

II FORO DE ANDORRA

Alianzas público-privadas para la
transición digital en Iberoamérica

SERVICIOS DIGITALES
ANDORRA LA VELLA, 28 Y 29 DE OCTUBRE DE 2025



FORO DE ANDORRA
Alianzas Público-Privadas
para la Transición Digital



FORO DE ANDORRA
Alianzas Público-Privadas
para la Transición Digital

BENVINGUTS,

El II Foro Digital de Andorra nace en un momento decisivo para la agenda digital iberoamericana. La aceleración tecnológica, y en particular el impacto de la inteligencia artificial, está redefiniendo la competitividad, la gobernanza y la forma en que nuestras sociedades se organizan y se relacionan. En este contexto, la cooperación entre instituciones públicas, sector privado y sociedad civil deja de ser una opción para convertirse en una condición indispensable.

Organizado conjuntamente por la Secretaría General Iberoamericana y el Gobierno de Andorra, este Foro forma parte del programa oficial de la Cumbre Iberoamericana. Se consolida como un espacio estable de diálogo y acción orientado a garantizar que la transformación digital sea inclusiva, ética y centrada en las personas. Desde Andorra, se reafirma el compromiso con un multilateralismo fuerte, capaz de traducir la innovación tecnológica en bienestar, cohesión social y prosperidad compartida.

Las reflexiones aquí recogidas reflejan la convicción de que la tecnología solo tiene sentido si mejora la vida de las personas y si el proceso de transformación es compartido, basado en la confianza, la cooperación y los valores que unen al espacio iberoamericano.

ÍNDICE

01	La oportunidad (y al mismo tiempo el desafío) de forjar alianzas público-privadas eficaces para la digitalización iberoamericana	Pág. 06
-----------	---	----------------

02	Programa	Pág. 08
-----------	-----------------	----------------

03	BLOQUE ADMINISTRACIÓN PÚBLICA	Pág. 10
-----------	--------------------------------------	----------------

Visión Iberoamericana en clave de ponencias (Bloque I)

3.1	“La identidad digital: oportunidades en el ámbito de la administración electrónica” por Nacho Alamillo, director general, ASTREA	Pág. 12
------------	---	----------------

3.2	“La transformación digital como palanca de progreso económico y social” por Alberto Gago, director de la Oficina España Digital 2030 e Internacionalización, Gobierno de España	Pág. 13
------------	--	----------------

3.3	“Innovación abierta e IA: una alianza público-privada en Brasil” por Camila Medeiros, directora de Innovación, Escola Nacional de Administração Pública (ENAP), Brasil	Pág. 13
------------	---	----------------

3.4	“Sí, se puede implementar Data Governance en el mundo de Agentic AI sin tener que empezar de nuevo” por Manuel Gómez, arquitecto principal de TI, Informática INC	Pág. 14
------------	--	----------------

3.5	“El futuro de la gobernanza digital en Iberoamérica” por Víctor Muñoz, fundador y socio, ARGIA	Pág. 14
------------	---	----------------

04	BLOQUE SERVICIOS FINANCIEROS	Pág. 15
-----------	-------------------------------------	----------------

Visión Iberoamericana en clave de ponencias (Bloque II)

4.1	“Fintech en Iberoamérica: regulación, retos y oportunidades” por Francisco del Olmo, subdirector responsable de Fintech y Ciberseguridad, Comisión Nacional del Mercado de Valores (CNMV)	Pág. 18
------------	--	----------------

4.2	“El futuro de los pagos digitales: innovación y tendencias” por Alejandro Banegas, director de Desarrollo de Negocio, Mastercard	Pág. 18
------------	---	----------------

4.3	“Tendencias en fintech” por Adrián Peribáñez, director de Innovación y Transformación Digital, Andbank	Pág. 19
------------	---	----------------

05	BLOQUE SERVICIOS DE SALUD	Pág. 19
-----------	----------------------------------	----------------

Visión Iberoamericana en clave de ponencias (Bloque III)

