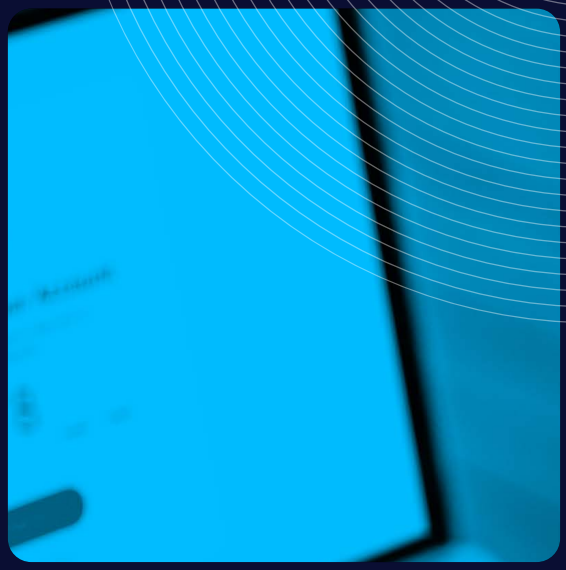
SOVOS



Siete Miradas Sobre la Transformación de la Confianza en el Entorno Digital

Sobre tecnología, regulaciones y protección de datos en los servicios de confianza

Contenido

Introducción

Vivimos en un mundo donde la confianza ya no se construye solo con un apretón de manos o cara a cara, sino con tecnología. En el mundo digital, las relaciones personales y las de negocios cruzan fronteras, industrias y dispositivos. Firmar, identificarse, contratar, proteger datos, cumplir la ley, todo ocurre en entornos digitales que requieren algo más que eficiencia: requieren credibilidad, seguridad y experiencia.

Pero ¿cómo se garantiza esa confianza en entornos tan diversos, rápidos y digitalizados?

En este eBook reunimos a siete líderes de Sovos que están transformando el modo en que habilitamos relaciones digitales confiables. No hablamos solo de soluciones. Hablamos de visión, diseño, personas y futuro.

Más allá de hablar de soluciones, este recorrido pone el foco en lo que está cambiando:

- La forma en que validamos quienes somos,
- La manera en que generamos acuerdos con valor legal,
- Y la forma en que protegemos nuestros datos y derechos en un entorno cada vez más automatizado.

En estas páginas reflexionamos sobre inclusión, ética, interoperabilidad y el papel estratégico de los servicios de confianza en una transformación digital que solo es posible si la confianza deja de ser una barrera y se convierte en motor.

“Hablamos de visión, diseño, personas y futuro”.

1. La nueva confianza: la identidad en tiempos digitales

Por Alberto Juárez, VP de Digital ID & Trust

En este artículo, Alberto Juárez explora cómo tecnología, regulación y enfoque ciudadano se combinan para construir un ecosistema digital seguro y legítimo. La identidad digital redefine la confianza en la era online.

Vivimos en una era en la que la identidad ya no se presenta solo con un apretón de manos, un documento físico o una firma en papel. En el mundo digital, cada interacción -desde acceder a una cuenta hasta firmar un contrato- exige saber con certeza quién está del otro lado. Y en ese nuevo escenario, la confianza ha dejado de ser un intangible: se ha convertido en infraestructura.

La transformación digital no solo cambió la forma en que nos comunicamos o hacemos negocios. Cambió las reglas del vínculo humano. Hoy, confiar en alguien significa confiar en los sistemas que lo representan. En ese marco, la confianza digital no es solo una cuestión tecnológica: es una construcción social, jurídica y cultural que define quiénes somos, cómo nos relacionamos y qué tan seguros estamos en el entorno online.

En el mundo digital, la confianza ya no es un valor agregado: es el cimiento. Cuando hablamos de confianza digital, no nos referimos solo a la seguridad o la privacidad de los datos, sino a la certeza de que estas están realmente ocurriendo. Es, en esencia, una relación de legitimidad entre tres actores: el ciudadano, la organización que valida su identidad, y la comunidad digital en la que ambos interactúan.

Más allá de la seguridad: el ciudadano como eje

La confianza se genera cuando el ciudadano percibe que sus datos -incluidos sus factores biométricos- están siendo tratados con responsabilidad. Pero también requiere transparencia en cómo las organizaciones capturan, administran y verifican esa identidad. No se trata únicamente de quién tiene la información, sino de cómo fue diseñada la tecnología que la gestiona. ¿Respeta los estándares? ¿Ofrece garantías de privacidad desde el diseño?

> **“En el mundo digital, la confianza ha dejado de ser un intangible: se ha convertido en infraestructura”**

Como ha señalado Thales en un estudio reciente, la confianza de los usuarios en las instituciones digitales está en descenso. Ninguna industria supera el 50% de confianza, y un porcentaje significativo de la Generación Z ha sido informado de intentos de fraude en su contra. La causa: arquitecturas de seguridad débiles, algoritmos mal entrenados o prácticas alejadas de la regulación.

Y, sin embargo, hay una paradoja alentadora: el mismo informe muestra que los usuarios confían cada vez más en la biometría como mecanismo de protección. La tecnología está lista. La confianza, como siempre, es una cuestión de implementación y propósito.

La identidad digital como llave del nuevo mundo

La identidad digital es la representación de cada uno de nosotros en la comunidad digital. Es la puerta de acceso a servicios, beneficios, derechos. Desde firmar un contrato hasta abrir una cuenta o emitir una póliza, necesitamos probar quiénes somos. Y la validación de ese yo digital tiene que partir del documento oficial -emitido, regulado y verificable- como base confiable.

La transformación ya está ocurriendo. Basta mirar un aeropuerto: en Argentina, Migraciones Express pasó de ser un experimento marginal a convertirse en la vía preferida por los viajeros. ¿Por qué? Porque es más rápido. Pero ese beneficio operativo esconde una lección más profunda: la tecnología bien diseñada construye confianza cuando ofrece ventajas tangibles.

De la biometría a la interoperabilidad

Las tecnologías biométricas no son nuevas: huella, rostro, voz, iris, comportamiento. Lo que viene ahora no es su invención, sino su evolución: su uso en nuevos escenarios y su implementación responsable. Para lograrlo, los gobiernos deben acompañar este proceso con marcos regulatorios claros. No para centralizar, sino para establecer reglas comunes.

Hoy, en Latinoamérica, la regulación está fragmentada. Hay países con avances importantes como Uruguay, Chile o Perú, pero sin un marco regional de interoperabilidad, la confianza se diluye. Una identidad digital nacional que no puedo usar para interactuar con mi municipio, mi licencia o en otro país, pierde algo de valor. La región necesita su propio eIDAS, un estándar común que permita escalar la transformación digital de forma segura y coordinada.

El triángulo virtuoso: identidad, firma y acuerdos

Cuando hablamos de servicios de confianza, a menudo intentamos jerarquizarlos. ¿Qué es más importante: la verificación de identidad, la firma electrónica o la gestión del documento o contrato? La verdad es que no se pueden separar. Son tres elementos de una misma ecuación:

- La identidad asegura que soy quien digo ser.
- La firma representa mi voluntad y aceptación.
- El documento es el contenedor de ese acuerdo.

