Whitepaper

El nuevo CIO: Navegando la transformación digital en un mundo regulado

Una mirada a las oportunidades y desafíos estratégicos que enfrentan los CIO en Latinoamérica en el escenario 2026–2027.

SOVOS

sovos.com/es

Contenido

04 Latinoamérica

05 Multiplicidad de frentes

11 Cómo se construye confianza

12 Desafíos específicos para los CIO

14 Elegir partners que aporten valor

15 ¿Cómo puede ayudar Sovos?

En las últimas décadas, el rol del CIO ha atravesado una transformación profunda. De ser, principalmente, guardianes de la infraestructura tecnológica, hoy, y de cara a los próximos años, están ocupando un nuevo lugar como líderes estratégicos y agentes de innovación, y juegan un rol esencial para impulsar resiliencia y competitividad en sus organizaciones.

En efecto, en un mundo cada vez más digital y regulado, el CIO debe ir mucho más allá de las fronteras del back office; su rol se vuelve transversal dentro de la organización. La digitalización creciente le exige equilibrar habilidades de negocio y tecnología, gestionar riesgos, anticipar regulaciones, articular estrategias complejas y fomentar una cultura organizacional ágil.

A la par, debe ser un líder con visión de negocio y una sensibilidad especial para gestionar el cambio, inspirar equipos y hablar el lenguaje del directorio.

De hecho, un 52% de los CIO anticipan que su rol será estratégico en los próximos 3-5 años, superando el enfoque operativo tradicional.

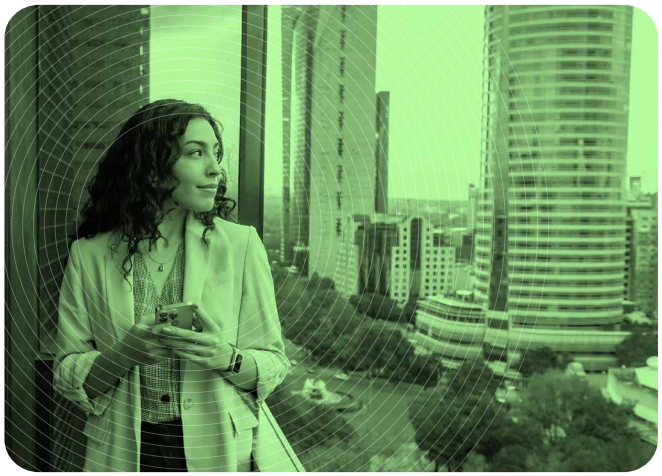
Esta evolución responde a una necesidad: las organizaciones exigen que la tecnología no solo funcione, sino que impulse la innovación, anticipe riesgos, genere valor. Y en ese proceso, el CIO se convierte en una figura fundamental.

El desafío es grande: según Gartner (2024), solo el 48% de las iniciativas digitales cumplen sus objetivos de negocio, una tendencia que se mantiene y refuerza la urgencia de evolucionar el liderazgo tecnológico hacia el futuro.

En este contexto, el CIO necesita asumir misiones claras que le permitan materializar la transformación estratégica y cultural dentro de la organización. Estas misiones funcionan como un marco para priorizar esfuerzos, alinear a los equipos y garantizar que cada iniciativa digital se oriente a resultados de negocio medibles y sostenibles:

- **Innovar con propósito:** La tecnología ya no es solo eficiencia: es motor de nuevos negocios, de ingresos y de expansión estratégica. Aquí aparece en juego el catalizador más disruptivo: la IA. Pero no es el único.
- **Blindar la resiliencia digital:** Frente a ciberamenazas y otras vulnerabilidades, el CIO construye infraestructuras que protegen datos y aseguran la continuidad operativa.
- **Velocidad y calma:** La rapidez es clave, pero sin perder la brújula: gobernanza, compliance y gestión de riesgos deben ir insertos en cada iniciativa.
- **Liderar el cambio humano:** Sin personas, no hay transformación digital. El CIO es agente cultural, fomenta el aprendizaje continuo y une áreas diversas bajo objetivos comunes.

Latinoamérica: un terreno con desafíos únicos



En Latinoamérica, el proceso de transformación del rol del CIO ocurre en un contexto marcado por una combinación singular de oportunidades y retos. La región se caracteriza por marcos regulatorios en evolución, un entorno de negocios que exige innovación constante y la necesidad de impulsar la digitalización como motor de competitividad.

