SOVOS

Optimización, Seguridad y Cumplimiento

Claves tecnológicas para escalar sin riesgos en la industria financiera

Contenido

Introducción

La industria financiera en Latinoamérica ha atravesado una transformación estructural, impulsada por la digitalización, la evolución del marco regulatorio y la necesidad urgente de modernizar sus infraestructuras tecnológicas. México, Chile y Perú se han consolidado como mercados clave en esta evolución, con contextos particulares que demandan enfoques técnicos diferenciados en materia de innovación, ciberseguridad y cumplimiento normativo.

La pandemia de COVID-19 aceleró de forma decisiva la transición hacia canales digitales, obligando a las entidades financieras a replantear su arquitectura tecnológica, escalar sus capacidades en la nube y asegurar la disponibilidad y seguridad de sus plataformas.

En México, Perú y Chile, los bancos aumentaron significativamente sus inversiones en plataformas en línea, automatización de procesos y aplicaciones móviles, buscando no solo mejorar la experiencia del usuario, sino también garantizar continuidad operativa en un entorno altamente exigente. Por ejemplo, en el primer trimestre de 2022 en Perú, el 40% del total de las transacciones intrabancarias se realizaron mediante billeteras digitales, que evidencia una rápida adopción de canales móviles que desafía la escalabilidad de los sistemas existentes.

A este entorno se suma la creciente irrupción de fintechs que operan con agilidad y alto grado de digitalización. Solo en México operan más de 1.100 iniciativas fintech, mientras que Perú alcanzó 346 en 2023, consolidando su posicionamiento como mercado en crecimiento. Esta proliferación ha generado una presión adicional sobre los equipos TI, que deben garantizar la interoperabilidad entre actores tradicionales y emergentes, habilitar esquemas de banca abierta y adaptar sus infraestructuras a modelos híbridos con múltiples integraciones API.

En paralelo, los gobiernos han endurecido sus marcos regulatorios con foco en la transparencia, la inclusión y la seguridad. Chile destaca con la promulgación de la Ley 21.521 (Ley Fintech), que establece las bases para un ecosistema de Finanzas Abiertas y fortalece el rol de la Comisión para el Mercado Financiero (CMF). Esta nueva legislación desafía a las áreas de TI a desarrollar capacidades avanzadas en seguridad de la información, gobierno de datos y cumplimiento automatizado, integrando la regulación desde el diseño (compliance by design).

“La pandemia de COVID-19 aceleró de forma decisiva la transición hacia canales digitales”

Impacto de la transformación digital en bancos, fintechs y aseguradoras

La transformación digital ha redefinido los modelos operativos de bancos, fintechs y aseguradoras en México, Perú y Chile, generando una presión directa sobre las áreas tecnológicas para responder con agilidad, resiliencia y seguridad. Ya no se trata solo de digitalizar servicios: hoy, la competitividad depende de la capacidad de las instituciones para integrar tecnologías emergentes en arquitecturas escalables, adaptativas y seguras.

Los bancos tradicionales han acelerado la modernización de sus plataformas core, impulsando iniciativas de banca omnicanal, automatización de procesos mediante RPA y el uso de inteligencia artificial para mejorar la experiencia del cliente.

Esto ha implicado adoptar modelos híbridos en la nube, desarrollar APIs abiertas y aplicar esquemas que integren la seguridad dentro del ciclo de vida de desarrollo de software (DevSecOps) para reducir el time-to-market de nuevos productos sin comprometer la seguridad. Casos como el de BBVA México, que adquirió la fintech Openpay para reforzar su oferta digital, ilustran cómo los líderes de TI están asumiendo un rol clave en la integración de capacidades externas dentro de los sistemas existentes.

Por su parte, las fintechs están impulsando un cambio estructural en el sector, con propuestas centradas en la experiencia del usuario y ciclos de desarrollo ultrarrápidos. Para los líderes tecnológicos de las instituciones tradicionales, esto representa un desafío doble: garantizar la interoperabilidad entre sistemas heterogéneos y evolucionar hacia infraestructuras que soporten esquemas de colaboración abiertos, modulares y seguros.

En Perú, más de la mitad de las fintechs están enfocadas en la inclusión financiera, lo que obliga a TI a contar con soluciones con alta disponibilidad, cobertura geográfica extendida y bajos requisitos de conectividad, todo ello sin descuidar la seguridad ni el cumplimiento normativo.

En el caso de las aseguradoras, la transformación digital ha impulsado el uso de tecnologías como blockchain para la trazabilidad de siniestros y contratos inteligentes, así como la adopción de plataformas de analítica avanzada y automatización para gestionar grandes volúmenes de datos en tiempo real. En Chile, la nueva legislación fintech está habilitando a las aseguradoras a ofrecer productos más personalizados, lo que requiere una integración fluida entre sistemas internos, aplicaciones de terceros y mecanismos robustos de protección de datos.

El papel de las regulaciones en la innovación y la seguridad: implicancias para TI

La evolución del marco regulatorio en la industria financiera de México, Perú y Chile ha sido clave para habilitar nuevos modelos de negocio. Sin embargo, para los líderes de Tecnología e Innovación, estas regulaciones son impulsores que demandan cambios estructurales en la arquitectura tecnológica, la gestión de datos y la ciberseguridad.

La Ley Fintech de México, aprobada en el 2018, se ha convertido en un referente de la regulación de tecnologías financieras, al establecer estándares para el uso de criptoactivos, pagos electrónicos y financiamiento colectivo.

No obstante, la implementación de su componente más innovador, la banca abierta, ha avanzado lentamente, lo que genera incertidumbre técnica sobre cómo diseñar, exponer y consumir APIs financieras de forma estandarizada y segura. Para los líderes de TI, esto implica anticiparse a escenarios de interoperabilidad compleja, diseñar gateways de integración robustos y asegurar un gobierno de datos compatible con futuros requerimientos.

En Perú, aunque no existe una ley fintech integral, las autoridades han optado por una estrategia gradual con lineamientos técnicos orientados a fortalecer la supervisión y a construir una arquitectura de finanzas abiertas. Esto representa tanto una oportunidad como un reto: los equipos de tecnología deben preparar sus plataformas para un entorno donde el control de acceso, la trazabilidad, el consentimiento del usuario y la gestión de riesgos deben ser nativos en cada desarrollo.

Chile, por su parte, ha adoptado una visión avanzada con la Ley 21.521 (Ley Fintech), que establece un marco para las finanzas abiertas y fortalece el rol de la Comisión para el Mercado Financiero (CMF). Desde la perspectiva de TI, esta normativa implica adoptar modelos de integración basados en APIs seguras, implementar procesos de autenticación y autorización bajo el principio de “consentimiento informado”, y garantizar la protección de datos en todas las transacciones. También sugiere la adopción de una infraestructura compliance-ready, que permita responder a nuevos requerimientos regulatorios sin rediseños estructurales.

En los tres países, los marcos normativos están avanzando hacia un modelo que combina regulación estricta con habilitación tecnológica. Para los CIOs y líderes de innovación, el desafío no es solo garantizar el cumplimiento, sino construir plataformas flexibles, seguras y escalables que integren desde el inicio la visión regulatoria. Esto implica adoptar enfoques como security & compliance by design, automatizar procesos de auditoría, y establecer una gobernanza sólida de datos e identidades.

Panorama financiero de México, Perú y Chile

México, un mercado en expansión con foco en el crecimiento fintech

En los últimos cinco años, el ecosistema fintech en México ha crecido exponencialmente, consolidándose como el segundo más grande de América Latina, sólo detrás de Brasil. Según el informe Fintech Radar México 2025 de Finnovista, el número de startups fintech pasó de 512 en 2021 a más de 800 en 2024, un crecimiento superior al 50%.

Este ha sido impulsado por diversos factores. Uno de ellos es la inclusión financiera, ya que el 50% de la población mexicana no tiene acceso a la banca tradicional, lo que ha impulsado a las fintechs como alternativa mediante soluciones digitales accesibles. Por otro lado, la aceleración de la digitalización durante la pandemia de COVID-19, que impulsó el uso de pagos electrónicos y el acceso a la banca en línea. De acuerdo con datos de la CNBV y BBVA Research, las cuentas móviles pasaron de 11,8 millones en 2017 a más de 82 millones en 2023, reflejando una adopción masiva de servicios financieros digitales.

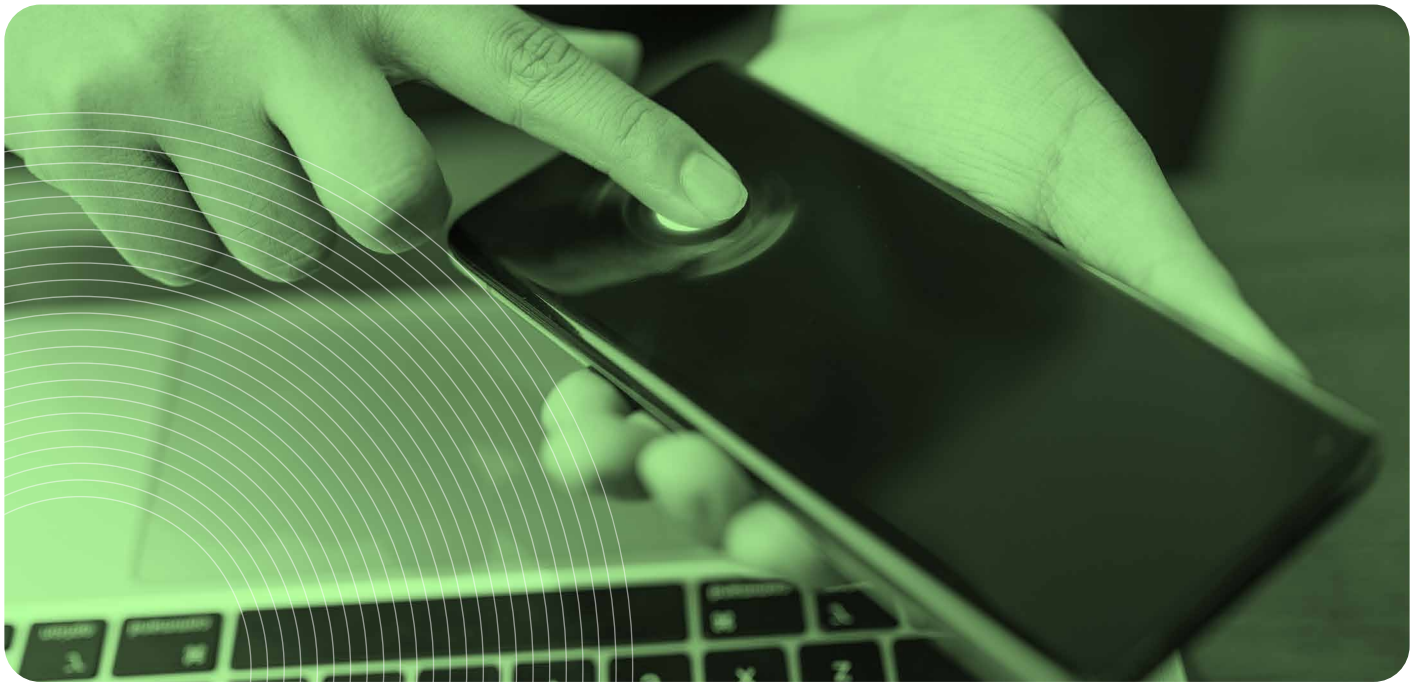
> **"El 50% de la población mexicana no tiene acceso a la banca tradicional"**

Este entorno también fomentó el crecimiento del comercio electrónico, que en 2024 registró un aumento del 20% respecto al año anterior, alcanzando un valor de 789,7 mil millones de pesos, según la Asociación Mexicana de Venta Online (AMVO). Las fintech han jugado un papel clave en este proceso, facilitando pagos en línea y ofreciendo financiamiento a negocios digitales, lo que ha contribuido a consolidar el ecosistema tecnológico del país.

Además, la innovación en modelos de negocio ha sido un motor esencial. Empresas como Clip y Konfío han desarrollado soluciones de pago y crédito dirigidas a pequeñas y medianas empresas, tradicionalmente desatendidas por la banca, ampliando así el acceso a herramientas financieras eficientes.