Si uno de estos pilares no es digital, todo el proceso se frena. Por eso, contar con soluciones integradas permite avanzar de forma armónica en esta transformación. No se trata solo de digitalizar por digitalizar, sino de construir entornos de confianza que funcionen en la práctica y generen valor real.

Brechas, mitos y oportunidades

Aún hay desafíos importantes. En la región, las brechas tecnológicas persisten: no todos los ciudadanos tienen acceso a dispositivos o conectividad suficiente para gestionar su identidad digital. También hay desconocimiento: muchas personas no entienden qué es, por qué importa o cómo puede beneficiarlas.

El tercer gran reto es regulatorio. Como revela el mismo informe de Thales, los gobiernos siguen siendo las instituciones que generan mayor confianza. Eso implica una responsabilidad: deben liderar el proceso con regulaciones claras que protejan tanto a ciudadanos como a organizaciones.

El futuro de la confianza digital es compartido

La transformación no es tarea de un solo actor. Gobiernos y empresas tienen objetivos distintos -el bien común, la rentabilidad-, pero pueden converger en un propósito común: construir una comunidad digital segura, eficiente y confiable.

En Sovos, entendemos que la confianza digital no se impone: se construye con tecnología segura, marcos regulatorios sólidos y una visión centrada en las personas. Por eso, desarrollamos soluciones integradas de verificación de identidad, firma y gestión documental que permiten a gobiernos y empresas avanzar con confianza hacia un ecosistema digital más seguro, interoperable y humano

Lo que hace falta hoy no solo es más tecnología, es visión, regulación y colaboración. Porque en el mundo digital, la confianza no se decreta: se construye.

2. Diseñar la confianza: innovación que se siente

Por Tomás Castañeda, Director, Product Development

Para Tomás Castañeda, una solución efectiva nace del cruce entre lo técnico, lo normativo y la experiencia de usuario. En esta nota, reflexiona sobre cómo traducir esa combinación en herramientas que funcionen y generen valor en entornos complejos.

> “La confianza no se instala, se diseña”

Cuando hablamos de servicios de confianza, solemos nombrar herramientas como la firma electrónica, la verificación de identidad o la gestión de contratos digitales. Pero la verdadera pregunta es: ¿cómo logramos que las personas realmente confíen en estas soluciones? La confianza no se instala, se diseña. No es solo una capa técnica: es una experiencia que debe sentirse fluida, segura y humana.

En el ámbito del desarrollo de productos he aprendido que la innovación tecnológica es solo una parte del trabajo. El verdadero reto está en combinar tecnología, regulación, experiencia de usuario y seguridad. Porque cuando uno desarrolla soluciones que protegen la identidad, validan transacciones o resguardan la firma de documentos legales, cualquier error puede tener consecuencias enormes. Y eso marca profundamente la forma en que pensamos y diseñamos cada nuevo desarrollo.

Innovar sin poner en riesgo lo que ya funciona

Una de las preguntas que me acompaña en cada iteración del ciclo de producto es: ¿cómo seguimos evolucionando sin comprometer la estabilidad de lo que ya está operativo? Parece simple, pero no lo es. Nuestros sistemas procesan miles de interacciones por segundo. Tenemos clientes que no pueden parar ni por un minuto: bancos que deben validar identidades, telcos que deben activar líneas móviles, clínicas que gestionan consentimientos informados.

A veces llega un requerimiento comercial urgente, o un cambio normativo que hay que implementar rápido, o una mejora funcional que podría aportar mucho valor. Pero todo eso tiene que pasar por un proceso riguroso de evaluación, pruebas, impacto, revisión de riesgos. La estabilidad del ecosistema es una prioridad. Lo que hacemos está en la capa crítica del negocio de muchos clientes, y no podemos permitirnos fallar.

Cuando el fraude es parte del paisaje

En este contexto, el fraude no es una amenaza teórica. Es algo con lo que convivimos todos los días. Vemos intentos de suplantación reales, ataques programados, bots diseñados para explotar vulnerabilidades. Nuestra tasa de detección es altísima, pero con los volúmenes que manejamos, incluso un margen ínfimo de error puede traducirse en impactos reales.

Y es ahí donde aparece un dilema constante en el diseño de producto: si subes demasiado el nivel de seguridad, puedes bloquear a usuarios legítimos. Pero si lo bajas, dejas la puerta abierta al fraude. No es fácil encontrar ese equilibrio, sobre todo cuando cada cliente tiene niveles de tolerancia distintos frente al riesgo.

Hay industrias, como la financiera o la de telecomunicaciones, donde la suplantación de identidad tiene un impacto directo en el negocio. Y otras, como la salud, donde el foco está más en la protección de datos personales. En cada caso, el diseño de la solución tiene que adaptarse, tanto al contexto regulatorio como al uso que le darán los usuarios finales.

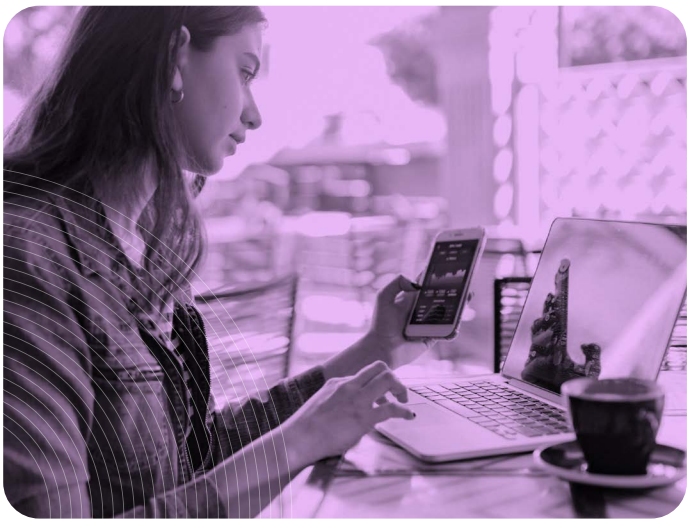
El impacto de los errores: más allá del software

A veces, cuando se trabaja en tecnología, se corre el riesgo de pensar que todo se resuelve desde el código. Pero en servicios de confianza, cada error tiene un rostro. Puede ser una persona que no logra firmar un consentimiento para hacerse un examen, o alguien que no puede acceder a su seguro porque el sistema no reconoció su rostro, o un cliente bancario bloqueado por un falso positivo.

Y eso no es trivial. Porque uno no trabaja solo para cumplir con un SLA (acuerdo de nivel de servicio: compromiso formal sobre tiempos y calidad de un servicio) o entregar una funcionalidad. Uno trabaja para que las personas puedan hacer su vida digital con seguridad y sin fricciones. Por eso, los errores duelen más que en otros rubros. Porque afectan la confianza, que es justamente lo que estamos comprometidos a proteger.