Sin embargo, este avance ocurre en un terreno que exige a los líderes tecnológicos un enfoque pragmático, adaptable y con una visión regional clara para gestionar realidades complejas.

Entre los desafíos que marcan el día a día del CIO latinoamericano se destacan:

- Disparidad en madurez digital entre países y sectores.
- Infraestructura desigual y brechas de conectividad.
- Presión presupuestaria constante y necesidad de eficiencia.
- Entornos normativos en evolución, con reformas tributarias, nuevas regulaciones sobre privacidad, identidad digital, firma electrónica y ciberseguridad.
- Altas expectativas de digitalización en clientes, reguladores y partners estratégicos.

Estas condiciones hacen que el CIO tenga que asumir un rol más versátil, pragmático e innovador que en otras regiones.

Además, debe ser el nexo entre áreas de negocio que necesitan agilidad, equipos técnicos que implementan cambios constantes y reguladores que exigen cumplimiento en tiempo real. Esto requiere una nueva capacidad para escuchar y articular.

El CIO debe conocer los marcos normativos relevantes (protección de datos, identidad digital, facturación electrónica); participar en mesas de toma de decisión que incluyen al área legal, finanzas y cumplimiento y anticipar impactos regulatorios sobre los modelos tecnológicos.

Multiplicidad de frentes: tecnología, compliance y experiencia

El contexto en el que operan los CIO en Latinoamérica es tan desafiante como estimulante. Navegan en un entorno caracterizado por disrupción tecnológica acelerada, presión regulatoria creciente, demandas de innovación constantes y una coyuntura económica que exige eficiencia extrema. Todo esto, enmarcado en una región que avanza de forma desigual, pero con señales claras de transformación digital estructural.

Estos líderes ya no enfrentan una agenda de TI, sino una agenda corporativa. Cada decisión tecnológica impacta en la operación, en el cumplimiento normativo, en la experiencia del cliente y en la percepción del negocio por parte del mercado.

Entre los grandes desafíos del escenario actual destacan:

- Tecnología como eje del negocio, no como soporte. Las soluciones TI están directamente conectadas con la competitividad.
- Proliferación de marcos regulatorios, especialmente en sectores como finanzas, salud, retail y telecomunicaciones.
- Consumidores más exigentes, que esperan experiencias digitales simples, seguras y personalizadas.
- Presión por reducir costos, sin perder capacidad de innovación o velocidad de respuesta.
- Falta de talento calificado, lo que obliga a pensar estrategias de retención, upskilling (enseñar nuevas competencias para optimizar el desempeño) y automatización inteligente.

En este contexto, la figura del CIO se vuelve crítica: no solo para operar, sino para sostener la continuidad del negocio y proyectarlo hacia el futuro.

Algunos de los retos más relevantes para los CIO:

IA: la avalancha ineludible

Como ya dijimos, Latinoamérica está viviendo una adopción acelerada -aunque no siempre madura- de tecnologías como inteligencia artificial, nube híbrida, blockchain, ciberseguridad avanzada y automatización de procesos, entre otras. El escenario cambia de manera continua y constante.

La inteligencia artificial .y en particular la IA generativa. se ha convertido en una de las tecnologías con mayor protagonismo en la agenda de los CIO, impulsando nuevas eficiencias operativas, automatización de procesos y capacidades avanzadas de análisis, generando altas expectativas sobre su capacidad de transformar los modelos de negocio.

La IA, en particular, es un hito transformador ubicado al centro de la agenda: según un estudio de Gartner, el 74 % de los CEO afirman que esta es la tecnología que tendrá mayor impacto en su sector; mientras que según State of the CIO Survey 2025, un 80% de los CIO están a cargo de investigar y evaluar tecnologías de IA, posicionándose como líderes clave en la agenda tecnológica.

Sin embargo, demostrar el retorno de la inversión en IA es aún un gran desafío: los costos asociados son difíciles de prever y los resultados, lentos en llegar.

Para justificar la inclusión de la IA, los CIO debieran elaborar un plan de negocio que considere tres mediciones críticas: el retorno de inversión (ROI), el impacto en la eficiencia de los empleados (return on employee, ROE) y el impacto en la preparación de la empresa para el futuro (return on the future, ROF).