En paralelo, el marco regulatorio ha proporcionado un impulso decisivo. La ley para regular las Instituciones de Tecnología Financiera (Ley Fintech), promulgada en 2018, brindó certeza jurídica a actividades como los fondos de pago electrónico y el financiamiento colectivo, fortaleciendo la confianza tanto de usuarios como de inversionistas. Gracias a esta normativa, hoy más de 40 instituciones operan bajo supervisión del Banco de México y la Comisión Nacional Bancaria y de Valores (CNBV), en un entorno más seguro y estructurado.

La ley también sentó las bases para el Open Banking, permitiendo el intercambio de datos financieros con consentimiento del usuario, y fomentando la creación de servicios personalizados. No obstante, su implementación ha avanzado lentamente debido a la falta de lineamientos secundarios y retrasos en su implementación técnica, lo que genera incertidumbre para algunas startups que buscan operar dentro de este marco.



Desafíos de seguridad y cumplimiento ante el fraude digital

El avance de la banca digital, el surgimiento de nuevas tecnologías y la implementación de un marco regulatorio sólido han transformado radicalmente los servicios financieros en México. Sin embargo, esta evolución también ha traído consigo importantes desafíos en materia de seguridad y cumplimiento, especialmente frente al creciente fraude digital.

De hecho, este tipo de delito se ha convertido en el más frecuente del país. La Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2024, elaborada por el INEGI, reporta que durante 2023 se registraron casi 7.000 casos de fraude por cada 100.000 habitantes, lo que representa el 21% del total de delitos. Estas cifras incluyen fraudes bancarios y al consumidor, con impacto tanto en personas como en empresas.

El sector de las criptomonedas y los pagos digitales también enfrenta vulnerabilidades, debido en parte a la falta de una regulación específica. A ello se suma la escasa educación financiera y digital entre los usuarios, lo que los expone a riesgos como el robo de datos, suplantación de identidad y otros ataques cibernéticos.

> **“Tecnologías como blockchain están ganando relevancia”**

Para enfrentar estas amenazas, las instituciones financieras han comenzado a incorporar tecnologías avanzadas en sus sistemas de protección. La autenticación biométrica —que permite verificar la identidad mediante huellas digitales, reconocimiento facial o de voz— se ha posicionado como una de las principales herramientas para reducir accesos no autorizados.

Asimismo, tecnologías como blockchain están ganando relevancia, al ofrecer mayor seguridad y trazabilidad en las transacciones, dificultando la alteración de registros y reforzando la confianza en los entornos digitales. En paralelo, la inteligencia artificial y el machine learning se han convertido en aliados clave para la detección temprana de fraudes, ya que permiten analizar patrones de comportamiento en tiempo real e identificar actividades sospechosas antes de que se conviertan en amenazas concretas.

A medida que los ciberdelincuentes perfeccionan sus métodos, la adopción de soluciones innovadoras será fundamental para mantener la seguridad digital y fortalecer la confianza de los usuarios en el ecosistema financiero.

Del efectivo a la banca digital: el camino de Perú hacia la inclusión financiera

En los últimos años, la banca digital ha ganado terreno en Perú, impulsada por la necesidad de modernizar el sistema financiero y facilitar el acceso a servicios bancarios. No obstante, el país aún conserva rasgos de un mercado tradicional, donde una parte importante de la población no utiliza servicios financieros formales. Según cifras del Banco Central de Reserva del Perú (BCRP), en el 2022 el 70% de los usuarios del sistema financiero eran considerados no digitales, lo que refleja una baja adopción de servicios bancarios digitales.

A pesar de este panorama, las billeteras móviles han experimentado un crecimiento notable. De acuerdo al último Índice de Inclusión Financiera de Credicorp, la tenencia de billetera móvil en el país es de un 58%, superando a países como Chile y México. Este avance se debe en gran parte a soluciones como Yape, del Banco de Crédito del Perú (BCP), y Plin, desarrollada en conjunto por BBVA, Scotiabank e Interbank, que han simplificado las transferencias electrónicas mediante el uso de números telefónicos o códigos QR.

Por su parte, el gobierno peruano ha promovido iniciativas regulatorias para fomentar la innovación en el sector financiero y acelerar la inclusión. Como miembro de Better Than Cash Alliance, Perú ha asumido el compromiso de reducir el uso de efectivo, mejorar la transparencia en las transacciones y propiciar un crecimiento más equitativo mediante la digitalización de pagos.

“Las billeteras móviles han experimentado un crecimiento notable”

Ciberseguridad y gestión de riesgos: desafíos clave del ecosistema financiero

La transformación digital ha revolucionado el funcionamiento de las entidades financieras en Perú. Desde la banca móvil hasta los servicios en la nube y el auge de las fintech, las innovaciones tecnológicas han redefinido la experiencia del cliente. Sin embargo, estos avances también han ampliado la superficie de exposición a ciberamenazas, exigiendo medidas de protección más sofisticadas para resguardar la información y los recursos financieros.

Según un informe de ICEX, en 2022 se registraron más de 15 mil millones de intentos de ciberataques en el país, lo que representa un aumento del 35% respecto al año anterior. El sector financiero es uno de los más afectados, enfrentando amenazas como phishing, ransomware, DDoS y suplantación de identidad, lo que evidencia la urgencia de reforzar capacidades preventivas y reactivas desde las áreas de TI.

Los desafíos son múltiples. Muchas instituciones aún operan con infraestructuras legadas, que limitan la implementación de controles modernos y dificultan la integración con soluciones avanzadas de detección y respuesta. A esto se suma la fragmentación organizacional entre las áreas de TI, Seguridad y Cumplimiento, lo que obstaculiza una visión unificada del riesgo y reduce la capacidad de reacción ante incidentes críticos.

Además, la escasez de talento especializado en ciberseguridad complica aún más el panorama, donde el 67% de las empresas reporta dificultades para contratar perfiles técnicos en esta área. Como consecuencia, muchas entidades optan por tercerizar servicios o incorporar herramientas automatizadas, que a veces no cuentan con el gobierno de datos o la visibilidad necesaria para mantener un control efectivo.

Por otra parte, los marcos regulatorios también han evolucionado. La SBS en Perú, por ejemplo, emitió la Resolución N.° 504-2021, que exige a las entidades financieras contar con políticas integradas de seguridad, planes de continuidad operativa, monitoreo de vulnerabilidades y pruebas periódicas de ciberresiliencia. Estas exigencias demandan del área de Tecnología una capacidad real de gobernanza, orquestación y cumplimiento automatizado.

La digitalización de servicios y la implementación de modelos como open banking han multiplicado los puntos de contacto con los usuarios. Si bien esto mejora la experiencia general, también introduce nuevos riesgos asociados al uso de APIs abiertas, infraestructuras en la nube y la tercerización de servicios. En este contexto, la protección de datos y la integridad transaccional requieren un enfoque integral de seguridad desde el diseño (security by design).

El escenario actual exige que las instituciones financieras peruanas avancen hacia modelos de ciberresiliencia, integrando tecnología, talento, cultura y gobernanza. La ciberseguridad dejó de ser un área aislada, transformándose en una responsabilidad estratégica compartida que impacta directamente en la continuidad del negocio, la relación con los clientes y la competitividad del sistema.

El futuro del ecosistema financiero depende en gran parte de una combinación de tecnología, procesos, personas y gobernanza. Los líderes de TI deben evolucionar hacia arquitecturas zero trust, monitoreo continuo y modelos de defensa activa, integrando la seguridad como un pilar central del negocio.

“67% de las empresas reporta dificultades para contratar perfiles técnicos en esta área”

La transformación del sistema financiero en Chile: de la estabilidad a la innovación

En los últimos años, Chile ha avanzado con fuerza en la modernización de su sistema financiero. Con una banca sólida, marcos regulatorios que impulsan el desarrollo fintech y una decidida apuesta por las finanzas abiertas, el país se ha consolidado como referente en innovación y seguridad digital en la región.

Un hito clave fue la promulgación de la Ley N° 21.521, conocida como la "Ley Fintech", en enero de 2023. Esta legislación fomenta la competencia y la inclusión financiera mediante el uso de tecnología, y define un marco claro para el funcionamiento de las empresas del sector. También establece las bases para el Sistema de Finanzas Abiertas (SFA), que permitirá a los clientes autorizar el intercambio seguro de su información entre distintas entidades mediante APIs, otorgándoles mayor control sobre sus datos y acceso a servicios más personalizados.

La implementación del SFA se realizará de forma progresiva entre 2023 y 2028, según lo proyectado por la Comisión para el Mercado Financiero (CMF), facilitando una transición gradual y segura para las instituciones financieras, que deberán modernizar sus plataformas y reforzar sus sistemas de protección digital.

En este escenario, la ciberseguridad y el cumplimiento normativo adquieren una relevancia estratégica. Diversas entidades financieras en Chile han adoptado estándares como ISO/IEC 27001, reafirmando su compromiso con la protección de datos y la gestión de riesgos. A su vez, la Ley Fintech exige medidas concretas para garantizar la integridad y confidencialidad de la información, junto con políticas internas robustas y mecanismos de control.

Otro avance relevante ha sido la implementación de la facturación electrónica obligatoria desde 2014, que ha mejorado la transparencia y eficiencia de las transacciones, fortaleciendo la supervisión y reduciendo la evasión fiscal. Gracias a estos esfuerzos, Chile ha construido un entorno financiero más abierto, competitivo y resiliente, con una base sólida para seguir liderando la evolución digital en América Latina.

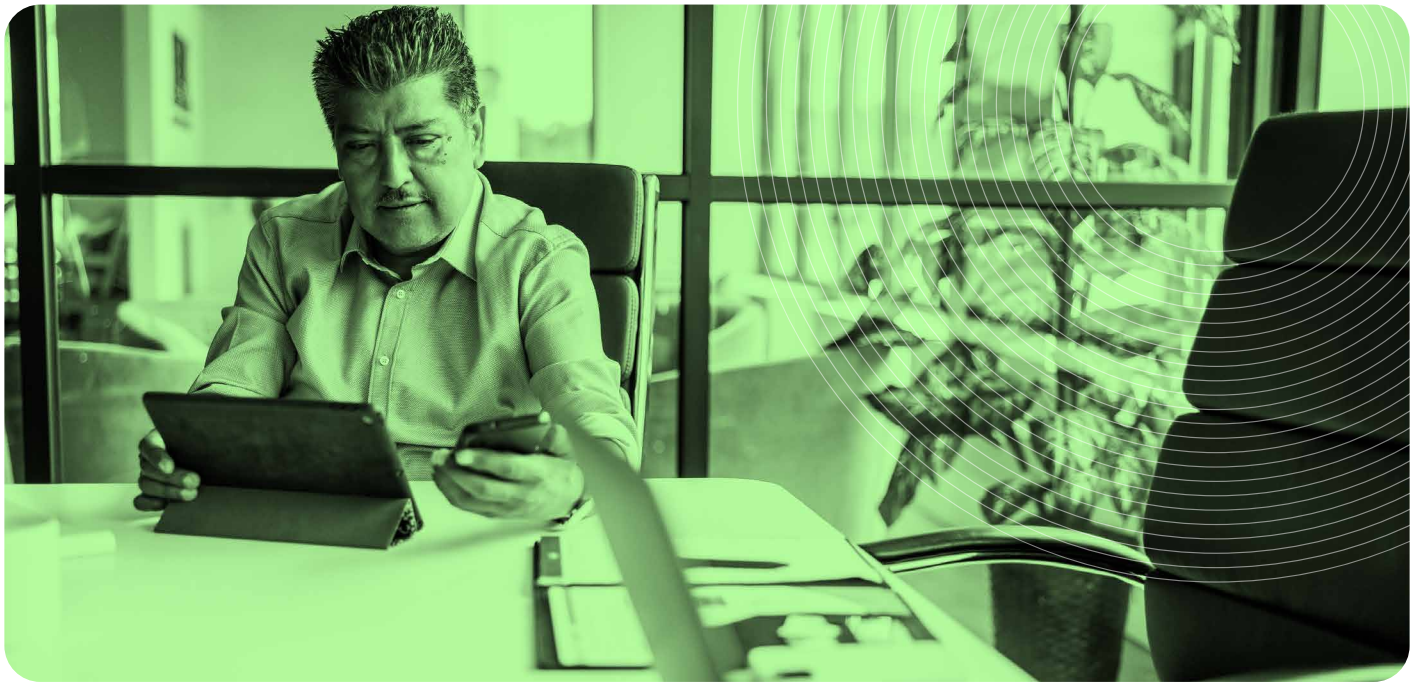
"Chile ha construido un entorno financiero más abierto, competitivo y resiliente"

Desafíos de la transformación digital de la industria financiera chilena

La modernización del sistema financiero chileno ha traído una serie de desafíos estructurales para los líderes de Tecnología e Innovación, que requieren visión estratégica, capacidad técnica y una arquitectura tecnológica adaptable.

