DATOS PERSONALES Y SERVICIOS FINANCIEROS

¿QUIÉN CUSTODIA LOS DATOS CUANDO UN BANCO ENTRA EN CRISIS?



Tecnología & Derechos Humanos

TEDIC

DATOS PERSONALES Y SERVICIOS FINANCIEROS

¿QUIÉN CUSTODIA LOS DATOS CUANDO UN BANCO ENTRA EN CRISIS?

Tecnología & Derechos Humanos

Tecnología & Derechos Humanos

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

La presente publicación ha sido financiada por la Unión Europea. Su contenido es responsabilidad exclusiva de TEDIC y no refleja necesariamente los puntos de vista de la Unión Europea.

DATOS PERSONALES Y SERVICIOS FINANCIEROS

¿QUIÉN CUSTODIA LOS DATOS CUANDO UN BANCO ENTRA EN CRISIS?

NOVIEMBRE 2026

AUTORÍA
Antonia Bogado Rodas

COORDINACIÓN Y EDICIÓN
Maricarmen Sequera

ASISTENCIA DEL PROYECTO
Maricel Achucarro

COMUNICACIÓN
Camila Rolón

DIAGRAMACIÓN
Horacio Oteiza

Este documento está licenciado con CC BY-SA lo que significa:
Usted es libre de:

- **Compartir** — copiar y redistribuir el material en cualquier medio o formato
- **Adaptar** — remezclar, transformar y crear a partir del material para cualquier finalidad, incluso comercial.

Bajo las condiciones siguientes:

- **Reconocimiento** — Debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios<. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licenciador o lo recibe por el uso que hace.
- **CompartirIgual** — Si remezcla, transforma o crea a partir del material, deberá difundir sus contribuciones bajo la misma licencia que el original.

https://creativecommons.org/licenses/by-sa/4.0/deed.es

TABLA DE CONTENIDO

SOBRE LA AUTORA 7

EL OTRO PASIVO: LOS DATOS 8

RELACIÓN SIMBIÓTICA: SERVICIOS FINANCIEROS Y BASE DE DATOS 8

EL MAPA NORMATIVO ACTUAL EN PARAGUAY:
¿ESTÁN PROTEGIDOS NUESTROS DATOS PERSONALES? 10

DE LA NORMA A LA ACCIÓN: ¿QUIÉN CUSTODIA NUESTROS
DATOS PERSONALES CUANDO UN BANCO ENTRA EN CRISIS? 14

RECAPITULANDO 17

DIVULGACIÓN SOBRE EL USO DE HERRAMIENTAS ASISTIDAS POR IA 18

REFERENCIAS 19

SOBRE LA AUTORA

ANTONIA BOGADO RODAS

Abogada y doctoranda en la Universidad Complutense de Madrid, donde investiga el uso de la inteligencia artificial (IA) en los servicios financieros y su impacto en los derechos. Es magíster en Derecho por la London School of Economics and Political Science (LSE), con especialización en Derecho Bancario y Regulación Financiera, y magíster en Gobernanza de la IA por la Universidad Pontificia de Salamanca.

EL OTRO PASIVO: LOS DATOS

El 2 de noviembre de 2026, el Banco Central del Paraguay (BCP) dispuso iniciar el proceso de resolución de Ueno Bank, considerado el primer banco digital del país (BCP, 2026). La intervención se dio luego de constatar que el índice de solvencia de la entidad había caído por debajo del 50% del mínimo legal exigido (ABC Color, 2026). Los procedimientos de resolución interrumpieron el acceso a los servicios bancarios para casi tres millones de clientes y desencadenaron una crisis financiera y política más amplia, que incluyó la destitución del presidente y la apertura de investigaciones penales (Desantis y O'Boyle, 2026).

Si bien, la primera actuación del ente regulador fue iniciar la devolución de los depósitos conforme a la ley vigente, posteriormente, la atención también pasó a notar que este banco digital no deja solo cuestiones de activos y pasivos, sino también bases de datos de identificación, transaccionales y biométricas de sus clientes (Ruíz Díaz, 2026b). Ante esto, surge la pregunta: **¿quién custodia hoy esa información, bajo qué reglas y quién responde por ella?**

TEDIC ya documentó con detalle la arquitectura tecnológica de ese ecosistema, el uso extendido de la biometría y sus implicancias para los derechos de las personas (Sequera Buzarquiz, 2026). Este artículo examina qué debería prever el régimen de resolución bancaria para los datos personales de una entidad en crisis desde una perspectiva de derechos humanos. Sostengo que **la gobernanza de datos debe formar parte de la supervisión financiera y de la respuesta del ente regulador.** Para ello, hacen falta reglas explícitas que definan quién asume la custodia y qué datos se conservan, se transfieren o se eliminan.

RELACIÓN SIMBIÓTICA: SERVICIOS FINANCIEROS Y BASE DE DATOS

Los servicios financieros, entiéndase estos como la apertura y gestión de cuentas, el otorgamiento de créditos, los medios de pago digitales, las transferencias, las inversiones y los seguros, siempre se basaron en información para evaluar solvencia, gestionar riesgos y prevenir fraudes. Y con la creciente digitalización de estos servicios se amplió el volumen y la variedad de la información requerida. Hoy los proveedores recurren a "datos alternativos" o información no asociada tradicionalmente al sector financiero, que puede igualmente contribuir a evaluar las circunstancias financieras de las personas (Aggarwal, 2021; IFC, 2026). Algunos ejemplos son los pagos de servicios, historial de transacciones digitales y de pagos móviles, y en ciertos contextos, incluso geolocalización e indicadores de comportamiento.