¿Por qué importan estas métricas? Porque la IA no es solo una mejora tecnológica: es una aliada estratégica. Y mientras el ROI evidencia la ganancia financiera, el ROE muestra cómo la IA potencia a los empleados, y el ROF prepara a la empresa para futuros cambios del mercado. Juntas, estas métricas permiten evaluar y optimizar de forma integral las estrategias de IA.

La IA también tiene una gran influencia en lo regulatorio: la necesidad de establecer marcos legales que aseguren un uso ético, responsable y seguro de la IA ha generado una carrera contra el tiempo por crear normativas actualizadas y efectivas.

Según un informe de la Comisión Europea de 2023, el 78% de los reguladores en Europa consideran que la regulación de la IA es un desafío prioritario, destacando la importancia de equilibrar innovación y protección.

En Latinoamérica, países como Brasil han comenzado a avanzar en esta dirección; en 2024, se aprobó el Proyecto de Ley 2338/2023, que propone la creación de un marco regulatorio para la inteligencia artificial. En Chile, el Decreto 12, del 28 de enero de 2025, aprobó la actualización de la política nacional de inteligencia artificial, sentando las bases para su implementación progresiva en los próximos años, que busca posicionarla como un motor clave para el desarrollo sostenible.

Estos cambios desafían la capacidad de las empresas para adaptarse a las condiciones del mercado e impulsar la innovación en IA. Los CIO deben abordar estos retos de forma proactiva mediante el desarrollo de marcos de cumplimiento ágiles.

Evangelización y cambio cultural: Para que la IA tenga un impacto real, es necesario educar y capacitar a los empleados, promoviendo una cultura de adopción tecnológica. Esto implica no solo implementar herramientas, sino también acompañar el cambio organizacional.

Es deber y responsabilidad del CIO -y de los líderes de cada empresa- trabajar activamente en esta tarea, liderando con el ejemplo y facilitando el camino hacia una cultura digital más madura.

IA, gobernanza y responsabilidad: el nuevo foco hacia 2026–2027

A medida que la inteligencia artificial se integra de forma estructural en los procesos de negocio, el foco deja de estar únicamente en la adopción tecnológica y se desplaza hacia la gobernanza, el control y la responsabilidad.

En el escenario 2026–2027, los CIO deberán asegurar no solo el rendimiento de los modelos de IA, sino también su trazabilidad y alineación con marcos éticos y regulatorios en evolución. Auditorías algorítmicas, gestión del riesgo automatizado y responsabilidad sobre decisiones basadas en IA pasarán a formar parte de la agenda cotidiana del liderazgo tecnológico.

En este contexto, el CIO se consolida como un orquestador clave entre tecnología, cumplimiento, áreas legales y negocio, garantizando que la innovación basada en IA genere valor sostenible sin comprometer la confianza ni el cumplimiento normativo.

> **“Las personas ya no comparan su banco con otros bancos, sino con apps de delivery, tiendas online o fintechs”**

Navegar marcos regulatorios dinámicos y fragmentados

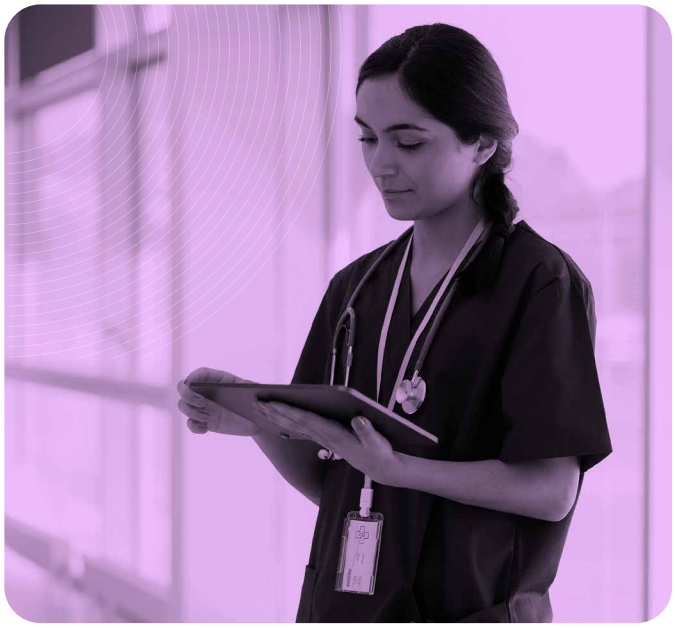
El entorno regulatorio en América Latina es como un terreno en constante reconfiguración. Normas fiscales, de protección de datos, ciberseguridad, identidad digital y firma electrónica evolucionan rápidamente. Pero no siempre de forma coordinada entre países o sectores. Esto genera:

- Cargas operativas para adaptarse a cada jurisdicción.
- Riesgos de incumplimiento por falta de alineación entre TI y Legal.
- Necesidad de contar con partners especializados para asegurar la adecuación normativa continua.