5.1	“La transformación digital en el sector social y sanitario: oportunidades para una mejor atención ciudadana” por Jesús Domínguez, director de Estrategia de Industria, Salesforce	Pág. 22
------------	--	----------------

5.2	“La inteligencia artificial en sanidad: ganando tiempo para una atención más humana” por José Rodríguez, director, Oracle Health	Pág. 22
------------	---	----------------

5.3	“El PERTE para la Salud de Vanguardia: impulsando la innovación en salud” por Silvia López, directora general, PERTE Salud de Vanguardía, Gobierno de España	Pág. 23
------------	---	----------------

5.4 “Reestructuración de los Sistemas de Salud en Iberoamérica: innovación, equidad y alianzas público-privadas” por Cristian Mazza, presidente, Asociación Latinoamericana de Sistemas Privados de Salud (ALAMI)

Pág. 23

06 BLOQUE EDUCACIÓN

Pág. 24

Visión Iberoamericana en clave de ponencias (Bloque IV)

6.1 “La Estrategia Iberoamericana para la Transformación Digital de la educación superior” por Félix García Lausín, coordinador del Espacio del Conocimiento Iberoamericano, SEGIB

Pág. 27

6.2 “Transformación digital sostenible en Educación Superior. El rol de MetaRed” por Esther Lucía Sánchez, rectora de la Universidad Nacional de Cuyo y presidenta de MetaRed

Pág. 27

07 BLOQUE CIBERSEGURIDAD

Pág. 28

Visión Iberoamericana en clave de ponencias (Bloque V)

7.1 “Implementación de la Carta Iberoamericana de Principios y Derechos de los Entornos Digitales (CIPDED)” por Alejandro Kawabata, director de Asuntos Jurídicos e Institucionales, SEGIB

Pág. 30

7.2 “Nación Frontera: IA y Ciberseguridad” por Alberto Pinedo, National Technology and Security Officer, Microsoft

Pág. 31

7.3 “Seguridad de productos, certificación y confianza digital” por Estefanía, Centro Criptológico Nacional de España (CCN-CERT), Ministerio de Defensa del Gobierno de España

Pág. 32

7.4 “Panorama de las amenazas cibernéticas: relatos desde la trinchera” por David Grout, CTO EMEA y director técnico, Google

Pág. 33

08 CONCLUSIONES PARA EL AVANCE DIGITAL IBEROAMERICANO

Pág. 34

Apostar por la tecnología es apostar por la competitividad. Solo con un proceso moderno y una administración abierta a la innovación podemos ayudar a nuestro tejido empresarial a crear, a adaptarse y a liderar en un mundo cada vez más digital.



Marc Rossell
Ministro de Función Pública,
Transformación Digital y
Telecomunicaciones de
Andorra

Vivimos este momento decisivo en el que la inteligencia artificial no es solo una revolución tecnológica, sino una oportunidad histórica para redefinir una colaboración internacional, solidaria y tangible.



María González Veracruz
Secretaria de Estado de
Digitalización e Inteligencia
Artificial del Gobierno de España

En un momento en que el mundo se enfrenta a grandes turbulencias, conflictos geopolíticos, fenómenos meteorológicos extremos y crisis económicas, Andorra, más que nunca, es una firme defensora de un multilateralismo fuerte e inclusivo.



Imma Tor
Ministra de Asuntos
Exteriores de Andorra

Solamente los países que logren que el mundo privado y el mundo público empujen en la misma dirección van a tener éxito. Los desafíos son tan grandes que ni los actores públicos ni los actores privados por sí solos los pueden afrontar.