El poder de la colaboración: reguladores, industria y usuarios

Una de las cosas que más valoro de trabajar en Sovos es que no estamos solos en esto. Mantenemos una relación constante con entidades regulatorias, autoridades técnicas y asociaciones de la industria. En muchos casos, incluso participamos activamente en la co-construcción de estándares o en pilotos que buscan mejorar la seguridad a nivel país.



“Uno trabaja para que las personas puedan hacer su vida digital con seguridad y sin fricciones”

También trabajamos muy de cerca con los equipos legales, comerciales y de atención al cliente. Porque muchas veces un cambio técnico tiene implicancias legales, contractuales u operativas que no se ven a simple vista. Esa capacidad de trabajar en red, de incorporar distintas miradas al diseño, es lo que termina marcando la diferencia entre una funcionalidad útil y una solución confiable.

La regulación y los cambios

El crecimiento de soluciones de banking-as-a-service, las billeteras electrónicas y la masificación del acceso financiero están remodelando el panorama. Esto no solo cambia cómo las personas acceden a servicios, sino también cómo los atacantes intentan vulnerarlos. Más acceso significa también más oportunidades para el fraude, para la suplantación de identidad, para el lavado de activos. Todo eso hay que abordarlo desde el diseño del producto, y hacerlo sin frenar el avance.

Identidad digital: una conversación cada vez más estratégica

Algo que está cambiando, y que celebro, es que la conversación sobre identidad digital dejó de ser un tema puramente técnico o normativo. Hoy, los líderes de las organizaciones están entendiendo que la forma en que validamos a las personas en entornos digitales es un pilar estratégico del negocio. Tiene impacto en la experiencia del usuario, en la prevención del fraude, en la inclusión y en el cumplimiento normativo.

La identidad es el nuevo perímetro de seguridad. Es lo que permite, o impide, que una transacción ocurra. Y por eso, está dejando de ser vista como una "funcionalidad más" para transformarse en un componente esencial de la arquitectura digital de cualquier empresa.

Lo que viene: adaptabilidad, escalabilidad y protección de datos

Mirando hacia adelante, veo tres grandes temas que seguirán marcando nuestra hoja de ruta: adaptabilidad ante nuevas tecnologías, como los deepfakes o los modelos generativos; capacidad de escalar con eficiencia, para seguir creciendo sin sacrificar performance ni disponibilidad; y protección proactiva de los datos personales, que ya no es solo una exigencia legal, sino una demanda ética.

Tenemos la ventaja de operar en múltiples países, con clientes de diversas industrias y casos de uso muy variados. Eso nos obliga a pensar de forma transversal, pero también nos da una enorme riqueza de aprendizajes. Sabemos que no hay una única forma de verificar una identidad, ni una única solución de firma electrónica que sirva para todos. Pero sí hay principios que deben guiar todo lo que hacemos: seguridad, transparencia, cumplimiento y una obsesión constante por mejorar.

> **"Tenemos la ventaja de operar en múltiples países"**

Confiabilidad como cultura

Al final del día, lo que hacemos en Sovos no es solo construir software. Construimos confianza. En cada iteración, en cada decisión de diseño, en cada conversación con nuestros clientes. Y esa es una responsabilidad que nos tomamos en serio.

La confianza digital no es un estado que se alcanza una vez y se mantiene para siempre. Es una relación que se gana todos los días, y desde el equipo el equipo de Producto, trabajamos para que esa relación no se rompa. Porque sabemos que detrás de cada firma, de cada identidad validada, de cada documento enviado, hay una persona que confía en nosotros para que todo funcione como debe.

3. Verificación de identidad: más que un paso, un ecosistema

Por Raúl Wong, Identity Product Manager

En estas líneas, Raúl Wong analiza los retos de la verificación de identidad frente al fraude, la importancia de un enfoque multifactor que equilibre seguridad y experiencia, y el rol de la inclusión digital para lograr un onboarding confiable, transparente y adaptado a cada usuario.

> **"La verificación de identidad ha dejado de ser una etapa aislada"**

Hoy, verificar una identidad va mucho más allá de confirmar que alguien es quien dice ser. Implica enfrentar ataques de suplantación cada vez más sofisticados, basados en ingeniería social; cerrar nuevas brechas de acceso; incorporar tecnologías biométricas avanzadas; y, sobre todo, cuidar lo esencial: la experiencia del usuario.

Esta última es determinante. Aunque existen múltiples tecnologías y métodos para realizar la verificación, el usuario debe sentirse cómodo y seguro al compartir sus datos biométricos. La confianza digital ya no se construye con una sola capa, sino con varias: protección, diseño, inclusión y criterio.

La verificación de identidad ha dejado de ser una etapa aislada. Es la puerta de entrada a cualquier interacción digital significativa: abrir una cuenta bancaria, contratar un servicio, firmar un contrato o acceder a plataformas de salud y educación. En todos estos casos, la identidad debe confirmarse tanto de forma presencial como remota, manteniendo altos estándares de seguridad y minimizando fricciones.

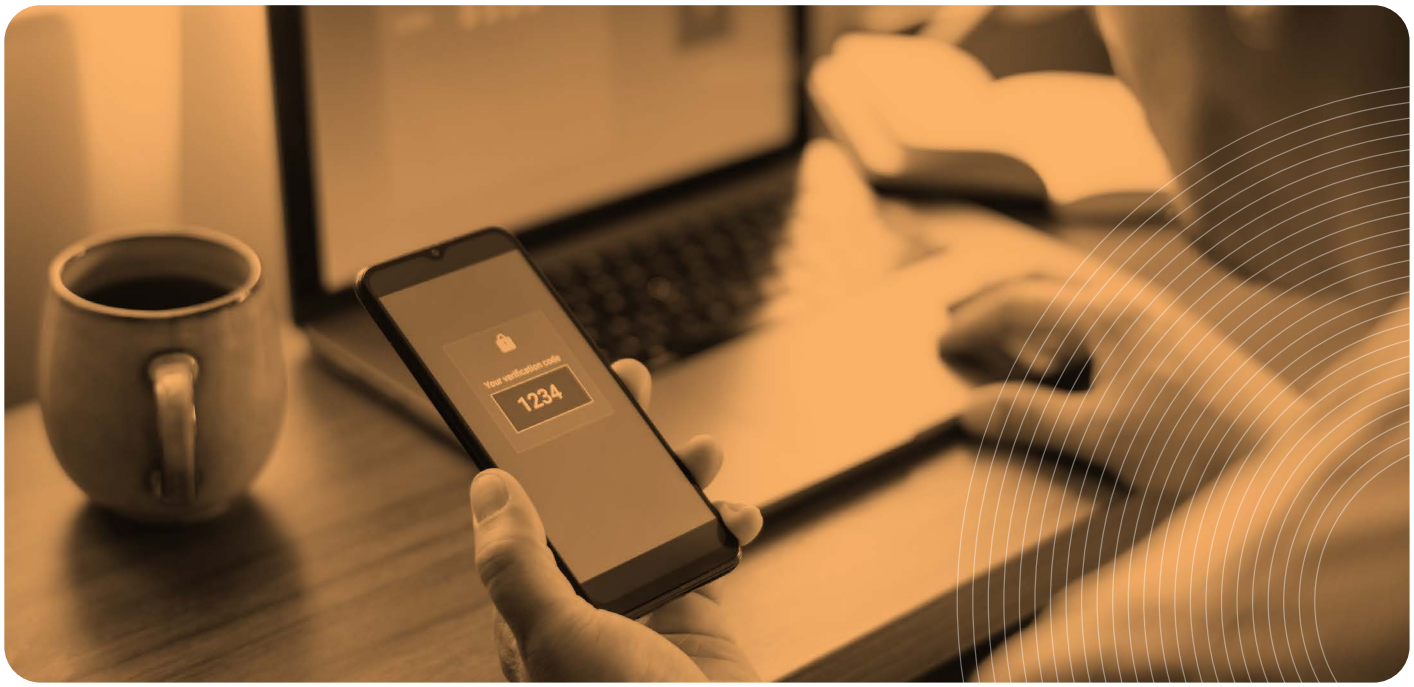
¿Cómo validar que una persona es quien dice ser?