Pero lejos de ser solo una restricción, la regulación -cuando se implementa con visión estratégica- puede actuar como catalizador de adopción tecnológica. Así lo demuestran casos como:

- Factura electrónica: ya es obligatoria en la mayoría de los países, aunque cada uno tiene sus propias reglas, formatos, documentos equivalentes y sistemas de validación.
- Normativas de protección de datos (como la Ley 29.733 en Perú, la LGPD en Brasil, la Ley 25.326 en Argentina, la nueva Ley N° 21.719 en Chile).
- Regulación de firma electrónica, que exige soluciones seguras, auditables y trazables.
- Normativas referentes al uso de la identidad digital, su validación y aplicación concreta, como la Resolución 566/2024 en Chile, que obliga a las empresas de telecomunicaciones a verificar con biometría la identidad de las personas involucradas en procesos comerciales.

Sin embargo, el contexto normativo sigue siendo complejo, cambiante y fragmentado. Para los CIO, esto representa un desafío en términos de cumplimiento y adaptación tecnológica y a la vez, una oportunidad para liderar proyectos que fortalezcan la gobernanza digital.



Complejidad operativa y expectativas de agilidad

En un entorno VUCA (volátil, incierto, complejo y ambiguo), en que las empresas se ven obligadas a prosperar adaptándose a cambios veloces, los CIO enfrentan una paradoja: deben reducir la complejidad, sin perder flexibilidad ni escalabilidad. Esto implica, entre otros elementos:

- Migrar a arquitecturas modulares.
- Automatizar procesos repetitivos.
- Reducir fricciones entre sistemas legacy y nuevos desarrollos.
- Priorizar soluciones interoperables y con rápida implementación.

Equilibrar continuidad e innovación

Uno de los mayores retos para los CIO es impulsar la transformación digital mientras garantizan la operación sin interrupciones. Es como intentar cambiar las ruedas de un auto en movimiento: las áreas de negocio exigen mejoras en tiempos de respuesta, escalabilidad y disponibilidad 24/7, mientras esperan automatización, experiencias digitales fluidas e incorporación de IA y analítica avanzada.

No innovar implica perder competitividad, pero innovar sin asegurar estabilidad operativa puede generar riesgos críticos. La clave está en priorizar iniciativas que aporten valor tangible al negocio, midan su retorno y puedan desplegarse con escalabilidad y resiliencia.

Datos como activo estratégico

Los datos bien gestionados permiten tomar decisiones más inteligentes, predecir comportamientos y personalizar experiencias, y son fundamentales para una estrategia que involucre la IA. Son un activo estratégico por excelencia, pero su volumen y diversidad hacen que su gestión sea un desafío diario. Los CIO deben enfrentar preguntas clave:

- ¿Dónde residen nuestros datos y bajo qué normativas?
- ¿Están protegidos y disponibles para los usuarios correctos?
- ¿Son confiables para la toma de decisiones en tiempo real?

Con la expansión de la nube híbrida, el edge computing y los entornos multicloud, garantizar soberanía, trazabilidad y calidad del dato se vuelve prioritario. Según Gartner, el 80% de los CIO considera que redefinir su estrategia de datos en el corto y mediano plazo será clave para sostener su transformación digital.

Para esto, algunos puntos que deben contemplar son:

- Contar con modelos sólidos de gobernanza de datos: calidad, trazabilidad, linaje.
- Tener políticas claras de ética y privacidad: consentimiento, propósito, derecho al olvido.
- Asegurar una capacidad analítica avanzada: desde analítica descriptiva hasta modelos predictivos y prescriptivos.

Alinear expectativas internas con capacidades reales

A medida que las áreas de negocio se digitalizan, crecen las expectativas sobre el área tecnológica. Pero no siempre esas expectativas van acompañadas de recursos, presupuesto o tiempo suficiente.