Uno de los retos más relevantes es responder a las expectativas de un cliente totalmente digitalizado. Según BancoEstado, el 66% de sus transacciones fueron digitales a diciembre de 2024, lo que está forzando a las instituciones financieras a rediseñar sus canales de atención y servicios. Desde la perspectiva tecnológica, esto implica:

- Desarrollar infraestructuras escalables y redundantes para garantizar disponibilidad continua.
- Asegurar experiencias omnicanal sin fricciones, conectando sistemas legacy con nuevos front-ends.
- Implementar plataformas de autoservicio, autenticación biométrica y análisis de comportamiento en tiempo real.



En la actualidad, la integración omnicanal es una obligación técnica que no se puede evadir. Sin embargo, muchas instituciones aún operan con sistemas fragmentados, sin capacidad de interoperar con fintechs o habilitar flujos digitales de extremo a extremo. Para superarlo, los equipos de TI deben adoptar arquitecturas modulares, basadas en microservicios y APIs, que permitan flexibilidad sin comprometer la gobernabilidad ni la seguridad.

En paralelo, la ciberseguridad ha adquirido un protagonismo clave. La digitalización masiva ha incrementado los vectores de ataque, haciendo imprescindible invertir en tecnologías de protección de datos, detección de amenazas avanzadas y cumplimiento normativo automatizado. La Ley 21.521 establece principios de seguridad y responsabilidad en el tratamiento de datos, y muchas instituciones complementan esto mediante estándares internacionales como ISO 27001 o NIST, que son clave para adecuarse a las exigencias regulatorias y proteger los entornos digitales.

Otro reto persistente es la modernización de infraestructuras heredadas. Muchos bancos aún dependen de plataformas core rígidas que dificultan la innovación, generan altos costos de mantenimiento y no están preparadas para operar en modelos nativos en la nube. Migrar a arquitecturas modernas es una decisión tecnológica, pero también organizacional, ya que se requiere apoyo del directorio, gestión del cambio, talento especializado y una hoja de ruta clara.

“Las fintechs han actuado como catalizadores del cambio”

En este entorno, las fintechs han actuado como catalizadores del cambio, forzando a las instituciones tradicionales a repensar sus modelos y adoptar prácticas más ágiles. Muchas entidades han respondido creando laboratorios de innovación, alianzas estratégicas o incluso unidades tecnológicas propias. Para los CIOs, esto supone liderar iniciativas de innovación abierta, garantizar compatibilidad tecnológica y proteger la integridad de los datos compartidos.

Por último, la transformación digital no será completa sin una inclusión financiera verdaderamente equitativa. Aún persisten brechas importantes en zonas rurales o sectores con baja alfabetización digital. Esto plantea el desafío, desde TI, de diseñar soluciones accesibles, livianas y seguras, capaces de operar en condiciones de conectividad limitada, y con una usabilidad pensada para todo tipo de usuarios.

Principales oportunidades para la banca digital en México, Perú y Chile

La banca digital está abriendo un abanico de oportunidades para las instituciones financieras en Chile, Perú y México, no solo modificando la forma en que operan, sino también la manera en que se relacionan con sus clientes. Esta evolución permite generar nuevas posibilidades de negocio, así como desarrollar soluciones más accesibles y personalizadas para distintos segmentos de la población.

Una de las ventajas más relevantes es la inclusión financiera. La digitalización facilita que los servicios bancarios lleguen a zonas rurales y a personas tradicionalmente excluidas del sistema financiero. En muchos países de América Latina, una parte importante de la población aún no cuenta con acceso a productos bancarios formales. Gracias a las plataformas digitales, ahora pueden abrir cuentas, solicitar créditos o realizar pagos sin necesidad de desplazarse a una sucursal, lo que favorece su inclusión en el sistema económico formal y mejora su calidad de vida.

Además, la digitalización mejora la eficiencia operativa. La automatización de procesos contribuye a reducir costos, optimizar recursos y acelerar la entrega de servicios. Desde la atención al cliente hasta la aprobación de préstamos, las herramientas tecnológicas permiten respuestas más ágiles y con menor margen de error, elevando así la experiencia del usuario y reforzando la confiabilidad de los canales digitales.

Otro avance importante es la aparición de nuevos modelos de negocio impulsados por la banca abierta. Este enfoque promueve la colaboración entre bancos tradicionales y fintechs, generando productos más adaptados a las necesidades reales de los usuarios. Las fintechs aportan flexibilidad y velocidad en el desarrollo de servicios, mientras que los bancos ofrecen solidez y alcance. Juntos, logran crear ofertas más atractivas, ágiles y centradas en el cliente.

A su vez, la personalización de los servicios se ha convertido en una de las características más atractivas de la banca digital. A través del análisis de datos, las instituciones pueden entender los hábitos de consumo, ahorro y comportamiento financiero de cada persona, y diseñar productos que respondan a sus necesidades específicas. Esto representa un cambio importante respecto a los modelos tradicionales, donde se ofrecían soluciones estandarizadas para todos los clientes.

Por último, las plataformas digitales han permitido una expansión geográfica sin precedentes. Hoy es posible operar con servicios bancarios desde cualquier lugar, lo que resulta especialmente valioso en una región como América Latina, donde la movilidad entre países es habitual. Esta capacidad de brindar atención transfronteriza abre nuevas oportunidades comerciales, al tiempo que fortalece la presencia regional e internacional de las instituciones financieras.

Desafíos clave del sector financiero en México, Perú y Chile

Cumplimiento normativo: un equilibrio entre regulación e innovación

El cumplimiento normativo ya no es una tarea exclusiva de las áreas legales o de cumplimiento. Para los líderes de TI, se ha transformado en una función crítica que impacta directamente en la arquitectura tecnológica, la gestión de datos, los procesos internos y la capacidad de escalar con agilidad en entornos regulados.

El principal desafío es mantener el equilibrio entre la innovación tecnológica y el cumplimiento efectivo de regulaciones cada vez más estrictas. Un marco normativo mal gestionado desde TI puede obstaculizar la adopción de nuevas tecnologías, ralentizar los despliegues de productos y aumentar los costos operacionales. En cambio, una infraestructura compliance-ready, diseñada para adaptarse de forma flexible a nuevos requerimientos regulatorios, se convierte en una ventaja competitiva.

México: pionero regulatorio con desafíos técnicos pendientes

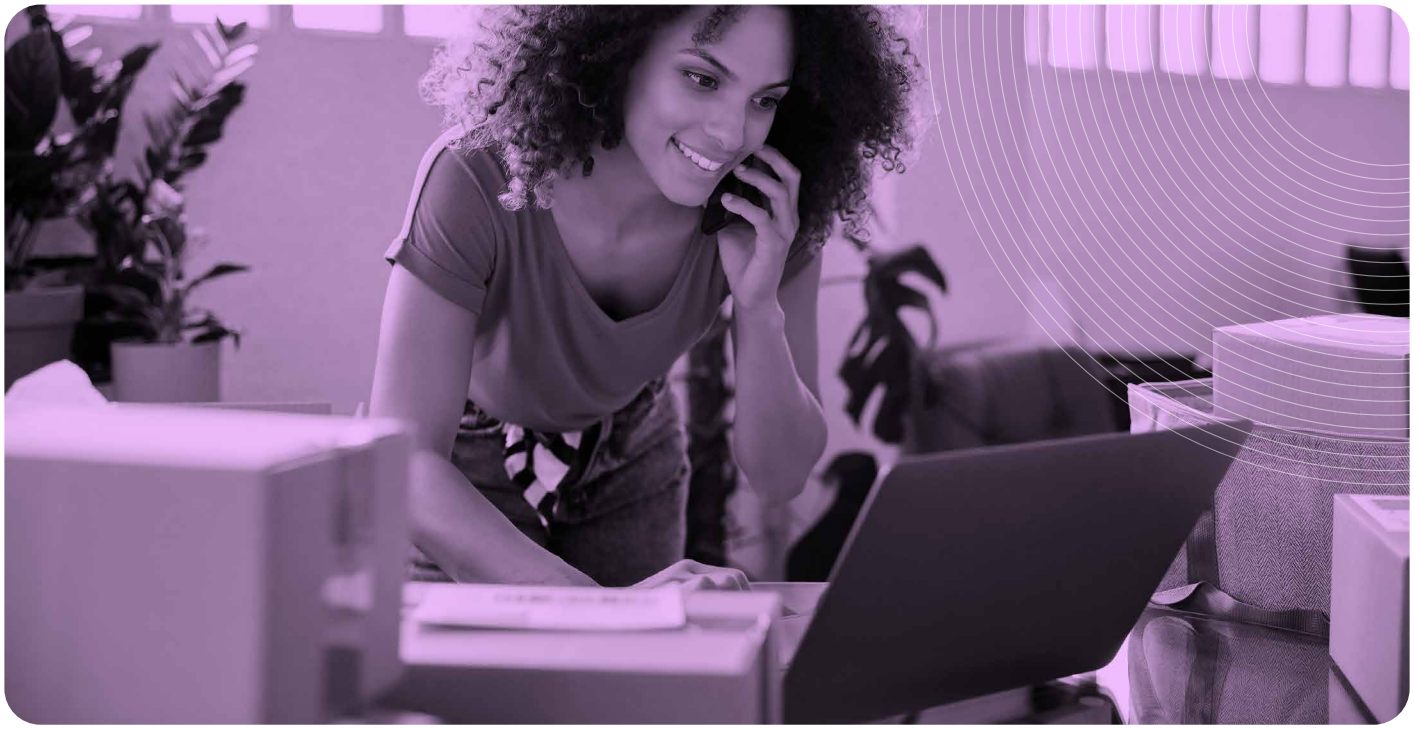
México lideró la región al promulgar en 2018 la Ley para Regular las Instituciones de Tecnología Financiera, conocida como Ley Fintech. Esta ley estableció requisitos claros para plataformas de pago electrónico, crowdfunding y banca abierta, incluyendo controles de capital, auditoría, ciberseguridad y protección al consumidor.

Desde la perspectiva de TI, se recomienda implementar prácticas como:

- Integraciones seguras mediante APIs estandarizadas.
- Arquitecturas que permitan trazabilidad, auditoría automatizada y control granular de datos.
- Sistemas de gestión de consentimiento alineados con el modelo de open banking.

Sin embargo, la implementación ha sido parcial. La ausencia de una regulación secundaria clara sobre datos transaccionales y datos agregados ha generado incertidumbre técnica en el diseño de soluciones alineadas con un ecosistema de finanzas abiertas. Para los CTOs y CIOs, esto implica trabajar con arquitecturas adaptables y monitorear activamente el desarrollo normativo para evitar retrabajos o riesgos de incumplimiento.

> **“Un marco normativo mal gestionado desde TI puede obstaculizar la adopción de nuevas tecnologías”**



Perú: avance segmentado con visión progresiva

Perú ha optado por una estrategia regulatoria gradual, con normas específicas para ciertos servicios fintech, pero sin una ley marco unificada. Aun así, ha desarrollado lineamientos técnicos relacionados con seguridad de la información, fintech, pagos digitales y finanzas abiertas.

Esto plantea para los equipos de TI el desafío de operar en un entorno normativo en evolución, en el que se esperan buenas prácticas como:

- Flexibilidad en la gestión de riesgos y en la integración con entornos externos.
- Capacidad para automatizar la trazabilidad de procesos regulados.
- Infraestructura adaptable para responder rápidamente a cambios en supervisión o fiscalización.