De hecho, la política de privacidad de Ueno Bank (s.f.) contemplaba recoger datos como "georreferenciación, dirección IP, dirección MAC, sistema operativo, información del User Agent, rastro digital en redes sociales, buscadores y páginas web". Y este tipo de prácticas no es un rasgo exclusivo de las bancas digitales, otros bancos considerados más tradicionales también procesan distintas categorías de datos, así lo informan en sus respectivas políticas de privacidad disponibles en sus páginas web. Itaú (s.f), en su política de privacidad, menciona entre sus fuentes de información "Internet, medios de comunicación, redes sociales y registros públicos", y Sudameris (s.f.), por su parte, dice recolectar datos como "dirección IP, dispositivo, sistema operativo, navegador, *cookies* y registros de acceso a nuestros sistemas".

El uso extensivo de datos alternativos está, además, estrechamente relacionado con la infraestructura tecnológica que sustenta los servicios de la banca moderna. Pero esta digitalización del sector va mucho más allá de las transacciones por Internet (BCBS, 2026), las aplicaciones móviles, los *chatbots* y los asistentes virtuales, los tokens de autenticación, los servicios de computación en la nube y los sistemas automatizados de toma de decisiones han transformado la forma en que las entidades del sector financiero interactúan con sus clientes.

Estas tecnologías permiten la recopilación, integración, almacenamiento y análisis de información en las distintas etapas de la relación con el cliente. Asimismo, involucran a distintos actores en la cadena de valor (FSB, 2024), incluyendo proveedores de servicios tecnológicos que actúen bajo instrucción de la entidad bancaria y conforme a las necesidades que la misma pretende cubrir.

Dentro de este ecosistema tecnológico, y considerando la experiencia reciente, las tecnologías biométricas merecen una especial atención. Los datos biométricos, como el reconocimiento facial y las huellas dactilares, son cada vez más usados para verificar identidad y autenticar operaciones. Su uso puede responder a un fin legítimo de seguridad, y tanto el Comité de Basilea como el Banco Mundial lo reconocen, siempre que se acompañe de minimización de datos, privacidad desde el diseño y una clara delimitación de responsabilidades entre entidades financieras y proveedores tecnológicos (BCBS, 2026; Montes y Appaya, 2021).

Sin embargo, la legitimidad de la finalidad inicial no autoriza, por sí sola, la conservación indefinida de los datos, su comunicación a terceros ni su reutilización para fines distintos. Cada una de estas operaciones requiere una justificación jurídica y garantías adecuadas, especialmente cuando se trata de datos biométricos, que tanto la Ley № 6534/2020 de "Protección de Datos Personales Crediticios"[1] como la Ley № 7593/2025 "De Protección de Datos Personales en la República del Paraguay"[2] califican como datos sensibles, por lo que requieren una especial protección. Cabe recordar que la Ley № 7593/2025 deroga algunas disposiciones de la Ley № 6534/2020, entre ellas sus definiciones de datos personales y de datos sensibles, categoría que incluye los biométricos. Sin embargo, como la nueva ley recién será plenamente aplicable en noviembre de 2027, esas disposiciones siguen vigentes hasta entonces.

La distinción clave es entre los datos que técnicamente pueden recolectarse y los que pueden tratarse legítimamente. Pero esa distinción rara vez es clara para el cliente, que sabe qué datos entrega, pero no quién los trata como responsable o encargado, con qué límites ni con qué autorizaciones, ni qué perfiles se elaboran sobre él (Wachter y Mittelstadt, 2019). A esto hay que agregar que, a menudo, no puede rechazar esas condiciones sin renunciar al servicio, lo que debilita el consentimiento, sobre todo para datos sensibles como los biométricos.

1 Para consultar el texto legal: República del Paraguay. (2020). Ley N.º 6534/2020, de protección de datos personales crediticios. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-

2 Para consultar el texto legal: República del Paraguay. (2025). Ley N.º 7593/2025, de protección de datos personales en la República del Paraguay. BACN. https://www.bacn.gov.py/leyes-paraguayas/12924/ley-n-7593-proteccion-de-datos-personales

Algunos términos importantes para recordar	
Datos sensibles	categoría que exige protección reforzada, entre ellos aquellos que se refieren a origen racial, salud, entre otros. Se incluye en esta categoría a los datos biométricos.
Datos biométricos	los que permiten identificar a una persona a partir de rasgos físicos, como el rostro o la huella. La plantilla biométrica es una representación matemática de esos rasgos que el sistema usa para validar, por ejemplo, una identidad.
Datos inferidos	perfiles, puntajes o predicciones que la entidad genera a partir de otros datos.
Responsable y encargado del tratamiento de datos personales	quien decide para qué y cómo se tratan los datos, y quien los trata por cuenta de aquel.

EL MAPA NORMATIVO ACTUAL EN PARAGUAY: ¿ESTÁN PROTEGIDOS NUESTROS DATOS PERSONALES?