Los CIO enfrentan tensiones como:

- Presión por entregar proyectos más rápido con menos presupuesto.
- Exigencias de disponibilidad 24/7, incluso con infraestructura heredada.
- Visiones fragmentadas entre equipos internos sobre las prioridades tecnológicas.

Aquí, la comunicación se vuelve una habilidad crítica: el CIO debe traducir necesidades en planes realistas, explicar prioridades y negociar recursos con una narrativa clara de valor de negocio.

Construir equipos resilientes (y retener talento clave)

De acuerdo con la Encuesta Global de Escasez de Talento de ManpowerGroup, el 76% de las organizaciones del sector TI reporta dificultades para encontrar profesionales calificados.

La falta de talento TI especializado es una constante en la región, y cuando se logra formar un equipo competente, surgen nuevos retos: altas tasas de rotación, sobrecarga operativa y otras empresas que compiten, a través de salarios o beneficios, para llevarse a los especialistas en temas como IA, ciberseguridad y arquitectura cloud.

Para Gartner, los CIO que busquen elaborar una estrategia de TI para el futuro y mejorar las capacidades digitales de su empresa deben:

1. Actualizar y mejorar las habilidades de los empleados de manera más rápida, continua y eficaz.
2. Buscar una forma eficiente de competir en el mercado para atraer a candidatos calificados y retener a los empleados especializados en áreas críticas.
3. Colaborar con RR. HH. para cubrir puestos clave y apoyar el aprendizaje, el desarrollo y la gestión de recursos.

Presupuestos restringidos: hacer más con menos

La presión presupuestaria es una constante en muchas organizaciones latinoamericanas. Esto se traduce en:

- Priorización de proyectos con ROI claro y rápido.
- Apuesta por soluciones modulares y escalables.
- Incremento de modelos “as-a-service” que permitan pagar por uso y reducir gasto de capital (CAPEX).

El CIO debe convertirse en un traductor de valor: explicar en términos de negocio por qué invertir en tecnología es invertir en competitividad y resiliencia.

“el CIO debe traducir necesidades en planes realistas, explicar prioridades y negociar recursos”

“90% de los CIO prioriza ciberseguridad como foco de inversión”

Amenazas cibernéticas y soberanía de datos

El aumento del espacio digital ha traído consigo una escalada sin precedentes en los riesgos de seguridad. Ransomware, fuga de datos, fraude por suplantación de identidad y accesos no autorizados son parte del nuevo panorama.

La ciberseguridad es mucho más que una cuestión de TI; es un imperativo empresarial estratégico, y son los CIO quienes cargan con la responsabilidad última de proteger sus organizaciones. De hecho, un 90% de los CIO prioriza ciberseguridad como foco de inversión.

IDC predice que, en 2026, el 50% de los CIO diversificarán y ampliarán las estrategias de seguridad a través de los equipos de TI y seguridad de su organización para hacer frente a las nuevas y rápidas amenazas a su ecosistema tecnológico y de cadena de suministro.

Por ejemplo, para conseguir que el área de TI esté más alineada con el negocio, los CIO deben colaborar con los directores de seguridad de la información (CISO) con el fin de actualizar el modelo operativo de ciberseguridad.

Las amenazas son múltiples. El IBM X-Force Threat Intelligence Index 2025 revela, entre otros puntos:

- Que los sectores financiero y de seguros en América Latina fueron los más atacados en 2024 (33%).
- Que los cibercriminales hoy prefieren robar datos (18%) en lugar de encriptarlos (11%), ya que enfrentan mayor detección y acciones legales, optando por ataques más rápidos.
- Que, en 2024, casi un tercio de los incidentes implicó robo de credenciales, usando métodos variados para obtener y aprovechar accesos de forma ágil.
- Y que, a medida que más empresas adopten la IA, aumentará el interés de los ciberdelincuentes en crear ataques dirigidos específicamente a estas tecnologías.

En paralelo, crecen las demandas de soberanía digital: dónde se alojan los datos, quién los gestiona, cómo se garantiza su integridad y privacidad.

Todo esto obliga al CIO a:

- Fortalecer sus estrategias de ciberseguridad con enfoque proactivo.
- Involucrarse directamente en decisiones sobre arquitectura de datos.
- Trabajar junto a compliance y legal para garantizar cumplimiento continuo.