Andrés Allamand
Secretario General
Iberoamericano

01 LA OPORTUNIDAD Y EL DESAFÍO

de forjar alianzas público-privadas eficaces para la digitalización iberoamericana

Por Jaume Gaytán

Responsable de Economía y Empresa, Secretaría General Iberoamericana

y David Vicente

Director del Programa de Transformación Digital de Andorra

El **Foro Digital de Andorra**, parte del programa oficial de la Cumbre Iberoamericana, se concibió desde su primera edición como un espacio de reflexión aplicada sobre uno de los vectores más determinantes del desarrollo contemporáneo: la transición digital. No como un fenómeno estrictamente tecnológico, sino como un proceso estructural con implicaciones profundas en la competitividad económica, la calidad institucional, la cohesión social y la forma en que los Estados se relacionan con la ciudadanía.

El primer encuentro, celebrado en Andorra la Vella en junio de 2024, situó este debate en el centro de la agenda iberoamericana, con un énfasis claro en las infraestructuras digitales como condición habilitante para la conectividad universal y como base material de cualquier estrategia de digitalización inclusiva.

Aquella primera edición permitió constatar que sin inversión sostenida en infraestructura, sin marcos regulatorios estables y sin cooperación entre actores públicos y privados, la digitalización corre el riesgo de convertirse en un nuevo factor de desigualdad. La brecha digital, lejos de reducirse de manera automática con el avance tecnológico, tiende a reproducirse allí donde no existen capacidades institucionales, financiación adecuada y modelos de gobernanza que alineen incentivos y responsabilidades.

Sin inversión sostenida en infraestructura, sin marcos regulatorios estables y sin cooperación entre actores públicos y privados, la digitalización corre el riesgo de convertirse en un nuevo factor de desigualdad.

El I Foro de 2024 dejó, por tanto, una hoja de ruta inicial y, al mismo tiempo, una convicción sobre la necesidad de dar continuidad a este espacio de diálogo.

Su segunda edición se inscribe en ese ejercicio de continuidad, pero responde también a un contexto sensiblemente distinto. La aceleración de la inteligencia artificial, la creciente concentración del poder tecnológico y la fragmentación del orden internacional han introducido nuevas capas de complejidad en la conversación sobre digitalización. Hoy, la transición digital ya no se limita a la expansión del acceso o al despliegue de redes, sino que atraviesa de forma directa el funcionamiento de las administraciones públicas, los sistemas educativos y sanitarios, los servicios financieros y los mecanismos de protección de derechos en entornos digitales.

En este escenario, se ha ampliado deliberadamente el foco. Sin abandonar la cuestión de las infraestructuras, la conversación se desplaza hacia los usos, los impactos y las decisiones de política pública que están configurando el ecosistema digital en Iberoamérica. La relación entre ciudadanía y administración, la inclusión financiera a través de soluciones digitales, la aplicación de la inteligencia artificial en salud y educación, o la ciberseguridad como condición de confianza colectiva, se convierten en ejes centrales del debate. Se trata de ámbitos donde la digitalización no es una promesa abstracta, sino una experiencia concreta que afecta a la vida cotidiana de millones de personas.

Este enfoque responde a la idea de que la transición digital es, ante todo, un proceso de transformación institucional y social. La tecnología puede mejorar el desempeño del Estado, ampliar el acceso a servicios esenciales y generar nuevas oportunidades económicas, pero solo si se inserta en marcos de

gobernanza claros y orientados al interés público. La calidad de la digitalización depende menos de la sofisticación técnica que de la capacidad de articular alianzas público-privadas eficaces, de generar confianza ciudadana y de garantizar que los beneficios del cambio tecnológico se distribuyan de manera equitativa.

El II Foro se celebra, además, en un momento en que el multilateralismo atraviesa tensiones evidentes. La emergencia de nuevos bloques de poder tecnológico y la competencia por definir estándares, normas y modelos de gobernanza digital plantean desafíos específicos para regiones como Iberoamérica. Frente a dinámicas de fragmentación, el espacio iberoamericano cuenta con activos singulares: una comunidad lingüística amplia, una tradición de cooperación política y una visión compartida que sitúa a las personas y a los derechos en el centro de la transformación digital. Estos activos no garantizan resultados por sí solos, pero ofrecen una base sólida para construir posiciones comunes y respuestas coordinadas.