La protección de datos personales en el sector financiero paraguayo no opera en un vacío normativo. La Constitución protege la intimidad y provee garantías constitucionales como el *hábeas data* (artículos 33 y 135). Por su parte, la Ley Nº 6534/2020, que sigue plenamente vigente hasta fines de 2027, reconoce derechos de acceso, rectificación, oposición y eliminación (artículos 5 y 8), califica como sensibles los datos biométricos, limita a cinco años la conservación de datos que puedan afectar a su titular salvo norma especial y otorga facultades de aplicación al BCP y a la Secretaría de Defensa del Consumidor y el Usuario (SEDECO). Hasta que la Ley Nº 7593/2025 sea plenamente aplicable, la SEDECO seguirá siendo autoridad competente bajo la Ley Nº 6534/2020. A partir de entonces, toda referencia a la SEDECO en esa ley deberá entenderse hecha a la Agencia Nacional de Protección de Datos Personales según el art. 58 de la Ley Nº 7593/2025.

A este marco, se suman también el secreto bancario de la Ley General de Bancos (Ley Nº 861/1996, Capítulo II) y la normativa contra el lavado de activos, que exige a los sujetos obligados conservar durante al menos cinco años los documentos que identifican a los clientes y sus operaciones, contados desde el cierre de la cuenta (Ley Nº 1015/1997, art. 18, modificado por Ley Nº 6497/2019).

Por su parte, la Ley Nº 7593/2025 completará este mapa con un régimen general cuando sea plenamente aplicable, en noviembre de 2027, y cuente con la reglamentación que sigue pendiente. Esta ley incorpora los principios de finalidad, minimización y proporcionalidad; deberes de diligencia que incluyen la privacidad desde el diseño y por defecto; salvaguardas reforzadas para los datos sensibles; derechos frente a decisiones automatizadas o semiautomatizadas, incluidas las crediticias (art. 33). Igualmente, pertinente para servicios tecnológicos tercerizados, el artículo 11 también prevé, entre otros puntos, que el tratamiento realizado por cuenta de un responsable deba regirse por un contrato u otro instrumento jurídico que defina su naturaleza, sus fines y sus condiciones.

Dicha ley también designa una Agencia Nacional de Protección de Datos Personales, como autoridad competente en la materia. Respecto a la futura autoridad, durante la tramitación de la ley, la Asociación de Bancos del Paraguay (ASOBAN) advirtió sobre posibles superposiciones entre ésta y el BCP (ABC Color, 2025). El texto finalmente sancionado contempla la coexistencia del régimen general de protección de datos personales con disposiciones específicas sobre información crediticia y las competencias sectoriales correspondientes.

Además de estas normas, se encuentran la Resolución Nº 3, Acto Nº 8, del 21 de febrero de 2023, en materia de protección de la información crediticia que establece las competencias del ente regulador en este respecto. Así también, la Resolución SB.SG. Nº 124/2017 fija un marco de gobierno de tecnologías de la información y control interno para las entidades supervisadas, y la Resolución Nº 10/2022 regula el uso de servicios en la nube, donde en su artículo 4 (b) se exige cumplir la normativa de protección de datos personales y crediticios, evaluar a los proveedores y proteger la información tratada fuera de la infraestructura propia de la entidad.

De hecho, esta última resolución regula varios puntos de la arquitectura tecnológica operativa de un ente regulado por el BCP. Su artículo 6, por ejemplo, exige que los contratos prevean obligaciones de confidencialidad y seguridad, restricciones al uso de la información, condiciones de subcontratación y mecanismos de devolución o borrado seguro de los datos; el artículo 8 obliga a informar a la Superintendencia de Bancos sobre los proveedores, sus subcontratistas y el lugar donde se procesa la información; y el citado artículo 4 (o) deja en claro que la responsabilidad por la seguridad de la información recae en la entidad supervisada. La norma no alcanza a todos los proveedores ni a todos los usos, pero demuestra que la identificación de proveedores, las garantías contractuales y la localización del tratamiento ya son materia de supervisión.

Su relevancia resulta particularmente evidente cuando los servicios se prestan desde el extranjero o a través de empresas vinculadas a una misma estructura empresarial. La Ley Nº 7593/2025 refuerza este marco al establecer reglas sobre el alcance territorial de su aplicación y las transferencias internacionales de datos (arts. 2 y 19). Pero, más allá de la ubicación física de los servidores, una cuestión fundamental es determinar quién ejerce el control efectivo sobre la información y en qué condiciones puede exigirse su acceso, conservación, transferencia o eliminación.

De hecho, la citada Resolución Nº 10/2022 también provee un parámetro para examinar la relación entre Ueno Bank e ITTI, la empresa tecnológica de su mismo grupo económico. Como ambas atraviesan dificultades financieras y operativas al mismo tiempo, se vuelve urgente determinar quién custodia los datos personales de los clientes, dónde se alojan (algo que la política de privacidad de la entidad no precisa) y cómo se asegura la continuidad de su tratamiento. El proceso de resolución debe identificar el rol legal de cada entidad, la información que está bajo su control y los mecanismos contractuales disponibles para garantizar el ejercicio de los derechos de los clientes en cuanto a sus datos.