Cómo se construye confianza en el ecosistema del CIO

> “No se trata solo de confiar en que los sistemas no fallen”

La palabra “confianza” aparece una y otra vez cuando hablamos de transformación digital. Pero ¿qué significa, en concreto, construir confianza en el día a día de un CIO? No se trata solo de confiar en que los sistemas no fallen.

En el ecosistema del CIO, la confianza se construye en varias capas:

Tecnológica
Que el sistema sea seguro, interoperable y auditable.

Regulatoria
Que cumpla con la norma, incluso cuando esta cambia.

Organizacional
Que las áreas usuarias entiendan y se comprometan con el cambio.

Relacional
Que los partners externos actúen con responsabilidad, transparencia y conocimiento experto.

Cada capa depende de la otra. Un sistema técnicamente perfecto, pero que no cumple con los requisitos legales, no genera confianza. Una solución segura pero incomprensible para el usuario, tampoco.

Desafíos específicos para los CIO en algunas industrias críticas

Cada industria enfrenta presiones particulares en su camino hacia la transformación digital. El CIO debe combinar conocimiento técnico con entendimiento profundo del negocio, de sus distintas áreas, y de su entorno regulatorio.

De cara a 2026–2027, el rol del CIO será clave para equilibrar innovación, cumplimiento y confianza digital en un entorno cada vez más exigente.

A continuación, un recorrido por cinco sectores clave en Latinoamérica.

> **"El rol del CIO será clave para equilibrar innovación, cumplimiento y confianza digital"**

Servicios financieros

Uno de los sectores más regulados y expuestos a disrupción tecnológica. Aquí, la confianza digital no es opcional.

- **Integración de identidad digital en procesos de onboarding:** los usuarios exigen alta velocidad sin sacrificar seguridad. Verificación de identidad biométrica y no biométrica, en línea y presencial, y KYC digital son hoy estándar esperado.
- **Cumplimiento regulatorio en entornos multijurisdiccionales:** los CIO deben asegurar interoperabilidad entre marcos regulatorios diversos.
- **Prevención de fraudes digitales y tokenización de datos:** la adopción de tecnologías como inteligencia artificial, verificación de identidad avanzada, detección de patrones y sandbox regulatorios (entornos controlados de pruebas para testear proyectos tecnológicos de innovación en los sistemas con pleno compliance) ayudan a anticiparse al fraude.

La tarea del CIO: liderar una arquitectura digital segura, modular y adaptable a nuevas regulaciones, con foco en la experiencia del cliente y la integridad del sistema.

Telecomunicaciones

Un sector clave para la infraestructura digital regional, que combina presión regulatoria con alta demanda tecnológica.

- **Escalabilidad de infraestructuras ante aumento exponencial de datos:** el auge del video, IoT y 5G exige optimizar redes, edge computing y almacenamiento distribuido.
- **Verificación de identidad para activación segura de servicios:** con el crecimiento del fraude de SIM swapping, los marcos regulatorios (como la Resolución 566/2024 en Chile) exigen métodos biométricos y trazabilidad.
- **Adopción de 5G y edge computing con foco en privacidad:** el CIO debe balancear latencia y procesamiento local con garantías de seguridad y cumplimiento normativo.

La tarea del CIO: alinear la modernización tecnológica con políticas de privacidad, gestión de identidad y disponibilidad de servicio continuo.

Retail

Transformación impulsada por la experiencia del cliente, omnicanalidad y protección de datos personales.

- **Experiencia omnicanal con foco en personalización segura:** integrar canales físicos y digitales con consistencia, sin comprometer datos sensibles.
- **Gestión de identidad y pagos digitales:** facilitar accesos rápidos, seguros y sin fricción, especialmente en contextos de comercio móvil y billeteras digitales.
- **Protección de datos sensibles del consumidor:** cumplimiento con leyes de privacidad y gestión del consentimiento.

La tarea del CIO: conectar experiencia, seguridad, cumplimiento y eficiencia en un entorno donde los datos del consumidor son el principal activo y riesgo.

Salud

Uno de los sectores más sensibles, donde interoperabilidad, privacidad y autenticación son críticas.

- **Creciente interoperabilidad de sistemas y datos clínicos:** la fragmentación entre instituciones públicas y privadas exige soluciones que hablen un lenguaje común. Chile está dando un paso con la nueva Ley 21.668 de Interoperabilidad de Fichas Clínicas.
- **Autenticación segura de pacientes y profesionales:** sistemas de firma electrónica robustos y verificación de identidad biométrica y no biométrica son clave para validar identidades en entornos híbridos.
- **Cumplimiento con normativas locales e internacionales:** protección de información de salud según leyes nacionales y marcos de gobernanza del dato.