El Banco Central de Reserva del Perú y la SBS han dado señales claras de su interés en fortalecer la supervisión digital. Esto requiere que las instituciones preparen sus sistemas no solo para cumplir lo vigente, sino para anticiparse a futuras exigencias regulatorias en ámbitos como la protección de datos, autenticación biométrica, continuidad operativa y ciberseguridad.

Chile: un marco robusto que impulsa la transformación digital

La Ley 21.521 promulgada en Chile en 2023 posiciona al país como referente regional en regulación de servicios financieros digitales. Esta ley exige estándares altos en transparencia, seguridad, gobierno de datos y colaboración entre actores financieros a través de APIs y en el marco de las finanzas abiertas.

Desde el punto de vista tecnológico, se les sugiere a las instituciones:

- Integrar políticas de cumplimiento en los flujos de desarrollo (compliance by design).
- Gestionar infraestructuras que soporten monitoreo continuo, reportabilidad automatizada y auditoría en tiempo real.
- Asegurar que la protección de datos esté integrada de forma transversal en toda la arquitectura de sistemas.

El nuevo rol de la Comisión para el Mercado Financiero (CMF) como ente regulador con mayores atribuciones genera un entorno más exigente pero también más claro, en el que la adopción de estándares internacionales (como ISO 27001, NIST o GDPR) será clave para sostener la operación y garantizar confianza.

Innovar sin límites, regular con visión: el nuevo equilibrio del sistema financiero

México, Perú y Chile están trazando sus propios caminos en materia de regulación fintech. Y aunque sus marcos legales tienen matices distintos, todos convergen en un objetivo común: crear un entorno que inspire confianza, impulse la competencia y habilite la innovación con responsabilidad.

Las autoridades regulatorias han comprendido que, para que el ecosistema financiero evolucione, no basta con ejercer control: es necesario acompañar, habilitar y facilitar el cambio. Por eso están adoptando enfoques más flexibles que permiten el desarrollo de soluciones tecnológicas disruptivas, sin perder de vista la estabilidad del sistema.

La colaboración entre instituciones financieras, fintechs y reguladores será la clave para diseñar un sistema más inclusivo, dinámico y seguro. Un ecosistema donde competir e innovar no sea una disyuntiva, sino una sinergia.

Cómo las fintechs y los bancos están navegando el cumplimiento sin frenar la innovación

En un entorno cada vez más regulado, las fintechs y los bancos en Latinoamérica —especialmente en Chile, Perú y México— enfrentan el reto de ajustarse a marcos normativos estrictos sin perder su capacidad de innovar ni responder con agilidad a un mercado en constante evolución. La clave ha estado en sumar esfuerzos, adoptar tecnologías avanzadas y participar activamente en la definición del marco regulatorio.

Una de las estrategias más efectivas ha sido la colaboración entre fintechs y bancos tradicionales, que ha generado sinergias tecnológicas cada vez más sofisticadas. Mientras las fintechs aportan velocidad de desarrollo, modelos centrados en el usuario y estructuras tecnológicas nativas en la nube, los bancos ofrecen experiencia regulatoria, infraestructura robusta y gestión de riesgos consolidada. Para los CIOs, esto implica orquestar modelos de integración ágiles, con capas de seguridad, control de acceso, trazabilidad y compatibilidad con los sistemas core existentes.

Gracias a este tipo de cooperación, ha sido posible acelerar la llegada de productos y servicios innovadores sin comprometer la seguridad ni la confianza de los usuarios. Para la banca, significa una oportunidad de responder más rápido a las nuevas expectativas del mercado. Para las fintechs, representa una vía sostenible de c recimiento dentro del marco legal.

Otra estrategia relevante ha sido la incorporación de soluciones RegTech (Regulatory Technology), que automatizan tareas críticas como la supervisión de transacciones, la prevención de fraudes, el análisis de riesgos y la generación de reportes regulatorios. Estas herramientas permiten a los actores financieros reducir tiempos y costos, minimizar errores humanos y aumentar su capacidad de respuesta ante auditorías o requerimientos de las autoridades.

Para los líderes tecnológicos, las RegTechs representan una oportunidad estratégica: permiten reducir carga operativa, mitigar errores humanos y responder más rápidamente a cambios regulatorios sin rehacer procesos ni rediseñar arquitecturas.

Además, tanto bancos como fintechs han adoptado una postura más activa en el diseño del marco legal. A través de mesas técnicas, foros sectoriales y espacios de consulta pública, los líderes de innovación están colaborando con entes reguladores para crear normativas más realistas, seguras y compatibles con los desafíos tecnológicos actuales. Esta cooperación público-privada está permitiendo establecer reglas claras que habiliten la disrupción tecnológica sin comprometer la estabilidad, facilitando una evolución armónica del ecosistema.

En este nuevo modelo, el área de TI ya no es un soporte técnico: es el puente entre el cumplimiento regulatorio y la innovación de productos. Su función es garantizar que cada innovación —desde una aplicación móvil hasta un motor de scoring basado en inteligencia artificial— sea segura, auditable, trazable y conforme a la normativa vigente y futura.

Fraude financiero y los ciberataques en América Latina: una amenaza en expansión

El crecimiento del comercio electrónico, la adopción de servicios financieros digitales y la expansión del open banking han creado un entorno fértil para la sofisticación del fraude digital en América Latina. En este contexto, los líderes TI enfrentan el reto de anticiparse a amenazas que evolucionan más rápido que la infraestructura tradicional de seguridad.

México se encuentra en el epicentro de esta tormenta digital. Solo en el primer semestre de 2024, el país registró más de 31 mil millones de intentos de ciberataques, representando más del 50% de las amenazas cibernéticas reportadas en toda la región. Chile y Perú también presentan una tendencia al alza, con miles de millones de intentos anuales dirigidos contra bancos, fintechs y plataformas de pagos. El sector financiero es el más atacado y el que mayores pérdidas enfrenta por fraude y brechas de seguridad.

Uno de los métodos más utilizados es el phishing, que busca manipular a los usuarios para obtener sus credenciales. Actualmente existen múltiples variantes, como el smishing, a través de mensajes de texto, y el vishing, mediante llamadas telefónicas. En España, por ejemplo, una red de estafa telefónica logró engañar a más de 10.000 personas, con un botín total de 3 millones de euros.

Otro vector crítico es el malware bancario. Según un informe de BioCatch titulado "Tendencias del Fraude Bancario Digital en América Latina 2024", los fraudes digitales impulsados por malware aumentaron un 113% en los últimos 12 meses, provocando pérdidas millonarias.

Asimismo, los ransomware y los troyanos bancarios continúan ampliando su alcance en la región. México registra cinco ataques por minuto, mientras que en Chile se registraron más de 4 mil millones de intentos de ciberataques durante el 2023. En Perú el número de incidentes creció en un 15% en el último año, alcanzando un total de 33.788 casos reportados.

Finalmente, la suplantación de identidad (spoofing) se ha vuelto cada vez más habitual. En estos casos, los atacantes se hacen pasar por instituciones financieras legítimas para obtener información confidencial. Una de las técnicas más comunes es enviar mensajes que aparentan ser alertas oficiales sobre supuestas actividades sospechosas o errores en transacciones, con el objetivo de recolectar datos personales o claves de acceso.

"El sector financiero es el más atacado y el que mayores pérdidas enfrenta por fraude y brechas de seguridad"

Desde la perspectiva tecnológica, esto exige una estrategia de defensa activa y multidimensional, en donde se implementen arquitecturas de ciberseguridad avanzada, centradas en:

1. Detección y respuesta inteligente

- Integración de soluciones SIEM (Security Information and Event Management) y XDR (Extended Detection and Response) con capacidades de correlación de eventos en tiempo real.
- Implementación de algoritmos de IA para analizar patrones de comportamiento y detectar anomalías antes de que escalen.
- Modelos de machine learning entrenados para reconocer señales tempranas de fraude, incluso en operaciones legítimas.

2. Autenticación robusta y gestión de identidades

- Autenticación multifactor (MFA) y biometría (voz, rostro, huella) como estándar en todos los accesos críticos.
- Segmentación de privilegios y gestión de accesos basada en riesgos: RBAC (Role-Based Access Control) y ABAC (Attribute-Based Access Control).
- Gestión y gobierno de identidades digitales, especialmente en entornos de finanzas abiertas y banca distribuida.

3. Hardening y actualizaciones permanentes

- Aplicación de políticas de ciberhigiene estrictas: parches de seguridad, desactivación de puertos no utilizados, monitoreo continuo de endpoints.
- Auditorías de configuración periódicas y simulación de ataques (pentesting, red teaming).

4. Formación continua y cultura de seguridad

- Entrenamiento de equipos técnicos y no técnicos en detección de ataques sociales y respuesta ante incidentes.
- Campañas internas de concienciación orientadas a disminuir el “error humano”, aún responsable de gran parte de los accesos no autorizados.

5. Colaboración público-privada y threat intelligence

- Participación en mesas sectoriales y colaboración con CERTs o CSIRTs, entes regulatorios y proveedores de tecnología.
- Adopción de servicios de threat intelligence para anticiparse a campañas masivas dirigidas al sector.

Ciberseguridad e innovación: dos caras de la misma estrategia

Durante años, la ciberseguridad fue un tema confinado al ámbito técnico: firewalls, servidores, segmentación de redes y controles internos. Sin embargo, en la industria financiera (donde los datos personales, transaccionales y regulatorios son activos estratégicos) esta visión ha evolucionado. Actualmente, la seguridad se ha convertido en un eje transversal que permite innovar sin poner en riesgo la continuidad del negocio ni el cumplimiento normativo.

Para los líderes de Tecnología e Innovación, esto representa una oportunidad y una responsabilidad, porque la transformación digital en banca, seguros y fintechs no se trata solo de lanzar nuevas funcionalidades, sino de asegurar que cada interacción digital sea segura, trazable y resiliente frente a ciberamenazas que evolucionan a la misma velocidad que los servicios digitales.

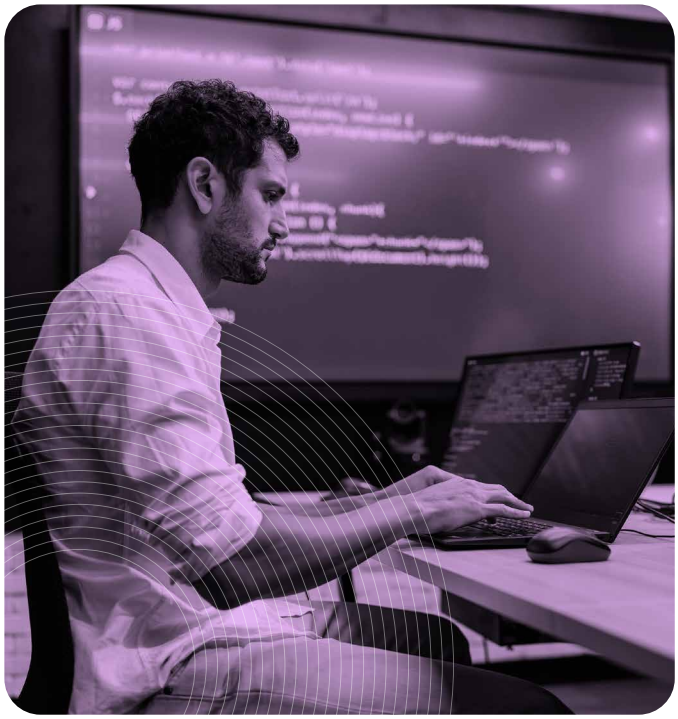
En este escenario, integrar la ciberseguridad desde el diseño (security by design), adoptar marcos de trabajo como Zero Trust, y asegurar la interoperabilidad de plataformas bajo estándares internacionales como PCI-DSS, ISO 27001 o conforme a los lineamientos regulatorios locales de entidades como la SBS (Perú), CNBV (México) o CMF (Chile) representa el camino más sólido y confiable para escalar operaciones de manera segura y sostenible.

Riesgos en un ecosistema hiperconectado

El sector financiero depende cada vez más de una arquitectura abierta: aplicaciones móviles, APIs para Open Banking, integraciones con fintechs, portales de autoservicio, onboarding 100% digital y canales transaccionales en tiempo real. Este ecosistema digital expone múltiples superficies de ataque que deben ser gestionadas con visión anticipatoria.