El caso Ueno Bank muestra la necesidad de actuar desde ahora. Las entidades financieras pueden aplicar las herramientas que ya ofrece la normativa vigente y, a la par, prepararse para cumplir las nuevas obligaciones de la Ley Nº 7593/2025. Esa preparación invita a revisar los contratos con proveedores tecnológicos, evaluar si el tratamiento de los datos es proporcional a los fines que persigue y verificar que los clientes reciban información clara sobre el uso de sus datos. Se puede partir por preguntarse: **¿Con qué base legal, bajo qué garantías y con qué restricciones contractuales trata hoy cada entidad los datos personales de sus clientes?**

Pero el cumplimiento de la legislación en materia de protección de datos no debe entenderse como el único criterio para determinar si una tecnología respeta los derechos de las personas. Los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos[3] distinguen entre el deber del Estado de proteger los derechos humanos y la responsabilidad de las empresas de respetarlos, lo cual incluye llevar a cabo una diligencia debida en materia de derechos humanos (Naciones Unidas, 2011, Principios 11, 13 y 17). Esta distinción es especialmente importante, por ejemplo, cuando se evalúa el uso de tecnologías como las de identificación biométrica por entes regulados como los bancos.

También los principios de legalidad, finalidad legítima, necesidad y proporcionalidad ofrecen un marco útil para evaluar las implicaciones de las tecnologías biométricas en los servicios financieros en materia de derechos humanos. Aunque estos criterios se desarrollaron principalmente para examinar la injerencia del Estado en los derechos de las personas, también sirven de referencia para la diligencia debida en materia de derechos humanos en el sector privado. De hecho, en esta línea, la Agencia Española de Protección de Datos (AEPD, 2026) se expidió en una consulta sobre la importancia de distinguir entre la necesidad del tratamiento biométrico, la disponibilidad de alternativas menos intrusivas y las condiciones necesarias para que el consentimiento sea verdaderamente libre. Dicha decisión también sugiere tener en cuenta los riesgos específicos que se abordan, la eficacia de las medidas alternativas y las características del sistema biométrico, en lugar de dar por sentado que todas las tecnologías implican niveles de riesgo equivalentes.

Esta evaluación cobra especial importancia en situaciones donde el registro biométrico se vuelve un requisito ineludible de acceso a un servicio, como se dio en el caso de la entidad bancaria intervenida. Según las bases y condiciones publicadas por Ueno Bank, para abrir una cuenta a través de su aplicación móvil, las personas usuarias debían grabarse un video para verificar su identidad. El banco también ofrecía autenticación biométrica para acceder a su aplicación. De hecho, esta práctica no es exclusiva de la entidad bancaria en proceso de resolución. Otras entidades del sector también ofrecen abrir cuentas desde sus aplicaciones mediante selfie y la fotografía del documento de identidad, como es la "Cuenta Light" de Itaú (InfoNegocios, 2025), o utilizan la biometría del dispositivo para autenticas operaciones, como el Banco Nacional de Fomento (BNF, s.f.).

3 Para consultar el texto, visitar el enlace. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2011). *Principios Rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar"* (HR/PUB/11/04). Naciones Unidas. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf



Fuente: Ueno Bank S.A. [@ueno_py]. (2026, 22 de octubre). ¡Tu nueva cuenta está a una selfie de distancia!. [carrusel]. Instagram. https://www.instagram.com/p/DezQVkckRne/?jplx=Nm8zYm81YTV2Zjd1

En esas condiciones, no basta con incorporar tecnología como propuesta de mejora al servicio ofrecido (Morozov, 2013). Las instituciones financieras deben poder justificar el uso de la identificación biométrica, evaluar previamente alternativas menos intrusivas y demostrar que los beneficios de seguridad esperados son proporcionales a los riesgos que implica para la privacidad y la protección de datos personales (ACNUDH, 2021). Cuando se recurre al consentimiento, es esencial que exista una verdadera libertad de elección, que implica contar con una alternativa real y efectiva, y que no suponga una carga desproporcionada para los clientes. Además, deben documentar de manera transparente el rol de sus proveedores tecnológicos, la ubicación y las condiciones del tratamiento de datos y las garantías contractuales aplicables, aspectos ya cubiertos por la Resolución Nº 10/2022 del BCP (artículos 6 y 8).

DE LA NORMA A LA ACCIÓN: ¿QUIÉN CUSTODIA NUESTROS DATOS PERSONALES CUANDO UN BANCO ENTRA EN CRISIS?

El régimen de la Ley Nº 2334/2003 de garantía de depósitos y resolución de entidades de intermediación financiera está pensado para ordenar depósitos, activos y pasivos y evitar el contagio al resto del sistema. Esta norma no establece un régimen específico para el tratamiento de bases de datos personales o biométricos durante ese procedimiento. Su artículo 14 atribuye a los interventores la realización de actos de conservación y aquellos necesarios para llevar adelante la resolución. Precisamente, este silencio normativo, plantea la necesidad de analizar cómo deben garantizarse, durante ese proceso, la integridad, disponibilidad y protección de la información que permanece bajo custodia de la entidad o de sus proveedores tecnológicos.

De hecho, podemos citar como caso comparativo lo ocurrido en Brasil, donde el tema se discutió tras la caída del conglomerado Banco Master. En dicho proceso se sostuvo que es el liquidador quien asume las obligaciones propias del responsable del tratamiento, entre ellas, de seguridad, prevención de incidentes, rendición de cuentas (Análise, 2026).