La tarea del CIO: proteger vidas y privacidad con infraestructura confiable, interoperable y con trazabilidad total.

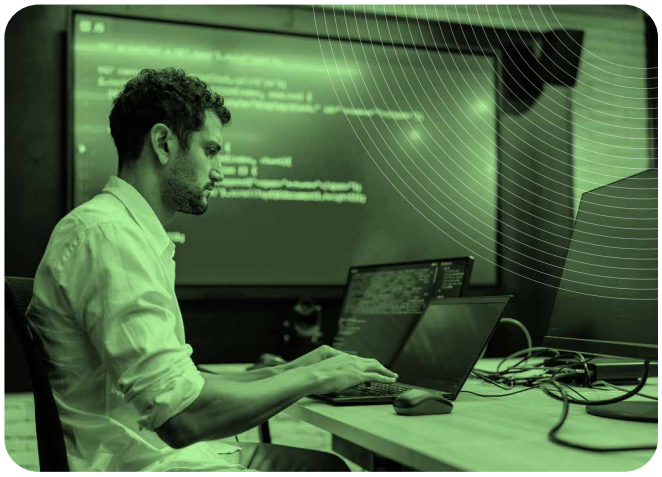
Educación

Transformación educativa acelerada gracias a la pandemia, que obliga a combinar inclusión digital con nuevas formas de garantizar la identidad.

- **Accesos digitales seguros a plataformas y contenidos:** desde el aula virtual hasta las bibliotecas digitales, la gestión de identidades es clave.
- **Prevención del fraude en certificaciones y evaluaciones:** verificación de identidad remota y presencial, validación de diplomas con blockchain y firma electrónica.
- **Inclusión digital y soporte a entornos híbridos de aprendizaje:** superar la brecha digital con infraestructura accesible, conectividad y herramientas adaptativas.

La tarea del CIO: garantizar el acceso equitativo y seguro al conocimiento, con foco en escalabilidad, interoperabilidad y ética digital.

Elegir partners que aporten valor, un apoyo para el CIO



> **“Actúen como partners estratégicos, no solo proveedores.”**

En un entorno con recursos limitados y demandas ilimitadas, saber qué mantener in-house y qué delegar a partners especializados es una habilidad estratégica esencial.

Los CIO priorizan partners que:

- Sean especialistas en áreas críticas (cumplimiento, datos, seguridad, integración).
- Actúen como partners estratégicos, no solo proveedores.
- Aporten escalabilidad y cumplimiento normativo desde el diseño.
- Equilibren innovación con cumplimiento.
- Sean un aliado para fortalecer la confianza digital.
- Ayuden a preparar a sus organizaciones para el futuro.

¿Cómo puede ayudar Sovos?

En Sovos, acompañamos a los CIO en esta misión, ofreciendo un ecosistema de soluciones que impulsan el negocio y convierten al compliance en un acelerador de la transformación digital y no en una barrera:

Servicios de confianza digital: Facilitamos la verificación de identidad biométrica y no biométrica, presencial y remota; la firma electrónica y la gestión documental segura, garantizando trazabilidad y cumplimiento normativo en cada transacción digital, mientras simplificamos la experiencia del usuario.

Facturación electrónica y cumplimiento tributario: Ayudamos a garantizar el cumplimiento de las regulaciones fiscales en todos los países de la región, con soluciones escalables y actualizadas en tiempo real ante cambios normativos, para que cada transacción cumpla con los requisitos locales y contribuya a la digitalización segura de los procesos de negocio.

Compliance como ventaja competitiva: Integramos estas soluciones con plataformas tecnológicas que permiten a los CIO reducir riesgos, eliminar silos de información y conectar procesos críticos bajo un mismo marco de cumplimiento, facilitando la interoperabilidad entre áreas de negocio y tecnología.

Sovos puede ayudar a los CIO no solo a garantizar la continuidad y resiliencia operativa de sus organizaciones; también actúa como un impulsor de la innovación responsable y sostenible, acompañándolos en los desafíos del escenario 2026–2027, y construyendo confianza digital en cada paso del camino.

Convierte el cumplimiento en una ventaja estratégica.

Transforma tu operación con Sovos.

Conoce cómo →