes**, medida por la proporción de notificaciones de infracción aceptadas por el participante en relación con el número total de notificaciones aceptadas en Pix;
- e. Índice de bloqueo indebido**, que refleja las cantidades bloqueadas en las notificaciones rechazadas en relación con el total analizado;
- f. Otros indicadores relevantes** que puedan ser definidos por acto del Banco Central de Brasil, con base en evidencias técnicas y científicas



Ranking de Instituciones Financieras con Altos Índices de Cuentas Fraudulentas



Coartar el uso abusivo del Pix como estrategia de marketing

SUPUESTO 🔍

Se debe priorizar la privacidad de la población y el Pix no debe ser utilizado como una herramienta de marketing por las empresas

RECOMENDACIÓN 💡

Prevenir el uso abusivo de las comunicaciones del Pix por parte de los proveedores, como el uso del Pix para campañas de marketing, comunicaciones de estilo spam u ofertas personalizadas basadas en el comportamiento de pago.



No compartir datos sensibles

SUPUESTO 🔍

Se deben respetar los principios de la Ley General de Protección de Datos (LGPD), especialmente los de finalidad, necesidad, transparencia y seguridad, garantizando que dicho intercambio tenga un interés público demostrado.

RECOMENDACIÓN 💡

Limitar el intercambio de datos personales, incluso sensibles, contenidos en bases de datos integradas al Gov.br, mediante acuerdos administrativos, asegurando la existencia de una base legal clara, con consentimiento específico e informado de los titulares, así como demostración concreta de un interés público legítimo. Cualquier excepción a esta regla debe estar precedida de amplia transparencia, consulta pública y supervisión regulatoria por parte de la ANPD.

RECOMENDACIONES DE SOBERANÍA Y GOBERNANZA:



SUPUESTO

El Foro Pix tiene una **baja presencia de organizaciones de la sociedad civil, incluidas las organizaciones de protección al consumidor** y derechos digitales. Esto limita la pluralidad de puntos de vista y puede comprometer decisiones más inclusivas y equilibradas.

RECOMENDACIÓN

- ➔ Se recomienda la **participación y el compromiso de más organizaciones de protección al consumidor**, así como de **derechos digitales**, para garantizar una pluralidad de actores de la sociedad civil, incluido un llamado activo para que estas entidades se unan al Foro Pix.
- ➔ Se recomienda que la agenda evolutiva del Pix sea sometida a consulta pública, asegurando la posibilidad de discusión sobre la priorización de las funcionalidades a desarrollar.

El Foro Pix fue diseñado para fomentar un espacio multisectorial centrado en el desarrollo y la mejora del sistema de pagos instantáneos. Según el Banco Central, se trata de un entorno de gobernanza destinado a apoyar a esta entidad en su rol respecto a las políticas operativas relacionadas con el ecosistema Pix.

Creación de un GT de Comunicaciones en el Foro Pix

RECOMENDACIÓN

Se recomienda la creación de un **Grupo de Trabajo de Comunicaciones y Difusión de la Agenda Pix** dentro del Foro Pix. Este grupo sería responsable de:

1. **Establecer directrices de comunicación y riesgo** a medida que surgen nuevas funciones.

SUPUESTO

La confianza de la población es un gran factor que puede promover o perjudicar el uso de las IPD. **Las noticias falsas** y la falta de comprensión de los impactos financieros de nuevas funcionalidades (como en el caso del Pix Parcelado) pueden afectar aún más este contexto.

2. **Desarrollar estrategias para combatir la desinformación** que pueda comprometer la confianza de la población en el uso del Pix.
3. **Especificar las oportunidades, los puntos de atención y los riesgos asociados a cada función** contribuyendo a la regulación del Banco Central.

SUPUESTO

Publicar documentos y ponerlos a disposición del público puede dar a las partes interesadas una mejor **comprensión de la toma de decisiones** y promover una mayor **transparencia** para la población

Realizar investigaciones para el perfeccionamiento de las evidencias

RECOMENDACIÓN

Además de los datos relevantes publicados periódicamente sobre las estadísticas de Pix, se recomienda la publicación regular de un Informe de Gestión del Pix para permitir el seguimiento de las inversiones realizadas, de los costos de mantenimiento de la estructura, así como de las acciones de combate a fraudes, entre otros aspectos.

Mejorar los mecanismos de participación social: publicidad y esfuerzos institucionales

SUPUESTO

Las directrices para **la participación de la sociedad civil** no son claras. Aunque la gobernanza se lleva a cabo a través del Foro Pix, no existe un equilibrio entre el sector privado, las organizaciones de la sociedad civil y otras agencias gubernamentales que podrían contribuir y ampliar el debate.

RECOMENDACIÓN

➔ Se recomienda que el Banco Central cree **mecanismos para incentivar el desarrollo de innovaciones en el sistema Pix**, no limitado a sus empleados o discusiones formales dentro del Foro Pix. Los ejemplos incluyen el apoyo a iniciativas de la sociedad civil como hackatones y laboratorios de innovación abierta, incluidos los destinados a combatir el fraude.

➔ **Directrices claras y públicas para una amplia participación** en el Foro Pix, con requisitos y obligaciones.

➔ **Publicación** de miembros, de grupos de trabajo, contribuciones y documentos estratégicos.

➔ **Modelo de secretaría** con coordinadores rotativos y/o mayor participación del Banco Central.



SUPUESTO 🔍

La construcción y gestión de infraestructuras públicas digitales debe implicar **transparencia** y **participación ciudadana**.

RECOMENDACIONES 💡

- ➔ **Directrices claras y públicas para una amplia participación**, con requisitos y obligaciones.
- ➔ Crear mecanismos de **gobernanza participativa** que incluyan a representantes de organizaciones de la sociedad civil y usuarios finales, garantizando que los puestos no sean ocupados por la Sociedad Civil Productiva (asociaciones empresariales), para asegurar que las decisiones sobre el sistema se basen en perspectivas diversas.
- ➔ Definir directrices de diversidad para las organizaciones participantes que puedan incluir representación de las cinco regiones del país.

**Para más
información sobre la
encuesta, acceda a:**



<https://idec.org.br/ipd>