Pero se debe recordar que estamos hablando de que esa información custodiada está conformada por distintas categorías de datos, personales y no personales. No todos los datos tienen el mismo destino y no a todos aplican las mismas reglas en cuanto a su tratamiento. Así, el primer error a evitar es tratar el consentimiento como la única base legal posible.

La Ley Nº 7593/2025, que ofrece el marco de referencia, aunque todavía no plenamente aplicable, admite el tratamiento cuando es necesario para cumplir una obligación legal, ejecutar un contrato con el titular, ejercer derechos en procedimientos judiciales o satisfacer un interés legítimo, además del consentimiento (artículo 5). En un proceso de resolución bancaria, algunas operaciones de tratamiento de datos personales podrían encontrar justificación en obligaciones legales de conservación, la continuidad de relaciones contractuales o la necesidad de atender procedimientos administrativos o judiciales. Sin embargo, la base jurídica aplicable debe determinarse atendiendo a la finalidad y las circunstancias de cada tratamiento.

Este aspecto requiere especial atención cuando se trata de datos sensibles. Dicha ley, en su artículo 20, establece un régimen reforzado para su tratamiento y contempla supuestos excepcionales que deben interpretarse conforme a sus requisitos específicos. En el caso de los datos biométricos utilizados para autenticación, corresponde examinar si su conservación o eventual transferencia sigue siendo necesaria y jurídicamente admisible una vez iniciada la resolución bancaria. Por ello, las plantillas biométricas no deberían trasladarse automáticamente junto con las carteras o contratos financieros, sino someterse previamente a una evaluación específica de su finalidad, base jurídica y garantías aplicables.

En este contexto, corresponde pensar en las medidas específicas que se necesitan para proteger las bases de datos personales, particularmente las que contienen información sensible. Esto cobra especial relevancia cuando los proveedores tecnológicos también enfrentan dificultades operativas o financieras, como es el caso de ITTI (La Nación, 2026a), dado que pueden surgir interrogantes sobre la disponibilidad de la información, las restricciones de acceso y el cumplimiento de las obligaciones contractuales de conservación, devolución o eliminación de datos. Acá, recordemos que, la Resolución Nº 10/2022 ofrece un punto de partida para examinar estas responsabilidades en el ámbito de los servicios de computación en la nube.

Entonces, cuando un banco y su proveedor de tecnología enfrentan dificultades al mismo tiempo, **¿quién garantiza la integridad, la disponibilidad y el manejo legal de los datos de los clientes?**

La respuesta del regulador no puede limitarse a los aspectos netamente financieros. Los interventores también deben identificar quién controla la información y verificar las medidas de seguridad que rigen su acceso, retención, transferencia o eliminación, especialmente cuando se trata de datos sensibles, como los biométricos.

Estas preocupaciones ya no son meramente teóricas. El jefe de Cibercrimen de la Policía Nacional de Paraguay, Diosnel Alarcón, advirtió recientemente sobre el riesgo de robo de identidad en caso de que la información biométrica fuera obtenida o comercializada de manera ilegal. También informó que se han enviado solicitudes a Google y Amazon para que protejan y bloqueen el acceso a la información almacenada por ITTI, tanto de clientes de servicios financieros como de asistentes a eventos masivos (Última Hora, 2026). Aunque estas declaraciones no confirman una filtración de datos, sí ponen hincapié en la urgencia de aclarar quién custodia esa información y qué medidas se han adoptado para protegerla de los riesgos asociados a la misma.

Guardar, transferir o borrar: ¿cuál debería ser el destino de nuestros datos personales?	
Datos que deberían conservarse	Los registros necesarios para cumplir obligaciones legales, regulatorias o atender investigaciones y procedimientos pendientes. Pero conservar no implica disponibilidad de uso, estos datos deben quedar protegidos, con acceso restringido y sin reutilizarse para finalidades incompatibles. La necesidad de conservar datos biométricos debe evaluarse específicamente.
Datos que pueden transferirse	La transferencia de cuentas, contratos o carteras puede requerir comunicar determinados datos personales a otras entidades. Deben transferirse únicamente los datos necesarios para la finalidad correspondiente, bajo garantías de seguridad, confidencialidad y transparencia. Los datos sensibles, como las plantillas biométricas, requieren una evaluación jurídica reforzada; no deberían trasladarse automáticamente junto con la cartera financiera.
Datos que deberían eliminarse	Los datos cuya conservación ya no responda a una finalidad legítima ni a una obligación legal deben suprimirse de forma segura, considerando los plazos aplicables. Esto puede incluir plantillas biométricas, información utilizada exclusivamente para mercadeo o perfiles derivados que ya no resulten necesarios. La eliminación debe comprender también las copias conservadas por proveedores tecnológicos, cuando corresponda, y ser verificable.