Un incidente de seguridad no solo interrumpe operaciones críticas: puede detener la originación de créditos, bloquear temporalmente cuentas de clientes, exponer datos confidenciales o desacreditar a una institución ante organismos reguladores. En contextos donde la confianza del usuario y la estabilidad operativa son pilares del negocio, cada brecha representa una amenaza real para la reputación, la continuidad y la ventaja competitiva.

La ciberseguridad no debe abordarse como un freno a la innovación, sino como el habilitador clave para sostener el crecimiento digital con gobernanza, eficiencia y cumplimiento.



Tres prioridades para los líderes de Tecnología e Innovación

Los equipos de Tecnología e Innovación están en una posición privilegiada para liderar la agenda de seguridad, no solo desde lo técnico, sino como parte del diseño estratégico del negocio. Estas son tres áreas críticas donde su liderazgo es determinante:

1. **Identificar y proteger los puntos críticos de información.** En instituciones financieras, los datos sensibles se procesan en múltiples entornos:
   - Plataformas de onboarding y validación de identidad
   - Módulos de scoring y motores de riesgo
   - Aplicaciones móviles y canales web
   - Servicios integrados vía APIs
   - Sistemas core bancarios y aseguradoras

Mapear dónde se almacenan, procesan o transfieren estos datos permite implementar controles proactivos, segmentar accesos y anticipar vulnerabilidades antes de que se conviertan en brechas.

2. **Evaluar y fortalecer las herramientas digitales con criterios de seguridad:** Las soluciones tecnológicas que impulsan la experiencia del cliente (como chatbots, biometría, apps móviles, autenticación sin fricciones y automatización de decisiones) deben ser evaluadas con una mirada de seguridad integral. Es indispensable:
   - Validar la seguridad de las integraciones con terceros (fintechs, partners, BaaS)
   - Mantener actualizados los enfoques de desarrollo seguro como DevSecOps
   - Auditar el ciclo de vida de APIs, SDKs y aplicaciones en producción
   - Aplicar pruebas de penetración periódicas y controles de acceso granulares

Los líderes de estas áreas deben garantizar que cada innovación esté acompañada de mecanismos de control que reduzcan la exposición al riesgo, sin comprometer la velocidad operativa ni la experiencia del usuario.

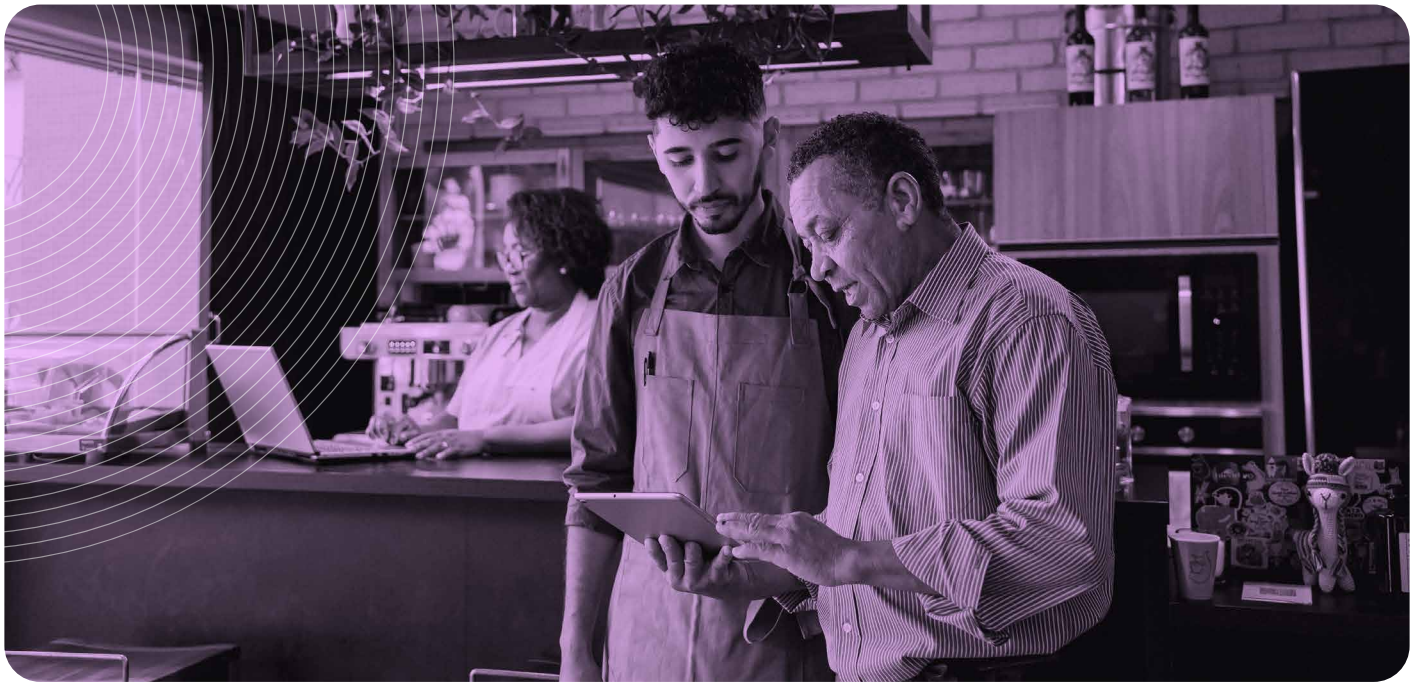
3. **Impulsar una cultura de ciberseguridad transversal:** La cultura de seguridad no es responsabilidad exclusiva del área de compliance o TI. Los líderes TI tienen un rol clave en difundir buenas prácticas, establecer procesos de respuesta y automatizar controles en toda la organización. Esto implica:
   - Implementar autenticación multifactor y control de sesiones
   - Sensibilizar a equipos internos frente a riesgos de ingeniería social o phishing
   - Automatizar alertas y monitoreo ante comportamientos anómalos
   - Establecer protocolos de respuesta ante incidentes con roles definidos

La seguridad es efectiva sólo cuando toda la empresa la asume como responsabilidad compartida. Formar equipos conscientes de la importancia de proteger los datos es tan relevante como contar con la infraestructura adecuada para hacerlo.

Seguridad como habilitador del crecimiento financiero

Las instituciones financieras que integran la ciberseguridad desde la estrategia tecnológica no solo cumplen con los marcos regulatorios: se posicionan como líderes en confianza digital. En un mercado donde los usuarios valoran la transparencia, el control de sus datos y la experiencia sin fricciones, la seguridad se convierte en un diferenciador competitivo.

Para los líderes TI, esto significa diseñar soluciones que combinen velocidad, escalabilidad y cumplimiento, además de tener un rol activo en la toma de decisiones estratégicas, alineando la arquitectura tecnológica con las metas comerciales.



Eficiencia operativa e innovación: el nuevo mandato tecnológico en la banca

La banca está atravesando un punto de inflexión. La digitalización ya no es una promesa: es un requisito operativo, estratégico y competitivo. Los líderes de TI e Innovación enfrentan una doble presión: escalar capacidades digitales para responder a clientes más exigentes y, al mismo tiempo, modernizar arquitecturas tecnológicas que fueron diseñadas para un mundo que ya no existe.

La realidad es que muchas instituciones financieras aún operan sobre modelos rígidos, sistemas heredados y procesos que requieren intervención manual en etapas críticas como apertura de cuentas, originación de créditos o resolución de reclamos. Esto no sólo ralentiza las operaciones: compromete la experiencia del cliente y eleva los costos estructurales en un entorno donde la eficiencia se ha vuelto un diferenciador clave.

Mientras tanto, el benchmark ha cambiado. Los usuarios ya no comparan su banco con otros bancos, sino con la inmediatez de una app de delivery, la personalización de una tienda online o la simplicidad de una fintech. Para competir en este nuevo escenario, la banca necesita transformarse internamente, con una visión centrada en tecnología ágil, automatización y analítica avanzada.

> **“Muchas instituciones financieras aún operan sobre modelos rígidos, sistemas heredados y procesos que requieren intervención manual”**

Automatización inteligente: la base de una banca eficiente

La automatización de procesos dejó de ser una tendencia para transformarse en una vía crítica de evolución. Tecnologías como la Automatización Robótica de Procesos (RPA, por sus siglas en inglés) permiten digitalizar tareas repetitivas y transaccionales (validación de documentos, ingreso de datos, conciliación de cuentas, actualización de registros) reduciendo errores, tiempos y costos operativos.

Para los líderes TI, esto implica la posibilidad concreta de:

- Liberar talento humano para funciones de mayor valor estratégico.
- Reducir los cuellos de botella operativos sin intervenciones estructurales mayores en los sistemas core.
- Crear flujos escalables que se adapten rápidamente a cambios regulatorios o de mercado.

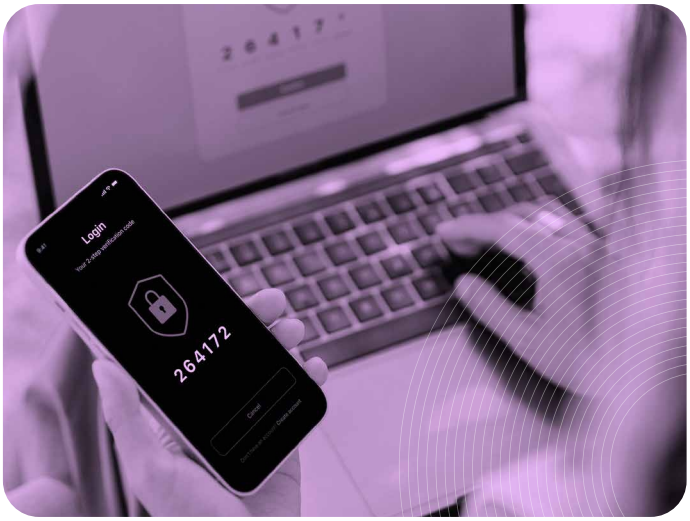
Más allá de la eficiencia, la automatización también habilita una infraestructura más resiliente y flexible, esencial para bancos que operan en múltiples regiones o atienden segmentos con necesidades diversas.

Inteligencia artificial y analítica: decisiones en tiempo real

Junto con la automatización, la inteligencia artificial (IA) y la analítica avanzada permiten aumentar la eficiencia operativa. Estas tecnologías no solo analizan grandes volúmenes de datos, sino que facilitan detectar patrones, anticipar comportamientos y ejecutar acciones precisas en el momento adecuado.