La verificación de identidad engloba una serie de acciones que permiten identificar al usuario a través de tres dimensiones clave:

- Algo que eres (biometría)
- Algo que tienes (propiedad)
- Algo que sabes (conocimiento)

Estas dimensiones se traducen en métodos como:

- Lectura automática de documentos (OCR)
- Verificación biométrica facial y dactilar, incluyendo detección de prueba de vida (liveness detection)
- Validación cruzada con bases de datos confiables
- Autenticación reforzada mediante códigos, tokens o conexiones a registros oficiales



No existe una fórmula única. Por eso, el enfoque multifactor es esencial. Una verificación robusta combina métodos complementarios que elevan la seguridad sin sacrificar la experiencia del usuario.

Este enfoque no solo mejora la tasa de éxito, sino que también protege a las organizaciones frente a amenazas cada vez más complejas. Hoy, los intentos de fraude van más allá de documentos falsos o capturas de pantalla. Nos enfrentamos a falsificaciones de alta calidad, ataques sintéticos generados con inteligencia artificial -tecnología que antes requería experiencia especializada y recursos significativos-, así como amenazas internas operadas desde dentro de las propias organizaciones.

Las soluciones modernas deben ser capaces de detectar alteraciones imperceptibles, adaptarse a la evolución tecnológica y registrar cada paso del proceso con trazabilidad verificable, garantizando la irrefutabilidad de cada acción.

Seguridad, experiencia e inclusión: el equilibrio necesario

Diseñar soluciones seguras no debe significar dificultar el acceso. Nadie entra a una plataforma para “verificarse”: lo que busca es abrir una cuenta, contratar un servicio o acceder a un beneficio. El rol de un proveedor de confianza es garantizar que ese proceso sea seguro, sí, pero también natural, fluido y empático. Es fundamental mantener el equilibrio entre seguridad y las necesidades del negocio.

> **“Diseñar soluciones seguras no debe significar dificultar el acceso”**

Por eso, la verificación debe ser multicanal y flexible. Algunas personas completarán el proceso desde su teléfono; otras requerirán asistencia. Algunas preferirán reconocimiento facial; otras, huella dactilar. Lo importante es que el sistema se adapte al usuario sin comprometer la seguridad.

Esta capacidad de adaptación es clave para avanzar en inclusión digital. Muchas personas no son nativas digitales o no tienen acceso constante a tecnología. Para ellas, debemos diseñar interfaces simples, accesibles y ofrecer alternativas asistidas o presenciales. Desde textos intuitivos hasta instrucciones inteligentes por voz, video o guías automatizadas, el diseño centrado en el usuario no es una tendencia: es una necesidad para generar confianza.

La identidad digital está evolucionando

El onboarding digital ya no es solo una etapa más del viaje del cliente: es el momento en que se define la confianza. Por eso, el futuro está en construir una identidad digital interoperable, robusta y respaldada por un ecosistema colaborativo entre actores públicos y privados.

En Europa, ya se están desarrollando identidades digitales paneuropeas para evitar que una vulnerabilidad individual comprometa todo el sistema. En América Latina, países como Chile cuentan con bases de datos confiables, pero aún es necesario abrir ese acceso controlado al sector privado, donde se concentran la mayoría de las interacciones con los ciudadanos.

Esto no significa exponer datos sin control. Al contrario: implica crear modelos basados en consentimiento, trazabilidad y soberanía de datos. En este nuevo paradigma, la identidad pertenece a la persona. Y las organizaciones deben demostrar que están preparadas para protegerla.

Hacia una confianza digital proactiva

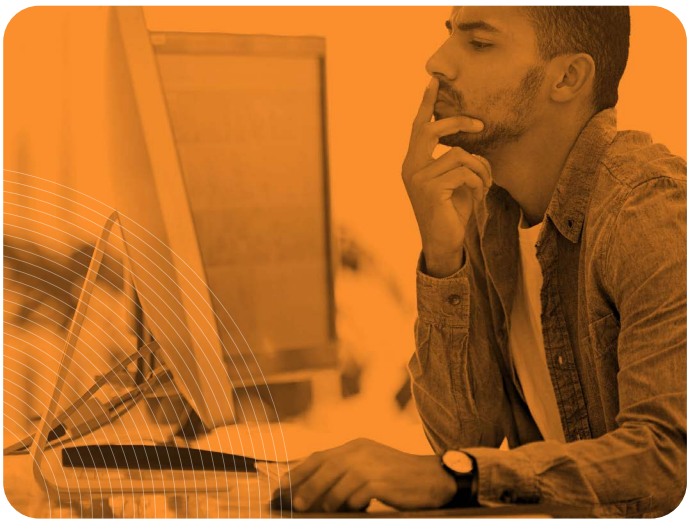
¿Cómo saber si un proceso de onboarding realmente funciona? Más allá de los tiempos de respuesta o las tasas de conversión, la clave está en la trazabilidad: poder mostrar, paso a paso, cómo se verificó una identidad, qué datos se utilizaron, qué métodos se aplicaron y con qué garantías se resguardó ese registro. Cuando una empresa puede entregar esa trazabilidad a un cliente, auditor o autoridad, está construyendo confianza de forma activa.

No hacerlo expone a un doble riesgo: el fraude, por un lado, y la pérdida de confianza del usuario -con todo lo que eso implica en reputación, cumplimiento y consecuencias legales- por el otro.

Nada de esto sería posible sin innovación. En nuestro trabajo, desarrollamos tecnologías que no solo responden a las amenazas actuales, sino que se anticipan a las futuras. Detectar deepfakes, adaptar métodos de verificación a distintos perfiles de usuario, incorporar inteligencia artificial que aprende de los ataques para prevenirlos: todo eso ya está en marcha.

Pero la verdadera innovación no está solo en la tecnología. Está en cómo la usamos para estar del lado de las personas.

En Sovos, trabajamos cada día para que eso sea posible. Nuestras soluciones de verificación de identidad no solo cumplen con las normativas más exigentes: están diseñadas para combinar seguridad, inclusión y experiencia, entendiendo las necesidades de cada industria y escuchando activamente el feedback de los usuarios. Creemos que la confianza digital no es solo una capacidad técnica: es una responsabilidad compartida.