Estas categorías no deben tomarse como reglas automáticas de conservación, transferencia o eliminación de datos personales, sino como criterios orientativos para evaluar el destino de la información en un proceso de resolución de una entidad bancaria, atendiendo a su naturaleza, finalidad y régimen jurídico aplicable. De igual manera, aunque todavía son limitadas las guías en cuanto a cómo deben ser tratadas las bases de datos personales como parte de lo que una resolución debe ordenar, se podrían esbozar algunas recomendaciones dirigidas sobre todo al ente regulador y sus interventores, con base en las normas y estándares que actualmente existen:

- **Realizar un inventario en plazo breve:** qué bases existen, quién las controla, dónde se alojan y qué proveedores y subcontratistas acceden a ellas. Buena parte de esa información ya debería estar en poder de la Superintendencia por la Resolución № 10/2022.
- **Clasificación con criterios legales y transparentes:** qué se conserva y bloquea, qué se transfiere y qué se elimina, con un registro de las decisiones adoptadas.
- **Medidas específicas sobre datos biométricos y otros datos sensibles:** identificación y protección reforzada de las bases, restricción de los tratamientos no necesarios para la resolución y evaluación de su conservación o eliminación segura, con mecanismos de verificación a los proveedores tecnológicos cuando corresponda. Además, proveer al respecto, información clara respecto a las vías disponibles para ejercer sus derechos.
- **Minimizar la concentración innecesaria de datos personales sensibles y biométricos:** en el marco de sus funciones de supervisión, el BCP, en coordinación con la futura Agencia Nacional de Protección de Datos, debería alentar a las entidades a evaluar sistemas de autenticación que no requieran bases de datos biométricas centralizadas y permanentes. Toda base persistente en este sentido, y su eventual uso compartido, debería justificarse expresamente.

Posteriormente, una vez sorteada la crisis, debería pensarse en cómo **socializar e incorporar una gobernanza de datos más robusta**, que prevea salvaguardas expresas en caso de riesgos como el presente y que hagan posible la identificación de los responsables de la información, las condiciones expresas para las transferencias y protección continuada de los datos personales.

La gobernanza preventiva de los datos también requiere evaluar el impacto potencial de las tecnologías antes de su implementación, en lugar de abordar sus consecuencias después de una crisis. El artículo 14 de la Ley № 7593/2025 establece la obligación de realizar evaluaciones de impacto en materia de protección de datos para las operaciones de tratamiento que impliquen riesgos significativos, incluyendo el tratamiento a gran escala de datos sensibles y ciertas formas automatizadas de elaboración de perfiles. Aunque estas obligaciones aún no están en vigor, su próxima implementación ofrece la oportunidad de fortalecer las prácticas actuales de supervisión financiera.

En el marco de sus actuales facultades regulatorias y de supervisión, **el BCP podría promover orientaciones más explícitas sobre la evaluación de los sistemas de identificación biométrica, la disponibilidad de alternativas menos intrusivas, las responsabilidades de los proveedores de tecnología y el manejo de información sensible durante la resolución financiera.** Además, estas medidas deben ir acompañadas de información pública accesible que explique las garantías aplicables a las personas y los derechos que pueden ejercer.

También, debería controlarse que los contratos con proveedores tecnológicos críticos garanticen el acceso del interventor, la continuidad del servicio y la devolución o el borrado de los datos aun si la entidad supervisada o el proveedor dejan de operar. Finalmente, de cara a la implementación de la Ley Nº 7593/2025, sería conveniente prever mecanismos formales de coordinación entre el BCP y la futura autoridad de protección de datos personales, especialmente para aquellos supuestos de intervención o resolución de entidades financieras que involucren el tratamiento de información sensible.

La gobernanza de los datos debe ser considerada como parte indefectible de la gestión de riesgos de las partes involucradas en la provisión de los servicios financieros. La protección de datos personales no debería convertirse en una preocupación solo después de que se produzca una crisis financiera, un incidente de seguridad o acusaciones de uso indebido. **Los datos personales no deben ser vistos solo como un activo comercial y su tratamiento debe estar sujeto a las obligaciones legales aplicables**, independientemente del sector y del valor económico que dicha información pueda representar.

RECAPITULANDO

Como actividad sujeta a la supervisión del Estado, la banca debe evaluar los riesgos de su transformación digital no solo en términos prudenciales y de cumplimiento legal, sino también desde un enfoque de derechos humanos, en línea con la debida diligencia que exigen los Principios Rectores de la ONU sobre las empresas y los derechos humanos. Este enfoque lleva a preguntarse no solo si una entidad está legalmente autorizada a recopilar información biométrica, sino también si esa práctica es necesaria, proporcionada y compatible con la privacidad, la autonomía de las personas y su acceso a los servicios financieros. La innovación tecnológica no equivale automáticamente a progreso, y menos para todos por igual, cuando las alternativas son limitadas y las personas tienen poco control sobre el uso posterior de su información.

La caída de Ueno Bank, presentado como el primer banco digital del país, muestra por qué estas preocupaciones no pueden quedar fuera de las atribuciones del ente supervisor. Cuando una entidad deja de operar, la protección de sus clientes debe ir más allá de los depósitos y abarcar también la información personal acumulada a lo largo de la relación bancaria. Esto es especialmente importante cuando están en juego datos sensibles, como los biométricos, cuyo uso indebido puede tener consecuencias mucho después del cierre de un banco.