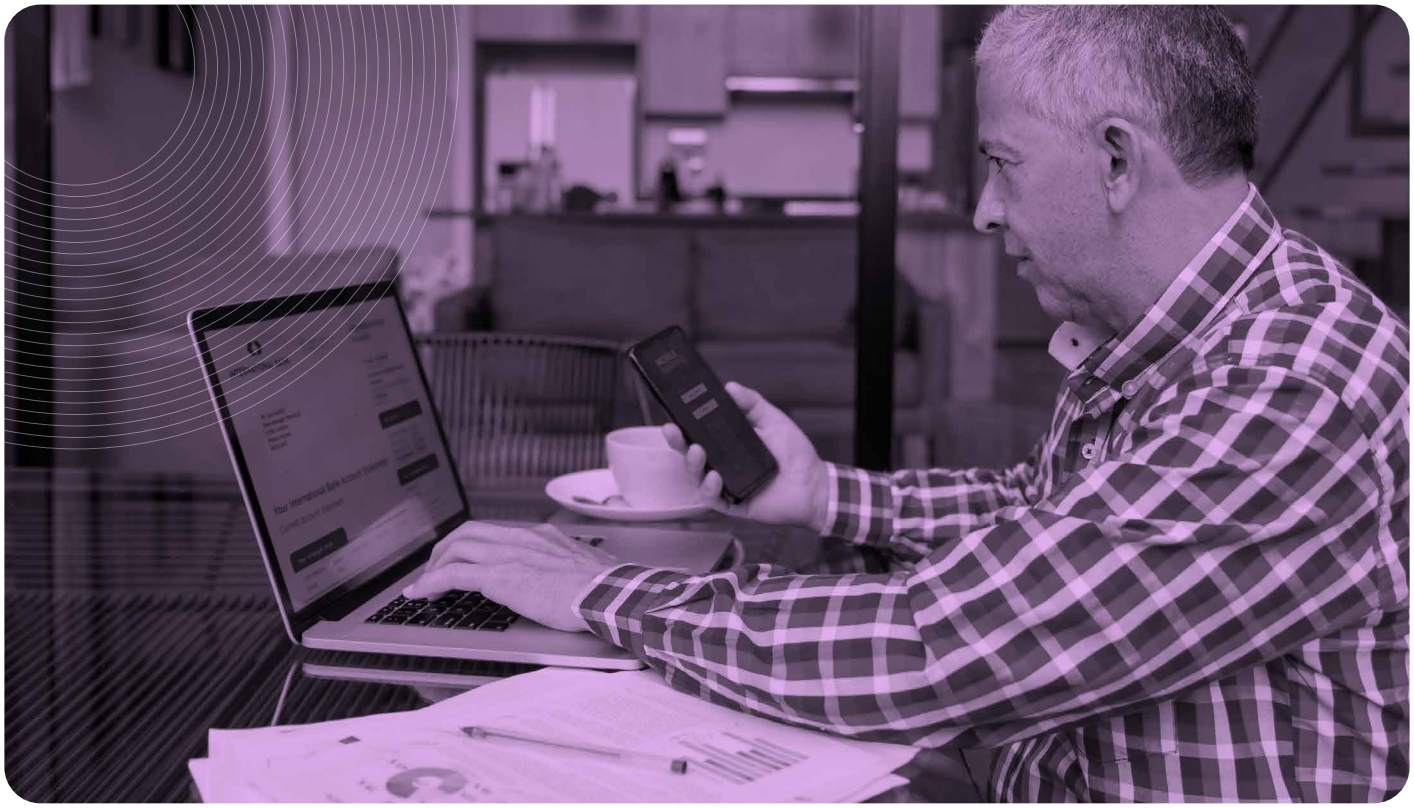
Para los líderes tecnológicos financieros, existen una serie de aplicaciones clave:

- **Prevención de fraudes:** detección temprana de operaciones inusuales en canales digitales.
- **Gestión de riesgo crediticio:** evaluación dinámica de la solvencia de clientes y escenarios de impago.
- **Personalización de servicios:** integración con CRM para activar ofertas o recomendaciones según el comportamiento del usuario.
- **Optimización comercial:** emisión de alertas automáticas cuando se detectan señales de abandono o desinterés del cliente.



> **“La automatización también habilita una infraestructura más resiliente y flexible”**

Estas capacidades no solo mejoran la operación diaria. También fortalecen el posicionamiento de la institución al ofrecer una experiencia más inteligente, contextual y adaptada a las necesidades reales de cada cliente.



Modernización tecnológica: más que sistemas, una visión

Uno de los principales desafíos que enfrentan los líderes tecnológicos es romper con la dependencia de sistemas legados que dificultan la integración con herramientas modernas, aumentan los costos de mantenimiento y ralentizan la evolución del negocio.

La modernización no se trata solo de migrar a la nube o renovar infraestructura. Se trata de repensar el modelo tecnológico con base en criterios como:

- Interoperabilidad y escalabilidad regional
- Cumplimiento normativo automatizado (SBS, CNBV, CMF)
- Diseño modular y adaptable a nuevas regulaciones
- Seguridad y trazabilidad en entornos digitales

Adoptar arquitecturas flexibles y basadas en microservicios o APIs abiertas, por ejemplo, permite incorporar nuevas funcionalidades sin afectar la operación central, acelerar pruebas de concepto y responder de manera más ágil a las demandas del negocio.

Tecnología como acelerador del negocio financiero

Las decisiones que se toman desde Tecnología no solo afectan al backoffice, sino que además impactan directamente la relación con el cliente. Un sistema ágil y automatizado permite ofrecer experiencias más fluidas, reducir tiempos de respuesta y fortalecer la confianza digital, especialmente en segmentos como banca corporativa, inversión, seguros o pagos.

Por eso, la transformación se ha vuelto ineludible. En un contexto económico complejo, con nuevas amenazas competitivas y presiones regulatorias crecientes, las instituciones que se atrevan a innovar desde sus cimientos tecnológicos serán las que lideren el nuevo ciclo de crecimiento.

La clave no está en sumar tecnologías de forma aislada, sino en diseñar un ecosistema inteligente donde automatización, IA, analítica y modernización trabajen de forma integrada. Esa es la misión del líder de Tecnología e Innovación: orquestar el cambio, anticipar tendencias y garantizar que la infraestructura digital esté estratégicamente alineada con los objetivos estratégicos del negocio.

“En América Latina, la adopción del modelo de Open Banking avanza a diferentes ritmos”

Fintech y banca tradicional: cooperación tecnológica para transformar el sistema financiero

En la última década, el panorama financiero en América Latina ha sido transformado por la irrupción de las fintech: empresas nativas digitales que ofrecen productos financieros más ágiles, accesibles y centrados en la experiencia del usuario. Su aparición no solo alteró las expectativas de los consumidores, sino que también desafió la lógica operativa de la banca tradicional.

Hoy, los usuarios esperan abrir una cuenta en minutos desde el celular, recibir atención inmediata sin trámites presenciales, y acceder a productos personalizados y transparentes. Este estándar —marcado por la innovación— ha obligado a los bancos a acelerar su modernización y repensar su arquitectura tecnológica.

Para los equipos de TI, este nuevo entorno representa tanto una amenaza como una oportunidad. La clave está en entender que el futuro del sistema financiero no se juega en la rivalidad, sino en la interoperabilidad y colaboración estratégica.

Open Banking: habilitador clave para un ecosistema integrado

En América Latina, la adopción del modelo de Open Banking avanza a diferentes ritmos: México cuenta con un marco regulatorio definido desde la Ley Fintech; Chile y Perú han iniciado procesos de consulta y normativas preliminares que buscan fomentar este enfoque colaborativo.

A pesar de lo anterior, se ha convertido en uno de los mecanismos más potentes de cooperación entre bancos y fintechs. A través de APIs seguras y estandarizadas, las instituciones tradicionales pueden habilitar el desarrollo de soluciones complementarias, creando un entorno más flexible y competitivo.

Para el área tecnológica, esta alianza implica:

- Diseñar arquitecturas abiertas y modulares que permitan una integración segura con terceros.
- Cumplir con regulaciones específicas sobre protección de datos y consentimiento (como las normativas de CMF en Chile, SBS en Perú o CNBV en México).
- Establecer marcos de seguridad robustos que garanticen la trazabilidad y el control de los datos compartidos.
- Adoptar enfoques API-first y compliance-ready desde el diseño de nuevos servicios digitales.

Para el usuario final, esto se traduce en experiencias financieras más simples, centralizadas y personalizadas. Para el banco, representa la posibilidad de ampliar su propuesta de valor sin necesidad de desarrollar todo desde cero.

Colaborar para escalar: velocidad, innovación y resiliencia

Las fintech destacan por su agilidad y capacidad de iterar rápidamente. Los bancos, por su parte, aportan experiencia en gestión de riesgos, cumplimiento y operación en escala. Cuando ambos actores colaboran bajo una visión compartida, se logran beneficios concretos:

- Validación rápida de soluciones mediante pilotos o sandbox regulados.
- Acceso a nuevos segmentos de mercado, especialmente a través de productos de nicho o modelos BaaS (Banking as a Service).
- Reducción del time-to-market, sin comprometer la seguridad o la gobernanza.

Desde la perspectiva tecnológica, se requiere una cultura organizacional que permita la experimentación sin comprometer los sistemas críticos, que fomente la interoperabilidad y que adopte modelos de cocreación tecnológica.

Incluso los entes reguladores están promoviendo espacios de colaboración como sandboxes o programas de innovación supervisada, que permiten validar nuevas propuestas en entornos controlados.

En ese sentido, la transformación del sistema financiero ya no depende únicamente del desarrollo interno de capacidades, sino de la articulación de ecosistemas, la integración de plataformas, la orquestación de datos y la garantía de estándares comunes entre actores diversos.

El líder de Tecnología e Innovación juega hoy un rol estratégico, en donde resulta clave la anticipación a los cambios. Explorar alianzas con fintechs, impulsar entornos de desarrollo abierto y facilitar la integración de terceros de forma segura son tareas que inciden directamente en la competitividad futura de la institución.

En ese sentido, el desafío no está en elegir entre competir o colaborar. El verdadero reto es construir infraestructuras que permitan ambas cosas: proteger lo que ya funciona, mientras se abren las puertas a lo que aún está por crearse.

“El líder de Tecnología e Innovación juega hoy un rol estratégico, en donde resulta clave la anticipación a los cambios”

El futuro del sector financiero en América Latina

La inclusión financiera ha crecido con fuerza en América Latina. Según el Global Findex 2021 del Banco Mundial, el 73% de la población adulta en la región poseía una cuenta en una institución financiera o con un proveedor de dinero móvil, lo que evidencia un avance significativo en bancarización, impulsado en gran parte por el crecimiento de las fintech, que han desarrollado soluciones digitales que amplían el acceso a los servicios financieros.

Sin embargo, persisten desafíos importantes. Aunque la adopción de pagos digitales ha aumentado, su uso aún no está completamente extendido. Además, muchas personas siguen sin acceder a métodos de ahorro formales. Estos desafíos muestran que la inclusión financiera total sigue siendo una meta por alcanzar.

La pandemia aceleró el uso de herramientas digitales, llevando a muchas personas a interactuar por primera vez con servicios financieros en línea. Este cambio marcó el inicio de una transformación más profunda: tecnologías como la inteligencia artificial (IA), el big data, el open finance y el machine learning están revolucionando la forma en que las instituciones financieras se relacionan con sus clientes.

¿Cómo enfrentar estos desafíos sin frenar el crecimiento?

Para avanzar en la transformación digital del sector financiero, es clave reforzar algunas áreas estratégicas.

La primera es la educación. Muchas personas aún no saben cómo utilizar los servicios digitales disponibles. Fortalecer la educación financiera y digital puede ser decisivo para aumentar su adopción. De hecho, informes como el del Banco Interamericano de Desarrollo destacan una brecha significativa en este ámbito.

En segundo lugar, es fundamental mejorar la infraestructura tecnológica. Sin una base robusta, escalable, confiable y segura, no se genera la confianza necesaria en las plataformas digitales. La inversión en tecnología debe ir de la mano con garantías de seguridad y disponibilidad.

Otro elemento clave es la regulación. Los marcos normativos deben equilibrar la innovación con la protección de los usuarios. Iniciativas como la Ley Fintech promulgada en Chile en 2023 marcan un precedente, al promover la competencia y establecer reglas claras.

Finalmente, la cooperación entre el sector público y el privado es esencial. Cuando el Estado, los entes reguladores y las empresas alinean sus esfuerzos, es posible construir soluciones eficaces que promuevan la inclusión financiera. Un ejemplo de ello es el impulso del ecosistema fintech en países como México.

Tendencias que marcarán el rumbo del sector

Mirando hacia el futuro, hay varias tendencias que seguirán transformando el sector financiero en la región.

La inteligencia artificial y la automatización están revolucionando la forma en que las instituciones gestionan sus procesos e interactúan con los clientes. Muchas de ellas están adoptando soluciones de código abierto y algoritmos inteligentes para optimizar operaciones y fomentar la inclusión financiera.

Las finanzas abiertas (open finance) también están ganando terreno. Permiten que los usuarios compartan su información financiera entre distintas entidades, lo que facilita el diseño de productos personalizados y les da mayor control sobre sus datos. Esta tendencia ya muestra impactos concretos en países como Brasil y México.