“Las organizaciones deben demostrar que están preparadas para proteger la identidad”

4. Del puño y letra a la criptografía: la evolución de la confianza

Por Fabiola Fernández, Product Manager

Fabiola Fernández recorre la evolución de la firma electrónica: de la desconfianza inicial al desarrollo de un sistema global basado en usabilidad, trazabilidad y seguridad, que combina tecnología, regulación e identidad digital para garantizar transacciones confiables y sin fronteras.

> **“Barreras culturales llevan a muchos usuarios a preferir la fila y el bolígrafo”**

Hasta hace unos años, la confianza digital se consideraba un concepto emergente. La mayoría de nosotros seguíamos atados al papel. Un contrato no era “oficial” hasta que no veíamos la firma de puño y letra de la otra persona.

Los procesos digitales eran vistos con recelo; la idea de abrir una cuenta bancaria con una selfie o firmar un acuerdo de millones de dólares con un clic parecía ciencia ficción. La confianza en el entorno digital era frágil, un simple reflejo de la confianza en el mundo físico. Era una mera transferencia, no una transformación.

El proceso de transformación se inició cuando las organizaciones comprendieron que la confianza digital debía consolidarse como un pilar fundamental de seguridad, y no limitarse a ser un mero elemento simbólico.

Se empezaron a usar certificados digitales, pero la experiencia era torpe, y el proceso, lento. Era como intentar manejar un auto deportivo con el freno de mano puesto. La mayoría de las soluciones se enfocaban en lo legal, en “probar” la validez de un documento, pero ignoraban el factor humano: ¿cómo logramos que la gente confíe de verdad en estos sistemas?

Hoy, el panorama es radicalmente distinto. El mundo ha superado la desconfianza inicial y abrazado la digitalización de la confianza. Ya no copiamos la confianza del mundo físico, sino que la construimos desde cero con la tecnología. Lo que antes era un simple sello digital, ahora es un ecosistema completo que entrelaza varias capas de seguridad y conveniencia.

Los pilares de la confianza en la firma

Para generar confianza, la firma electrónica se basa en tres pilares principales e interconectados que garantizan su adopción y fiabilidad:

1. **Usabilidad:** El proceso de firma debe ser simple, claro y rápido, minimizando la fricción, desde el envío del documento hasta la firma final.
2. **Trazabilidad:** Un producto de firma electrónica confiable ofrece una "evidencia" robusta del proceso de firma, creando un rastro digital que puede ser revisado en caso de disputa legal. Esto incluye quién firmó, cuándo, dónde y cómo.
3. **Seguridad:** La firma electrónica debe asegurar la autenticidad del firmante, la integridad del documento y el no repudio de la firma para que sea legalmente válida y confiable.

El desafío de la seguridad y el reto de la experiencia de usuario

El mayor desafío es encontrar el equilibrio perfecto entre seguridad y usabilidad. Si el proceso de autenticación es demasiado complejo, la gente se frustrará y buscará alternativas más simples. Por eso, se debe trabajar para que la seguridad sea robusta, pero que al mismo tiempo se sienta invisible para el usuario final.

Un mapa global de confianza

La transformación de la confianza no se puede tomar como un fenómeno aislado; es un movimiento global impulsado por la necesidad de agilidad y seguridad. Lo que empezó como un nicho tecnológico se ha convertido en una regulación, y las empresas que ofrecen servicios de firma electrónica se transforman en un puente entre la ley y la tecnología.

En Europa, el reglamento eIDAS (Electronic Identification, Authentication and Trust Services) es la brújula que guía la confianza. Su enfoque en la estandarización permite dar a la firma cualificada la misma validez que una firma en papel en los 27 países de la UE. Para las empresas, esto significa que un contrato firmado en Berlín es tan válido en Lisboa como en Varsovia, eliminando la incertidumbre y acelerando el comercio digital.

En Estados Unidos, la Ley ESIGN (Electronic Signatures in Global and National Commerce Act) ha permitido que la firma electrónica se base en el "consentimiento implícito" del firmante. A diferencia de Europa, no hay una certificación centralizada, lo que ha impulsado a las empresas a innovar en la experiencia del usuario y en la integración con otros servicios. La competencia se centra en la facilidad de uso y la automatización de flujos de trabajo, haciendo que la firma sea parte de un proceso más grande y sin fricciones.

En América Latina, la evolución se enfoca en la identidad digital como el corazón de la confianza. Países como México están en la vanguardia con la CNBV y sus regulaciones para la biometría, así como la próxima CURP biométrica que busca centralizar la identidad de los ciudadanos. La meta es clara: usar datos biométricos para autenticar a las personas de forma inequívoca en transacciones financieras y trámites públicos y privados. La confianza se está construyendo desde la raíz de la identidad.

"En América Latina, la evolución se enfoca en la identidad digital como el corazón de la confianza".

La brecha generacional: educando en la era digital

Si bien se han realizado avances, todavía persiste el desafío de educar al mercado. Mientras los nativos digitales adoptan estas nuevas formas de confianza, una parte considerable de la población prefiere los métodos tradicionales.

En Sovos, nos enfocamos en demostrar por qué un código es más seguro que una firma en papel, y por qué nuestra solución no solo es más eficiente, sino también más confiable. Como profesionales del sector, nuestro reto es seguir innovando para que cada clic, cada huella dactilar y cada línea de código refuerce la seguridad y permita que las personas y empresas interactúen de forma segura, sin importar la distancia.

“En Sovos nos enfocamos en demostrar por qué un código es más seguro que una firma en papel, y por qué nuestra solución no es solo más eficiente, sino también más confiable”

5. Documentos y contratos que trabajan por ti: automatización que genera confianza

Por Óscar Gómez, Senior Product Manager, gestión de documentos y contratos digitales

Oscar Gómez nos cuenta cómo la gestión documental digital va mucho más allá de almacenar archivos: automatiza procesos, asegura trazabilidad y genera confianza en cada etapa del ciclo de vida de documentos y contratos.

Generar confianza en el ciclo de vida de la gestión documental es un arte y un beneficio sustancial que se deriva del uso de una solución robusta y bien desarrollada. El verdadero valor de la gestión documental está en la suma de sus partes, desde la creación de un documento o contrato, a su firma y almacenamiento.

Un gestor de documentos y contratos digitales bien diseñado permite que las empresas ganen mucho más que velocidad. Por cierto, reduce tiempos y errores, pero también se aumenta el control, minimiza riesgos críticos, estandariza versiones y facilita la colaboración entre áreas.

Cada documento se convierte en un activo estratégico, que se puede seguir en tiempo real y que entrega información útil para tomar decisiones más acertadas.

Un flujo integrado, de la firma a la trazabilidad

Todo esto es posible gracias a la integración de múltiples funcionalidades en un solo flujo. Los documentos o contratos se crean, organizan y envían en una cadencia predeterminada para su firma digital. Una vez firmados, ingresan automáticamente a un sistema de trazabilidad que registra cada visualización, modificación o envío, con fecha y hora.