La implementación de la Ley Nº 7593/2025, que será plenamente aplicable en noviembre de 2027, ofrece la oportunidad de avanzar hacia un modelo de gobernanza preventivo, en el que la innovación se evalúe no solo por su eficiencia y su seguridad, sino también por su impacto en los derechos de las personas. Para que la rendición de cuentas sea efectiva, las entidades reguladas, sus proveedores tecnológicos y las autoridades competentes deben comenzar a abordar estos riesgos antes de que se materialicen y no solo ante una crisis.

DIVULGACIÓN SOBRE EL USO DE HERRAMIENTAS ASISTIDAS POR IA

En la preparación de este artículo se utilizaron herramientas de IA generativa (Claude y Gemini LM) como apoyo en la búsqueda y verificación de fuentes, revisión lingüística, edición en cuanto a la extensión del texto, revisión de formulaciones y unificación de las referencias en formato APA. El análisis jurídico, la interpretación de fuentes, el contenido final y las conclusiones, corresponden a la autora.

REFERENCIAS

Agencia Española de Protección de Datos [AEPD]. (2026, 3 de noviembre). Análisis sobre la necesidad, libertad de elección y riesgo efectivo en el tratamiento de datos biométricos. https://www.aepd.es/informes-y-resoluciones/criterios-juridicos-aepd/analisis-sobre-necesidad-libertad-de-eleccion-datos-biometricos

Aggarwal, N. (2021). The norms of algorithmic credit scoring. The Cambridge Law Journal, 80(1), 42–73. https://doi.org/10.1017/S0008197321000015

Alta Comisionada de las Naciones Unidas para los Derechos Humanos [ACNUDH]. (2021). El derecho a la privacidad en la era digital (A/HRC/48/31). Consejo de Derechos Humanos. https://docs.un.org/es/A/HRC/48/31

Análise. (2026, 27 de febrero). Veja como preservar dados de clientes em uma liquidação extrajudicial. https://analise.com/noticias/veja-como-preservar-dados-de-clientes-em-uma-liquidacao-extrajudicial

ABC Color. (2025, 6 de julio). Preocupa a Asoban que ley de datos personales sea barrera para acceder a registros de funcionarios públicos. https://www.abc.com.py/politica/2025/07/06/preocupa-a-asoban-que-ley-de-datos-personales-sea-barrera-para-acceder-a-registros-de-funcionarios-publicos/

ABC Color. (2026, 3 de noviembre). Ueno Bank: el BCP anuncia “procedimiento de resolución”. https://www.abc.com.py/economia/2026/11/03/ueno-bank-el-bcp-anuncia-procedimiento-de-resolucion/

Banco Central del Paraguay. (2017). Resolución SB.SG. N.º 124/2017: Manual de Gobierno y Control de Tecnologías de Información.

Banco Central del Paraguay. (2022). Resolución N.º 10, Acta N.º 43: Reglamento de uso de servicios para computación en la nube.

Banco Central del Paraguay. (2023). Resolución N.º 3, Acta N.º 8: Reglamento de burós de información crediticia y protección de información personal crediticia.

Banco Central del Paraguay. (2026, 3 de noviembre). Banco Central inicia el procedimiento de resolución de Ueno Bank. https://www.bcp.gov.py/web/institucional/w/banco-central-inicia-el-procedimiento-de-resolucion-de-ueno-bank

Banco de Desarrollo de América Latina [CAF]. (2016) La Revolución De Las Empresas Fintech Y El Futuro De La Banca. Disrupción tecnológica en el sector financiero. ISBN 978-980-6810-67-9.

Basel Committee on Banking Supervision [BCBS]. (2026). Digitalisation and financial technology risks (Basel Consolidated Guidelines, RMA50). Bank for International Settlements. https://www.bis.org/committees/bcbs/basel-consolidated-guidelines/module/rma/50

Banco Nacional de Fomento [BNF]. (s.f.). BNF Paraguay [Aplicación móvil]. App Store. Recuperado el 19 de noviembre de 2026, de https://apps.apple.com/py/app/bnf-paraguay/id6503985911?l=en-GBBNF Paraguay

InfoNegocios. (2025). Itaú acelera la banca digital: Lanza Cuenta Light y promete abrir cuentas en solo minutos. https://infonegocios.com.py/conosur/itau-acelera-la-banca-digital-lanza-cuenta-light-y-promete-abrir-cuentas-en-solo-minutos

Bogado Rodas, A. (2026). Vigilancia biométrica: Reconocimiento facial y derechos humanos en eventos deportivos de Paraguay. TEDIC. https://www.tedic.org/wp-content/uploads/2026/05/Vigilancia-biometrica-en-los-estadios-WEB.pdf

Desantis, D. y O'Boyle, B. (2026, 8 de noviembre). How a digital bank's collapse toppled Paraguay's president. Reuters. https://www.reuters.com/business/finance/how-digital-banks-collapse-toppled-paraguays-president-2026-11-08/

El Surtidor. (2024, 4 de diciembre). Tus datos, el negocio del Grupo Vázquez. https://elsurti.com/oligarquia/reportaje/2024/12/04/tus-datos-el-negocio-del-grupo-vazquez/

Fernández, M. I., & Heredia, R. (2026). Pilotos de transformación digital para las instituciones financieras de desarrollo: Avances en la digitalización financiera en América Latina. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0013933

Financial Stability Board. (2024). Guidance on arrangements to support operational continuity in resolution (revised version 2024) https://www.fsb.org/uploads/P180324.pdf