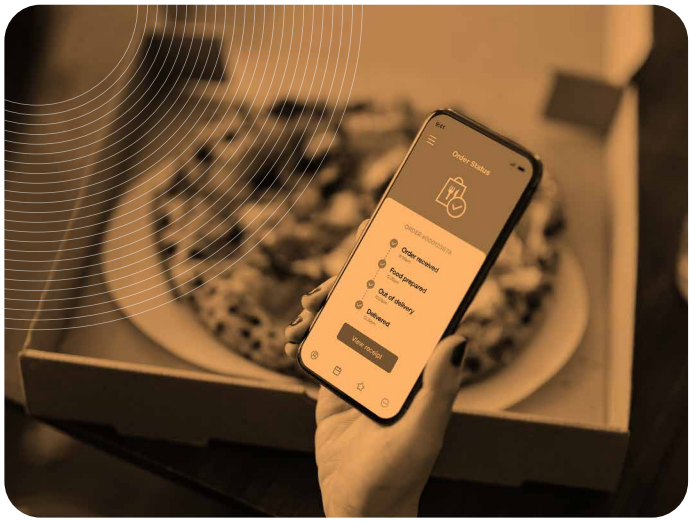
La regulación tecnológica se perfila como una prioridad para los reguladores y actores del sistema financiero. Con la creciente digitalización del sector, temas como la resiliencia operativa y el cumplimiento normativo tomarán mayor protagonismo, exigiendo a las instituciones adecuarse en aspectos como la arquitectura tecnológica y la protección de datos.

En ese contexto, la ciberseguridad es indispensable. A medida que aumentan los servicios digitales, proteger los datos de los clientes y garantizar el cumplimiento regulatorio resulta fundamental para mantener la confianza y evitar sanciones.

Este es el momento para que las instituciones financieras de América Latina refuercen su compromiso con la innovación, sin dejar de lado la inclusión y la seguridad. La tecnología no es solo una herramienta, sino un motor que puede transformar el acceso al sistema financiero, haciéndolo más justo, eficiente y preparado para el futuro.

> **“Temas como la resiliencia operativa y el cumplimiento normativo tomarán mayor protagonismo”**

Optimización, seguridad y cumplimiento: tres pilares que definen la agenda tecnológica



La evolución del liderazgo tecnológico en la industria financiera latinoamericana

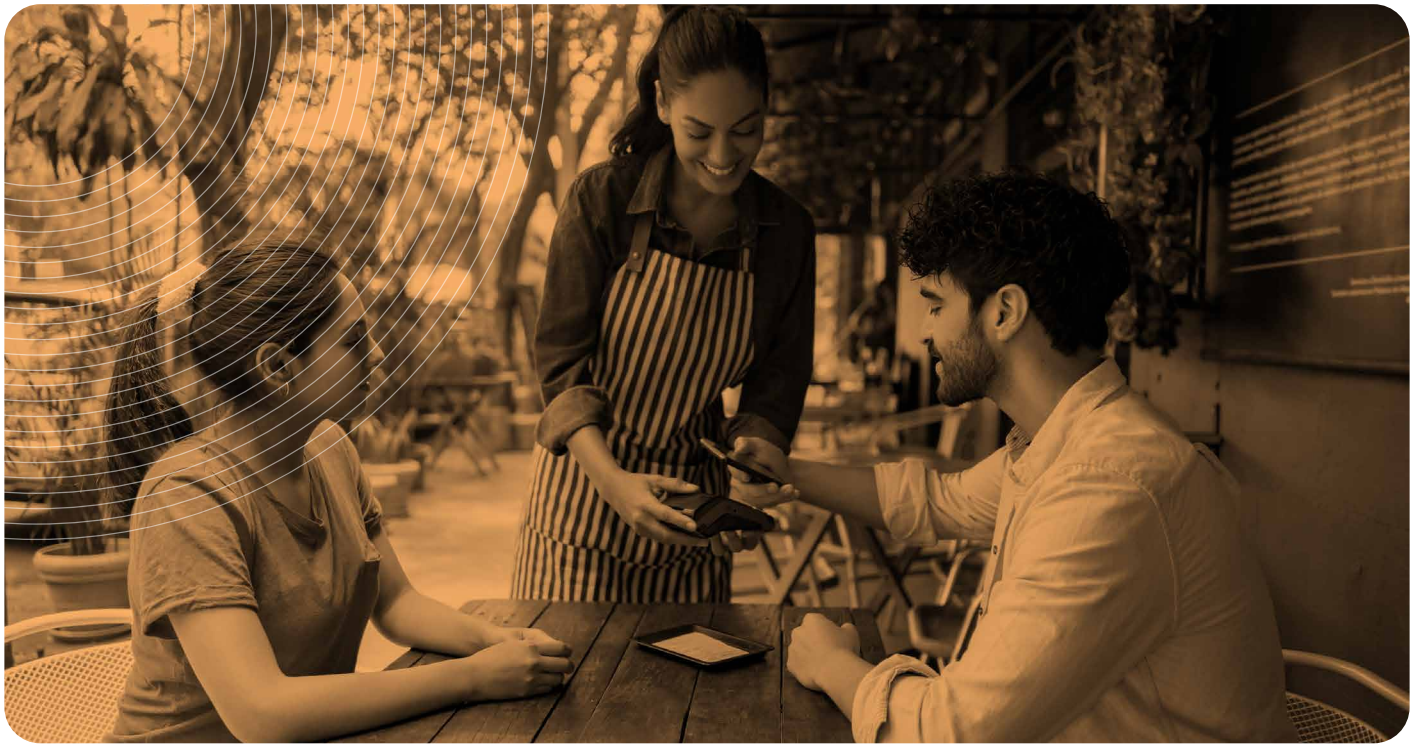
Históricamente, el liderazgo en la industria financiera se centraba en alcanzar metas comerciales a través de la captación y retención de clientes. Sin embargo, en el contexto actual de transformación digital, el auge de las fintech y el incremento de amenazas cibernéticas, el concepto de liderazgo ha evolucionado hacia una visión estratégica transversal y multifuncional.

Para los líderes TI, este cambio implica dejar de ver la tecnología como una simple herramienta de soporte y posicionarla como el motor estratégico que articula eficiencia operativa, seguridad y cumplimiento normativo. Ahora la competitividad se fundamenta en la capacidad de diseñar arquitecturas seguras y ágiles que potencien tanto la experiencia del cliente como la resiliencia del negocio.

Según el Global Cybersecurity Leadership Insights Study, el 62% de las empresas latinoamericanas reconoce haber sufrido filtración de datos, lo que pone de manifiesto la vulnerabilidad de los entornos digitales. Este dato reafirma la urgencia de que los líderes tecnológicos implementen estrategias que integren:

- **Gestión de riesgos:** incorporación de soluciones de ciberseguridad robustas y protocolos de respuesta ante incidentes.
- **Cumplimiento normativo:** adaptación a los marcos regulatorios locales e internacionales (por ejemplo, SBS en Perú, CNBV en México, CMF en Chile) para mitigar riesgos y evitar sanciones.
- **Innovación continua:** utilización de tecnologías emergentes como inteligencia artificial, automatización y análisis de datos para anticipar amenazas y personalizar la experiencia del cliente.

Estos desafíos no solo afectan la seguridad, sino que también condicionan la percepción de la marca y la confianza de los clientes en un mercado altamente competitivo.



El nuevo perfil del líder tecnológico: competencias y sinergias

Como consecuencia de lo antes expuesto, el liderazgo en el ámbito tecnológico ya no se limita a habilidades técnicas aisladas. Hoy se requiere un perfil transversal que combine:

- **Visión estratégica de negocio:** Comprender cómo la innovación tecnológica puede impulsar ventajas competitivas y transformar la relación con los clientes.
- **Conocimiento normativo y de seguridad:** Integrar la protección de datos y el cumplimiento en el diseño de soluciones digitales, evitando que incidentes de seguridad afecten la reputación institucional.
- **Dominio de herramientas digitales:** Implementar sistemas basados en inteligencia artificial, automatización y analítica para anticipar tendencias y optimizar la toma de decisiones.

Este perfil es clave para consolidar una infraestructura resiliente y un ecosistema digital que soporte tanto el crecimiento como la sostenibilidad del negocio. Sin embargo, el éxito en la transformación digital ya no depende únicamente del área de TI, sino de la capacidad para trabajar en conjunto con áreas comerciales, legales y de compliance.

En este contexto, el rol del líder de Tecnología e Innovación es el de:

- Orquestar iniciativas que integren las necesidades del negocio con los requerimientos de seguridad y cumplimiento.
- Facilitar la colaboración entre equipos para asegurar que cada nueva solución digital mejore la experiencia del cliente, garantizando al mismo tiempo altos estándares de seguridad.
- Anticipar y gestionar riesgos de manera proactiva, estableciendo sistemas de monitoreo y respuesta ante incidentes.

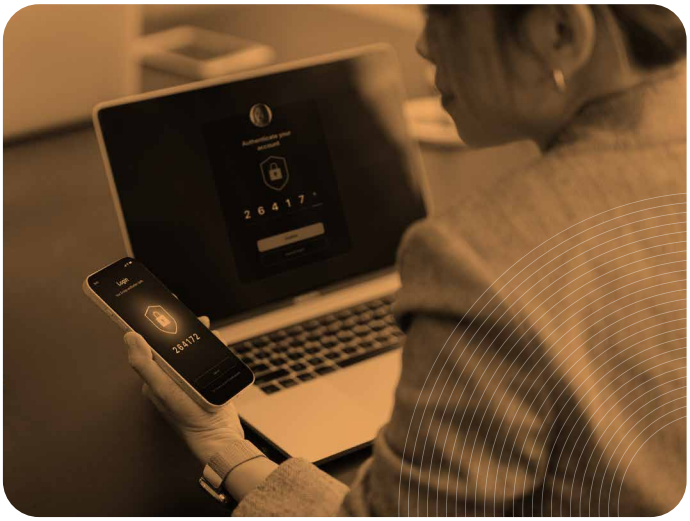
Esta colaboración multidisciplinaria es esencial para evitar crisis reputacionales y consolidar relaciones sólidas en el mercado. Después de todo, el liderazgo tecnológico actual trasciende lo meramente operacional; se trata de transformar toda la estructura organizacional para enfrentar los desafíos de un mercado en constante cambio. Integrar la gestión de riesgos, la ciberseguridad y el cumplimiento regulatorio en la estrategia digital no solo protege a la institución frente a amenazas, sino que también constituye una ventaja competitiva duradera.

Onboarding digital: el nuevo frente de innovación y eficiencia

Mientras las fintech avanzan con agilidad operativa, las instituciones financieras tradicionales enfrentan un desafío estructural: modernizar sus procesos de incorporación de clientes sin comprometer la seguridad, el cumplimiento ni la experiencia del usuario.

El onboarding es hoy un punto de fricción clave. Según The State of Intelligent Automation Report, el sector financiero lidera la tasa de abandono de clientes durante esta etapa, con un 23%. Las principales causas: procesos lentos, repetitivos y carentes de automatización. Un tercio de los usuarios encuestados menciona la complejidad del proceso como el mayor problema, seguido por los controles de identidad y la intervención manual.

Desde la perspectiva de tecnología e innovación, estos desafíos exigen respuestas estructurales. No se trata solo de optimizar la interfaz de usuario, sino de redefinir el journey digital desde su raíz, integrando soluciones que permitan escalar la operación sin perder trazabilidad ni control regulatorio.



"El impacto real depende de la alineación entre equipos, procesos y cultura organizacional"

El rol de la verificación digital: agilidad con cumplimiento

Organismos reguladores como la CNBV (México), SBS (Perú) y la CMF (Chile) han avanzado en marcos normativos que permiten y exigen digitalizar procesos de validación de identidad, siempre que se garantice la autenticidad, integridad y resguardo de la información.

En este contexto, tecnologías como:

- Biometría facial o dactilar
- OCR para lectura automática de documentos
- Análisis de datos en tiempo real
- IA para detección de fraude
- Plataformas de firma electrónica certificada

no solo agilizan el onboarding: lo blindan ante auditorías y fortalecen la trazabilidad, lo que es crítico para cumplir con normas locales e internacionales como Ley Fintech (México), Ley de Protección de Datos Personales (Perú) o la Ley 19.628 (Chile).

Además, la automatización del proceso de incorporación puede integrarse vía API-first architectures, facilitando su adopción progresiva sin afectar los sistemas core existentes. Esto permite reducir los tiempos de implementación, contener costos de mantenimiento y facilitar el escalado regional.

Sin embargo, la tecnología por sí sola no garantiza el éxito. Su impacto real depende de la alineación entre equipos, procesos y cultura organizacional. La experiencia demuestra que los proyectos de transformación digital fallan no por falta de herramientas, sino por silos internos, resistencia al cambio y falta de visión transversal.