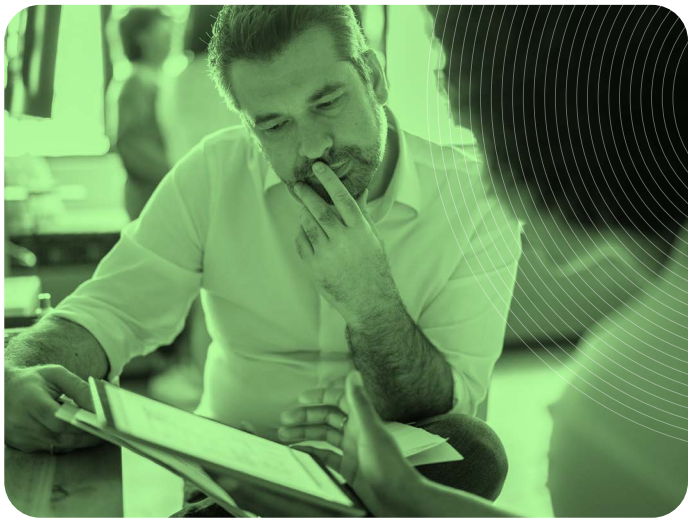
Incluso se puede integrar verificación de identidad en el flujo, para garantizar que quien firma es quien dice (y quien debe) ser y proporcionar así mayor seguridad al proceso.

“Un gestor de documentos y contratos bien diseñado permite a las empresas ganar velocidad y minimizar riesgos críticos”

Todo queda vinculado a un almacenamiento seguro, que garantiza la integridad del documento. Así, la validez legal no es una promesa: es una consecuencia directa de cómo está construido el sistema.

Y ese diseño también tiene un impacto directo en la forma en que las empresas enfrentan sus obligaciones legales. Hoy, los marcos normativos son más exigentes y cambiantes, y las soluciones tecnológicas deben estar preparadas para ayudar a cumplir con esos requerimientos.

Automatizar procesos no solo ahorra tiempo: también facilita auditorías, asegura control de versiones y deja un registro claro y confiable de quién hizo qué, cuándo y cómo.



Escalar sin perder el foco en la confianza

Ahora bien, no basta con que una solución funcione bien en un contexto local. Vivimos en un entorno global y digital, donde las plataformas deben ser capaces de escalar sin perder rendimiento. Por eso es fundamental contar con una infraestructura sólida, multilenguaje, compatible con distintas normativas de protección de datos y, ojalá, con la capacidad de conectarse a sistemas empresariales como CRM o ERP. En los mercados donde aún no se cuenta con presencia directa, las alianzas estratégicas con socios locales se vuelven una forma efectiva de adaptar las soluciones al entorno.

También se vislumbra un camino hacia contratos más inteligentes. Contratos que no solo se firman digitalmente, sino que se gestionan solos. Imaginemos acuerdos que se renuevan automáticamente cuando se cumplen ciertas condiciones, sin necesidad de intervención humana, salvo para verificar la identidad del firmante.

La inteligencia artificial ya permite resumir documentos, extraer datos clave, anticipar vencimientos o detectar riesgos de incumplimiento. Cada vez será más común que estas herramientas se conecten con plataformas internas de las organizaciones, creando flujos de trabajo sin interrupciones.

De documentos a contratos: una diferencia esencial

Toda esta evolución tecnológica tiene un eje común: la confianza. Para que las organizaciones puedan operar de forma eficiente y segura en entornos digitales, necesitan soluciones que aseguren autenticidad, integridad y trazabilidad. La gestión documental cumple un rol central en ese sentido: permite transparencia en las operaciones, protege los datos sensibles y ofrece certeza jurídica en cada paso.

Y hay una diferencia importante que no se puede perder de vista: no es lo mismo gestionar documentos que gestionar contratos. Mientras lo primero se enfoca en organizar y almacenar archivos, haciendo la operación más ordenada y eficiente, lo segundo implica manejar acuerdos legales vivos. Hablamos de creación, negociación, aprobación, firma, seguimiento de obligaciones y renovaciones.

Cada documento o contrato tiene un ciclo de vida propio y requiere herramientas especializadas para acompañarlo desde el inicio hasta su cumplimiento.

Esta manera de trabajar también mejora las relaciones entre empresas y clientes o proveedores. En el caso de los contratos digitales, todo queda claro, firmado y trazado. No hay lugar para dudas ni demoras. La transparencia y la agilidad fortalecen la confianza entre las partes, y eso -en cualquier negocio- es un valor incalculable.

El diferencial de Sovos: cumplimiento como ADN

Desde mi rol en Sovos, he visto cómo la gestión contractual se transforma cuando el cumplimiento normativo está en el centro. Nuestras soluciones no solo permiten firmar documentos: garantizan validez legal, protección de datos, escalabilidad y seguridad. Eso es lo que nos diferencia. Creamos herramientas en las que nuestros clientes pueden confiar plenamente, porque están diseñadas para cumplir desde el primer clic hasta el último.

> **“En el caso de los contratos digitales, todo queda claro, firmado y trazado”**

6. Regulación en movimiento: normas que habilitan, no que frenan

Por Andrés Landerretche, Director, Regulatory Analysis and Design

La confianza digital necesita reglas que impulsen, no que frenen. En Latinoamérica, nos dice Andrés Landerretche, avanzar hacia marcos regulatorios que habiliten la innovación es clave para una transformación digital segura e inclusiva.

En el mundo actual, la confianza no es estática: evoluciona con la expectativa y demandas de los usuarios.

La transformación digital ha redefinido la manera en que operan las sociedades modernas. Dentro de este proceso, la digitalización de la confianza se ha vuelto un factor central para habilitar interacciones seguras en entornos remotos. Pero ¿cómo están respondiendo los marcos normativos a esta necesidad creciente en Latinoamérica?

Del mundo al detalle: el marco global de la confianza digital

La digitalización es un fenómeno global, aunque su ritmo y profundidad varían de una región a otra. En Latinoamérica, los avances normativos han sido significativos, particularmente en lo que respecta a firmas electrónicas, certificados digitales y leyes de protección de datos. Sin embargo, la región aún enfrenta el desafío de anticipar y regular nuevos desarrollos como la inteligencia artificial, cuya aplicación -por ahora- se encuentra principalmente guiada por marcos éticos más que legales.

> **“La región aún enfrenta el desafío de anticipar y regular nuevos desarrollos como la inteligencia artificial”**

Al respecto, países como Estados Unidos y los miembros de la Unión Europea están liderando la conversación, con propuestas regulatorias que pretenden establecer lineamientos generales para luego avanzar en normativas más específicas. En Latinoamérica, por ejemplo, Chile ha dado un primer paso con un proyecto de ley que busca definir un marco de acción para la inteligencia artificial. Sin duda, un hito inicial que deberá perfeccionarse para entregar mayor certeza jurídica y que debe ser replicado.