Galli, G. (2024). Protección de datos personales en el sector privado en Paraguay: Un estudio exploratorio. TEDIC. https://www.tedic.org/wp-content/uploads/2024/08/Proteccion-datos-personales-WEB.pdf

International Finance Corporation. (2026). Cracking the credit code: Alternative data and AI for financial inclusion. https://www.ifc.org/content/dam/ifc/doc/2026/cracking-the-credit-code-alternative-data-and-ai-for-financial-inclusion-summary.pdf

Itaú Paraguay. (s.f.). Política de privacidad. Recuperado el 12 de noviembre de 2026, de https://www.itau.com.py/Paginas/Politicas_de_privacidad#informacion

Kerse, M., Newbury, L. B., & Staschen, S. (2024). Financial inclusion and disruptive innovation: Regulatory implications (Working Paper). CGAP. https://www.cgap.org/research/financial-inclusion-and-disruptive-innovation-regulatory-implications

King, Brett. (2018). Bank 4.0: Banking everywhere, never at a bank. Marshall Cavendish International (Asia) Pte Ltd. ISBN 9814771767

La Nación. (2026a, 6 de noviembre). Caso ueno: ITTI cae de A+ a C en calificación de riesgo y advierten posible incumplimiento de deudas. https://www.lanacion.com.py/negocios/2026/11/06/caso-ueno-itti-cae-de-a-a-c-en-calificacion-de-riesgo-y-advierten-posible-incumplimiento-de-deudas/

La Nación. (2026b, 12 de noviembre). Ocho bancos iniciaron entrega de tarjetas para jubilados que cobraban por Ueno Bank. https://www.lanacion.com.py/negocios/2026/11/12/ocho-bancos-iniciaron-entrega-de-tarjetas-para-jubilados-que-cobraban-por-ueno-bank/

MarketData. (2026). La información biométrica de Ueno y los límites legales para su utilización dentro del grupo económico. https://marketdata.com.py/laboratorio/analisis/la-informacion-biometrica-de-ueno-y-los-limites-legales-para-su-utilizacion-dentro-del-grupo-economico-156905

Montes, F., & Appaya, S. (2021). Digital ID to enhance financial inclusion: A toolkit for regulatory authorities. World Bank Group. https://documents.worldbank.org/curated/en/099650005162214653

Morozov, E. (2013). To save everything, click here: The folly of technological solutionism. PublicAffairs.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2011). Principios Rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (HR/PUB/11/04). Naciones Unidas. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

República del Paraguay. (2020). Ley N.º 6534/2020, de protección de datos personales crediticios. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-

República del Paraguay. (2025). Ley N.º 7593/2025, de protección de datos personales en la República del Paraguay. BACN. https://www.bacn.gov.py/leyes-paraguayas/12924/ley-n-7593-proteccion-de-datos-personales

Ruíz Díaz, Laura. (2026a, 7 de noviembre). Ueno bank cayó, ¿quién responde por los datos personales de casi 3 millones de clientes? Última Hora. https://www.ultimahora.com/ueno-bank-cayo-quien-responde-por-los-datos-personales-de-casi-3-millones-de-clientes

Ruíz Díaz, Laura. (2026b, 15 de noviembre). Los datos de un país, un activo en el limbo tras la caída de ueno. Última Hora. https://www.ultimahora.com/los-datos-de-un-pais-un-activo-en-el-limbo-tras-la-caida-de-ueno

Sequera Buzarquis, M. (2026, 12 de noviembre). Caso UENO: biometría, datos personales y la deuda del Estado paraguayo. TEDIC. https://www.tedic.org/caso-ueno-biometria-datos-personales-y-la-deuda-del-estado-paraguayo/

Sudameris. (s.f.). Política de Privacidad y Protección de Datos Personales. Recuperado el 12 de noviembre de 2026, de https://www.sudameris.com.py/institucional/politica-privacidad

TEDIC. (2025). Expo Paraguay 2025: Surveillance, lack of protection, and exclusion of citizens. https://www.tedic.org/en/?p=29609

Ueno Bank S.A. (s.f.-a). Política de tratamiento de datos personales. Recuperado el 12 de noviembre de 2026 de https://www.ueno.com.py/proteccion-de-datos/

Ueno Bank S.A. (s.f.-b). Contrato único de productos y servicios bancarios. Recuperado el 18 de noviembre de 2026. https://web.archive.org/web/20261106113647/https://www.ueno.com.py/bases-y-condiciones/

Ueno Bank S.A. (s.f.c). Bases y Condiciones. Recuperado el 18 de noviembre de 2026. https://web.archive.org/web/20261119103218/https://www.ueno.com.py/bases-y-condiciones/

Última Hora. (2026, 18 de noviembre). Datos biométricos: Tres millones de usuarios expuestos a la suplantación de identidad, advierte jefe policial. https://www.ultimahora.com/datos-biometricos-tres-millones-de-usuarios-expuestos-a-la-suplantacion-de-identidad-advierte-jefe-policial

UNID. (s.f.). unid. Recuperado el 18 de noviembre de 2026 https://web.archive.org/save/https://unid.com.py/#faqs

Wachter, S., y Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494–620 https://journals.library.columbia.edu/index.php/CBLR/article/view/3424/1370


Tecnología
& Derechos
Humanos