El rol de los equipos de TI es ser articuladores de esta transformación, anticipándose a las tendencias regulatorias, construyendo puentes entre TI, áreas comerciales y legales, y diseñando procesos donde el cliente y la eficiencia operativa convivan con la seguridad y el cumplimiento.

Cumplimiento normativo: ¿obstáculo o ventaja competitiva para la innovación?

Para los líderes de Tecnología en la industria financiera latinoamericana, el cumplimiento regulatorio ya no es un tema ajeno o exclusivo del área legal. Normativas como KYC, AML, FATCA o las exigencias de los entes locales (CMF en Chile, SBS en Perú, CNBV en México) exigen que su implementación esté integrada desde el diseño mismo de las arquitecturas tecnológicas.

En este contexto, el cumplimiento normativo se ha convertido en una de las principales prioridades para los CIO, CTO y líderes de innovación. No solo por las multas y riesgos reputacionales, sino porque afecta directamente la velocidad de integración de nuevos productos digitales, la experiencia del usuario y la escalabilidad operativa.

Cumplir con los marcos regulatorios exige mucho más que checklists. Supone diseñar plataformas que incorporen desde el inicio principios de seguridad, trazabilidad, validación de identidad y monitoreo continuo. Modelos como compliance-by-design o DevSecOps permiten reducir tiempos de auditoría y aumentar la confianza en cada interacción digital.

Al adoptar soluciones automatizadas de cumplimiento normativo, como orquestadores KYC/AML, herramientas de firma electrónica con trazabilidad legal o flujos de onboarding digital con autenticación biométrica, las áreas de TI pueden disminuir la carga operativa, garantizar integridad regulatoria y liberar capacidad técnica para innovación.

Asimismo, la inteligencia artificial y el aprendizaje automático están convirtiendo el cumplimiento en un proceso dinámico, automatizado y preventivo. Hoy es posible implementar sistemas capaces de detectar patrones inusuales, validar identidades en tiempo real y anticipar riesgos de fraude, incluso antes de que ocurra una transacción.

Según el informe Banking on AI de Accenture, la adopción de inteligencia artificial generativa puede mejorar la productividad en el sector bancario hasta en un 30%, especialmente en funciones como gestión de riesgos, cumplimiento normativo, tecnología, recursos humanos y legal.

“45% de las empresas en México reportó intentos o casos efectivos de fraude”

Riesgos reales, amenazas crecientes que afectan a la reputación y confianza

La industria financiera en México, Perú y Chile enfrenta serios desafíos relacionados con la confianza y la reputación. Entre los principales riesgos se encuentran los fraudes, la suplantación de identidad y el manejo inadecuado de información sensible.

En 2024, el 45% de las empresas en México reportó intentos o casos efectivos de fraude, siendo los más comunes el robo de identidad y los conflictos de interés. En Perú, una filtración masiva en Interbank expuso datos sensibles de tres millones de clientes, lo que puso de manifiesto la urgencia de fortalecer la ciberseguridad. En Chile, las entidades financieras también han enfrentado incidentes similares, lo que refuerza la necesidad de implementar estrategias preventivas sólidas.

Estos incidentes no solo representan pérdidas económicas: también erosionan la confianza del cliente y ponen a prueba la robustez de las plataformas tecnológicas. Ante esto, los líderes de TI están llamados a implementar modelos de Zero Trust, fortalecer la autenticación multifactor y asegurar la gobernanza de datos sensibles en entornos híbridos.

Colaboración entre áreas: clave para generar confianza digital en Latinoamérica

Uno de los mayores retos para la implementación de soluciones de cumplimiento regulatorio es la fragmentación organizacional. La colaboración entre Tecnología, Compliance, Seguridad, Legal y Comercial no es solo deseable: es indispensable.

En Chile, el Consejo de la Innovación Financiera promueve esta sinergia entre el sector público y privado. En México, la Ley Fintech ha impulsado mecanismos de integración entre banca y startups tecnológicas. Y en Perú, los regulatory sandboxes permiten testear innovaciones sin comprometer la estabilidad del sistema.

Estas experiencias confirman que el cumplimiento regulatorio puede ser un acelerador de innovación, siempre que exista una infraestructura tecnológica preparada y una cultura organizacional que fomente la colaboración.

Para convertir el cumplimiento en una ventaja competitiva, las instituciones deben pasar de una lógica reactiva a una proactiva, adoptando medidas como:

- Implementar arquitecturas tecnológicas que incorporen trazabilidad y validación automatizada desde el origen.
- Integrar herramientas de IA que anticipen riesgos y optimicen procesos regulatorios.
- Fomentar la colaboración entre áreas para reducir fricciones en la entrega de valor.
- Adoptar frameworks de seguridad centrados en datos y usuarios, como Zero Trust.

> **“El cumplimiento regulatorio puede ser un acelerador de innovación”**

Ecosistema de confianza digital de Sovos: seguridad, cumplimiento y eficiencia

Confianza digital: un imperativo para escalar con seguridad

La digitalización del sector financiero ha traído consigo nuevas oportunidades de negocio, pero también ha elevado las exigencias sobre las áreas tecnológicas, considerando además que el cumplimiento normativo es dinámico y las amenazas cibernéticas son constantes, la confianza es una condición crítica para crecer y competir.

Para los equipos TI, esto implica asegurar que cada punto de contacto con el cliente (desde el onboarding hasta la firma de contratos o el acceso a plataformas) esté respaldado por infraestructura segura, escalable y compliant por diseño. Ya no se trata sólo de implementar tecnología: se trata de garantizar experiencias digitales fluidas y confiables, cumpliendo con normativas como KYC, AML y los marcos regulatorios locales en Chile, Perú y México.

> **“La confianza es una condición crítica para crecer y competir”**

La seguridad y el compliance como habilitadores de innovación

En la actualidad, los equipos de TI tienen la oportunidad de convertir al cumplimiento en un diferenciador competitivo. Tecnologías como las que ofrece Sovos permiten a las organizaciones automatizar procesos críticos de verificación e identificación, mediante biometría facial y dactilar, digital footprint, OTP y otros métodos adaptados a la legislación de cada país.

Estas soluciones no solo mitigan riesgos operacionales y reputacionales, sino que además se integran de forma nativa con los sistemas actuales, sin requerir desarrollos complejos. Esto acelera el time-to-market, reduce la fricción tecnológica y evita cuellos de botella operativos.

Además, Sovos facilita el cumplimiento normativo desde la arquitectura del sistema:

- Verificación de identidad robusta
- Firma electrónica conforme a la legislación local.
- Automatización del ciclo de vida documental.

Todo esto, bajo una plataforma única y centralizada que soporta la operación multi-sede y omnicanal, lo que es clave para instituciones financieras con presencia regional o que operan en entornos híbridos.

Sovos: automatización y cumplimiento normativo para impulsar el crecimiento del negocio

En la industria financiera latinoamericana, el cumplimiento regulatorio se ha vuelto cada vez más complejo a medida que las organizaciones crecen y digitalizan sus operaciones. Esto no solo impacta al área legal o tributaria: también ralentiza a los equipos comerciales, retrasa iniciativas estratégicas y obstaculiza la innovación.

Frente a este escenario, Sovos ofrece una propuesta tecnológica robusta, diseñada para resolver los desafíos normativos con un enfoque automatizado, escalable y seguro. Su ecosistema de confianza digital permite a las áreas de Tecnología e Innovación apoyar a las unidades de negocio con soluciones listas para el cumplimiento (compliance-ready) y fácilmente integrables a los sistemas existentes. El resultado: menos fricción, mayor agilidad y reducción de riesgos operativos y legales.

Sovos cuenta con una infraestructura nativa en la nube, modular y escalable, que se adapta a los entornos tecnológicos más exigentes. Gracias a su suite de APIs seguras, las soluciones pueden integrarse rápidamente con los sistemas internos, sin desarrollos complejos ni sobrecarga operativa.

Además, su diseño permite adaptarse de forma proactiva a los cambios regulatorios, sin necesidad de rediseños estructurales. Esto reduce los costos y facilita la continuidad operativa en un entorno normativo en constante evolución.

1. Verificación de identidad: Sovos combina tecnologías biométricas (facial, dactilar) y no biométricas (OTP, huella digital, vigencia de documentos) para validar identidades de forma remota o presencial, cumpliendo con las normativas KYC y AML en cada país:

- **Chile:** Verificación biométrica facial y dactilar, y no biométrica como digital footprint, códigos OTP y vigencia de documentos.
- **Perú:** Verificación biométrica facial y dactilar, y no biométrica como digital footprint y OTP.
- **México:** Verificación biométrica facial y no biométrica, como OTP y digital footprint.

Estas soluciones, certificadas bajo estándares internacionales (ISO 27001, ISO 30107-3 Nivel 2, IQNet) y locales, reducen significativamente el tiempo de onboarding de clientes y previenen fraudes desde la primera interacción.

2. Firma electrónica: Sovos soporta los distintos tipos de firma según los marcos normativos de cada país, permitiendo firmar contratos y acuerdos en tiempo real, desde cualquier dispositivo, con plena validez jurídica.

3. Gestión documental automatizada (Chile y Perú): Permite la generación, firma, envío y almacenamiento de documentos y contratos digitales de forma automática y trazable. Entre sus beneficios clave:

- Integración directa con otros sistemas.
- Trazabilidad en tiempo real del estado de cada documento.
- Cumplimiento garantizado ante auditorías o fiscalizaciones.

Esta automatización mejora los tiempos de respuesta, reduce los costos y fortalece la experiencia del cliente, al tiempo que asegura cumplimiento legal y evidencia verificable en cada transacción.

Beneficios clave del ecosistema de confianza digital de Sovos para líderes de Tecnología e Innovación

Los líderes de TI enfrentan el desafío de mantener operaciones ágiles, seguras y alineadas con normativas locales e internacionales, sin frenar el crecimiento del negocio.

Sovos entiende esta presión y ofrece una propuesta pensada específicamente para quienes están a cargo de diseñar, escalar y asegurar la infraestructura tecnológica de las instituciones financieras. Su ecosistema de confianza permite:

- **Reducir la complejidad operativa,** integrándose fácilmente con los sistemas actuales mediante APIs abiertas, sin necesidad de desarrollos costosos ni interrupciones en los flujos existentes.
- **Automatizar el cumplimiento normativo (SBS, CNBV, CMF, entre otros),** adaptándose con agilidad a los cambios regulatorios sin rediseñar procesos ni cargar al equipo TI con tareas manuales.
- **Reforzar la ciberseguridad operativa,** garantizando la protección de identidades y transacciones críticas con trazabilidad completa y validación en tiempo real.
- **Disminuir el riesgo tecnológico,** gracias a una solución compliance-ready que asegura continuidad operativa y permite anticiparse a auditorías, evitando incidentes que afecten la reputación o provoquen sanciones.
- **Optimizar la gestión de recursos técnicos,** liberando tiempo del equipo de tecnología al eliminar procesos redundantes, centralizar la administración de identidades y acelerar la implementación de servicios digitales seguros.

Con Sovos, los equipos tecnológicos pueden ofrecer a su organización una infraestructura robusta y flexible, alineada con las demandas del negocio y con las exigencias regulatorias, sin sacrificar escalabilidad ni innovación.

Sus resultados hablan por sí solos: actualmente, Sovos realiza más de 90 millones de verificaciones de identidad al año y habilita la firma y distribución de más de 60 millones de documentos electrónicos, alcanzando tasas de conversión de hasta un 99,7% en procesos de onboarding remoto.

Gracias al enfoque consultivo, presencia regional y profundo conocimiento regulatorio, Sovos no es solo un proveedor; es un socio estratégico para líderes de TI que buscan acelerar la transformación digital con seguridad jurídica, interoperabilidad y eficiencia.

Si quieres conocer cómo este ecosistema de confianza digital puede adaptarse a los desafíos específicos de tu empresa, agenda una reunión con nuestros expertos y conversemos sobre cómo Sovos puede ayudarte a acelerar la transformación digital con seguridad y cumplimiento.

SOVOS

Optimización, Seguridad y Cumplimiento:

Claves tecnológicas para escalar sin riesgos en la industria financiera

Contáctanos: https://sovos.com/es/contacto/
contacto@sovos.com