Confianza en entornos digitales: identidad, biometría y verificación

En el ámbito digital, la certeza depende de la confianza, y confiar implica verificar con seguridad la identidad de quien está al otro lado de una transacción. Para ello, los mecanismos de verificación de identidad, especialmente los que incorporan factores biométricos, se vuelven esenciales. Aunque aún no existe una regulación específica sobre este punto en la región, hay esfuerzos incipientes y grandes referentes internacionales como el reglamento eIDAS, de la Unión Europea, donde debemos mirar.

Este es un campo muy dinámico, que va cambiando a velocidad vertiginosa, y, en este escenario, los marcos normativos suelen ir detrás. Primero está la innovación, las nuevas ideas, nuevos conceptos, que una vez que empiezan a masificarse, llevan a los legisladores a pensar cuáles serían los marcos regulatorios. Como está pasando con la inteligencia artificial, por ejemplo, donde en Chile, si bien aún no existe una ley de inteligencia artificial plenamente vigente, hay un proyecto de ley en avanzado estado de tramitación -presentado por el Gobierno en mayo de 2024- que busca establecer un marco normativo para el desarrollo, uso y regulación de los sistemas de inteligencia artificial (IA) en el país.

En términos generales, México, Perú y Chile son países que llevan la delantera en la región. La implementación de documentos de identidad modernos -con chips o elementos biométricos- facilita el despliegue de soluciones de verificación de identidad robustas. En algunos casos, como México y Perú, incluso se han abierto bases de datos biométricos oficiales para consulta bajo ciertos acuerdos, lo que habilita procesos más seguros y ágiles.

Interoperabilidad regulatoria: una meta aún lejana

Uno de los grandes desafíos para la región es la interoperabilidad regulatoria. Actualmente, cada país opera con su propia normativa, generando un entorno fragmentado. Avanzar hacia la interoperabilidad requiere voluntad política, madurez institucional y colaboración internacional.

Un ejemplo concreto de avance es el diálogo bilateral entre Chile y Argentina, que ya trabajan en acuerdos para reconocer la validez mutua de firmas electrónicas. No obstante, pensar en una interoperabilidad regional integral es todavía lejano, ya que implica ceder ciertos grados de soberanía normativa, un paso complejo en un contexto donde las prioridades nacionales están enfocadas en temas más urgentes como salud, educación y reactivación económica.

> **“La regulación ideal debe funcionar como un habilitador, no como una traba”**

Lo que viene: regulación como habilitador

La regulación ideal debe funcionar como un habilitador, no como una traba. Es decir, debe promover la adopción tecnológica garantizando altos estándares de seguridad, pero también, cuidando la experiencia del usuario y reduciendo fricciones. Este enfoque regulatorio equilibrado es clave para permitir el desarrollo de flujos digitales seguros y eficientes en múltiples industrias.

En ese sentido, los proveedores de servicios de confianza desempeñan un rol esencial como habilitadores de la transformación digital. Son los responsables de que múltiples procesos -firmas, validaciones, gestiones documentales- se realicen de forma remota, segura y simple. Pero también tienen una responsabilidad mayor: salir al mercado a ofrecer confianza, y para ello, deben garantizar el cumplimiento de los más altos estándares de seguridad y calidad.

Sector privado y regulación: velocidades distintas

Un reto adicional es la desalineación entre la velocidad del sector privado y la del regulador. En la mayoría de los casos, la innovación tecnológica corre más rápido que las leyes. Además, la actitud de los gobiernos hacia el sector privado influye directamente en este dinamismo: algunos Estados desconfían del involucramiento empresarial, mientras que otros -por necesidad o visión estratégica- se apoyan fuertemente en actores privados.

Casos como los de México y Perú son ejemplos de colaboración público-privada, donde empresas privadas certifican transacciones fiscales, como la factura electrónica, otorgándoles validez legal ante las autoridades. Este modelo podría ser replicado en otras industrias, como la verificación de identidad, impulsando la masificación de soluciones innovadoras.

La digitalización de la confianza es un fenómeno irreversible. Pero su consolidación requiere más que tecnología: demanda marcos normativos sólidos, colaboración público-privada, interoperabilidad gradual y un enfoque que entienda la confianza como un activo dinámico. Latinoamérica ha avanzado, pero aún enfrenta desafíos estructurales y políticos que debe superar para habilitar una transformación digital plena, inclusiva y segura.

Por eso, es esencial que las regulaciones no actúen como freno, sino como habilitadores: deben establecer un equilibrio entre seguridad, experiencia de usuario y libertad para innovar. Aquellos países que logren este balance tendrán más posibilidades de atraer inversión, desarrollar tecnología y ofrecer servicios digitales confiables.

> **“Diseñamos nuestras soluciones cumpliendo con los más altos estándares internacionales”**

Sovos y la confianza digital

En Sovos, entendemos que nuestra responsabilidad es mayor: salimos al mercado a ofrecer confianza. Por ello, diseñamos nuestras soluciones cumpliendo con los más altos estándares internacionales y adaptándonos a los marcos normativos de cada país. Acompañamos a empresas y gobiernos en su transformación digital, facilitando procesos seguros, eficientes e intuitivos.

Como socios estratégicos en procesos de digitalización, reafirmamos nuestro compromiso con la promoción de la confianza como pilar fundamental para habilitar un entorno digital virtuoso. Un entorno donde las normativas garanticen protección equitativa para todos los actores, fomentando la transparencia, la equidad y la integridad. Solo mediante marcos regulatorios claros, éticos y coherentes será posible construir un ecosistema digital más inclusivo, accesible e interconectado.

7. Tu dato, tu derecho: privacidad en la era del consentimiento digital

Por Roberto Guerrero, Counsel, LATAM Commercial

La privacidad ya no es opcional: es un derecho que exige garantías claras y mecanismos efectivos. En un contexto de creciente regulación en Latinoamérica -nos comenta Roberto Guerrero- proteger los datos es clave para construir confianza digital.

Hoy, la protección de datos personales es uno de los pilares fundamentales de la confianza digital. En el último año hemos sido testigos de un auge normativo en la región: Ecuador promulgó su ley en 2023, Argentina, Uruguay y Colombia avanzan hacia marcos alineados con el GDPR, Perú publicó un reglamento que representa una actualización significativa del marco normativo peruano y en Chile, la nueva Ley 21.719 -que entrará en vigor en diciembre de 2026 y reforma la actual Ley 19.628- nos enfrenta a un periodo de adecuación que representa un desafío importante para todos los actores involucrados.

A pesar de las diferencias entre legislaciones, todas estas normas comparten principios de origen europeo y apuntan hacia un mismo horizonte: transformar en forma efectiva el dato, de un simple insumo en un derecho, dotado de salvaguardas efectivas.

Sin embargo, no basta con tener una ley. Es indispensable contar con mecanismos concretos de cumplimiento (compliance) orientados a prevenir el fraude. La normativa chilena, por ejemplo, propone un modelo voluntario de prevención de infracciones que contempla análisis de riesgos, protocolos de control, canales de denuncia y la designación de un Data Privacy Officer (DPO), entre otros elementos clave.

Estas herramientas no deben verse como una carga burocrática, sino como una estrategia fundamental para mitigar riesgos y evitar sanciones, que podrían alcanzar hasta el 4% de los ingresos anuales de una empresa en el peor de los casos. En este escenario, el compliance, la proactividad y la educación emergen como los pilares que sustentan la confianza en el ecosistema digital.

“La protección de datos personales es uno de los pilares fundamentales de la confianza digital”

Cuando hablamos de servicios de confianza -como la firma electrónica, la verificación de identidad o la gestión de contratos digitales- entramos de lleno en el tratamiento de datos sensibles, como la biometría. En estos casos, el consentimiento digital adquiere un rol crucial: debe ser libre, informado, específico e inequívoco. Solo bajo esas condiciones, el titular recupera el control sobre sus datos y puede ejercer plenamente sus derechos: acceso, rectificación, supresión, oposición, portabilidad y bloqueo.

Cada vez que se solicite un dato como el DNI, el rostro o la huella para validar una identidad o firmar digitalmente, se debe informar con absoluta claridad:

- Qué datos se solicitan.
- Por qué se requieren.
- Cuánto tiempo serán conservados.
- Qué medidas de seguridad (técnicas y organizativas) se aplicarán para protegerlos.
- Cómo se pueden ejercer los derechos de acceso, rectificación, supresión, revocación, portabilidad y bloqueo.

Uno de los grandes desafíos actuales es promover la educación ciudadana en materia de protección de datos personales. Esta es una condición indispensable para reducir la brecha de conocimiento entre las organizaciones -en especial las empresas- y los ciudadanos. En contextos donde predomina una baja alfabetización digital, el reto se duplica: no solo se requiere el diseño de interfaces accesibles y comprensibles, sino también un esfuerzo sostenido en educación comunitaria.

“No podemos exigir a los usuarios que comprendan conceptos técnicos o jurídicos complejos”

No podemos exigir a los usuarios que comprendan conceptos técnicos o jurídicos complejos; es nuestra responsabilidad, como organizaciones que tratamos datos personales, presentar la información en formatos claros: infografías, videos explicativos o mensajes simples al momento de solicitar consentimiento, además de ofrecer canales de atención accesibles y personalizados.

En esta tarea, el rol de profesionales especializados, asociaciones, organismos públicos y privados, y los propios gobiernos, es esencial. Todos deben actuar como agentes activos de concientización, acercando la protección de datos a la ciudadanía desde un enfoque inclusivo, pedagógico y cultural. Solo con este esfuerzo conjunto podremos construir una verdadera cultura de respeto a la privacidad.

Buenas prácticas como base

Análisis de brechas (gap analysis): punto de partida para identificar riesgos en cada proceso de tratamiento.

Política de protección de datos clara: acompañada de la designación de un DPO, programas de seguridad con controles de acceso y encriptación, y protocolos de respuesta ante incidentes.

Privacy by design: integrar a los equipos legales desde la etapa de diseño de cualquier producto o servicio que involucre datos personales, previene incumplimientos y evita costosas correcciones posteriores.

Educación continua: capacitar a todos los equipos en cultura de datos, para que cada colaborador entienda su rol en la protección de la información.

La inteligencia artificial (IA) y el big data traerán complejidades adicionales al tratamiento masivo de datos, pero también, herramientas para identificar patrones y mitigar riesgos. Hacia el futuro, es previsible un entorno más regulado, donde converjan normativas sobre IA, ciberseguridad y protección de datos en marcos coherentes y con agencias responsables bien definidas.

También veremos una tendencia creciente hacia la transparencia: los titulares de datos exigirán saber con claridad qué información se recolecta, con qué finalidad y por cuánto tiempo será utilizada.

En un mundo cada vez más marcado por los deepfakes, la automatización y el uso intensivo de algoritmos, la educación digital -tanto de la ciudadanía como del sector empresarial- será decisiva. Este conocimiento será crucial para determinar si las nuevas normativas lograrán proteger efectivamente los derechos fundamentales, o si quedarán relegadas a meras formalidades. El éxito dependerá, una vez más, de una transformación cultural profunda y del rol activo de las instituciones.

En aquellos países donde aún no existen pilares robustos en materia de protección de datos, ni una cultura de privacidad ni autoridades con facultades sancionatorias, el resultado será inevitable: mal uso de datos, perfilamientos abusivos, consentimientos forzados y brechas de seguridad. Por eso es urgente que los países se alineen con estándares internacionales, fomenten una sistemática educación al respecto y creen agencias especializadas con atribuciones claras.

Sector privado y regulación: velocidades distintas

Al final del día, la privacidad no es un obstáculo, sino un habilitador de la confianza digital. Cuando un usuario sabe que sus datos son gestionados con transparencia, seguridad y trazabilidad, se genera un círculo virtuoso: el usuario confía, la empresa cumple, y ese ecosistema favorece la innovación sin sacrificar derechos. Para lograrlo, es clave una cultura ciudadana basada en el uso responsable de los datos.

En Sovos, entendemos que la protección de datos va mucho más allá del cumplimiento legal: es la piedra angular de cualquier servicio que aspire a construir confianza. Nuestro compromiso es acompañar a las organizaciones en cada etapa del proceso de adecuación normativa, con soluciones que integran la privacidad desde el diseño, aseguran cumplimiento y garantizan una experiencia de usuario fluida. En definitiva, incorporar la privacidad a las operaciones de nuestros clientes no solo es una necesidad, sino un verdadero valor añadido.

Confianza, la base de lo digital: conclusiones

A lo largo de estas conversaciones, emerge una verdad poderosa: la confianza ya no es un valor intangible, sino una capacidad concreta que se construye con tecnología, diseño, regulación, protección de datos y visión estratégica.

Desde la firma electrónica y la verificación de identidad hasta la gestión automatizada de contratos y otros documentos digitales, cada solución que forma parte del ecosistema de servicios de confianza de Sovos responde a una necesidad esencial: garantizar que lo que ocurre en el mundo digital sea tan creíble, válido y seguro como en el mundo físico.

Pero también hay algo más profundo: el deseo de generar experiencias inclusivas, fluidas, interoperables. De ir más allá del cumplimiento y aportar verdadero valor a las personas y las organizaciones.

En Sovos, esta visión se concreta en el trabajo diario de equipos que no solo desarrollan tecnología, sino que se preguntan constantemente cómo humanizarla, cómo anticipar el futuro regulatorio y cómo acompañar a cada cliente en su propio camino hacia la transformación digital.

Lo que se abre, entonces, no es solo un nuevo escenario tecnológico, sino una nueva cultura digital basada en relaciones de confianza, habilitadas por soluciones sólidas, éticas y escalables.

Estamos apenas comenzando. Y lo que viene, creemos, es una confianza más visible, más diseñada y más decisiva que nunca.

> **“Lo que se abre es una nueva cultura digital basada en relaciones de confianza”**

SOVOS

Siete Miradas Sobre la Transformación de la Confianza en el Entorno Digital

Sobre tecnología, regulaciones y protección de datos en los servicios de confianza

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