La calidad de la digitalización depende menos de la sofisticación técnica que de la capacidad de articular alianzas público-privadas eficaces, de generar confianza ciudadana y de garantizar que los beneficios del cambio tecnológico se distribuyan de manera equitativa.

En este sentido, se consolida como un espacio estable para traducir principios en prácticas. La presencia de responsables públicos, empresas tecnológicas, entidades financieras, academia y organismos internacionales permite contrastar visiones, identificar cuellos de botella y explorar modelos replicables. No se trata de alcanzar consensos formales, sino de generar un lenguaje común y una comprensión compartida de los retos que enfrenta la región en su transición digital.

Organizado conjuntamente por la Secretaría General Iberoamericana y el Gobierno de Andorra, reafirma la vocación de continuidad iniciada en 2024 y refuerza el papel de Andorra como punto de encuentro para el diálogo iberoamericano. No solo revisa avances y aprendizajes, sino que plantea

preguntas estratégicas sobre el tipo de digitalización que la región necesita y sobre los mecanismos de cooperación que pueden hacerla viable.

Las páginas que siguen recogen las principales ideas y debates que atravesaron los días 28 y 29 de octubre de 2025. No constituyen una relatoría exhaustiva de las intervenciones, sino un ejercicio de síntesis y análisis orientado a facilitar una lectura de la transición digital en Iberoamérica. Un proceso en curso, abierto, que exige liderazgo público, compromiso privado y una mirada compartida sobre el papel de la tecnología en el desarrollo sostenible de nuestras sociedades.



02 PROGRAMA II FORO DE ANDORRA

ANDORRA LA VELLA, 28 Y 29 DE OCTUBRE DE 2025

DÍA 1

Inauguración institucional

La apertura del Foro contó con la participación de **Marc Rossell** (ministro de Función Pública, Transformación Digital y Telecomunicaciones de Andorra), **María González Veracruz** (secretaria de Estado de Digitalización e Inteligencia Artificial del Gobierno de España), **Imma Tor** (ministra de Asuntos Exteriores de Andorra), y **Andrés Allamand** (Secretario General Iberoamericano).



Bloque I: Administración pública

Intervinieron **Nacho Alamillo** (ASTREA), **Alberto Gago** (Gobierno de España), **Camila Medeiros** (Escola Nacional de Administração Pública de Brasil), **Manuel Gómez Ramos** (Informatica Inc.) y **Víctor Muñoz** (ARGIA).

La mesa redonda sobre la evolución de la relación ciudadanía-administración reunió a **Albert Gomà** (Gobierno de Andorra), **Camila Medeiros** (ENAP - Brasil), **José Raúl Solares Chiu** (Gobierno de Guatemala) y **Leo Van-Troi Mercedes** (Gobierno de República Dominicana), moderada por **David Vicente** (director del Programa de Transformación Digital de Andorra).



Bloque II: Servicios financieros

Participaron **Francisco del Olmo** (CNMV), **Alejandro Banegas** (Mastercard) y **Adrián Peribáñez** (Andbank), quienes analizaron la evolución regulatoria, la innovación en medios de pago y las oportunidades de desarrollo del ecosistema fintech en Iberoamérica.

La mesa sobre fintech como herramienta de inclusión reunió a **Carlos Salinas** (MoraBanc), **Eloi Noya** (Instituto de Estudios Financieros) y **Gabriela Eguidazu** (Fundación Microfinanzas BBVA), moderada por **David Cerqueda** (director general de la Autoridad Financiera de Andorra).



02

PROGRAMA II FORO DE ANDORRA

ANDORRA LA VELLA, 28 Y 29 DE OCTUBRE DE 2025

DÍA 2

Bloque III: Salud

Intervinieron **Jesús Domínguez (Salesforce)**, **José Rodríguez (Oracle Health)**, **Silvia López (PERTE para la Salud de Vanguardia – Gobierno de España)** y **Cristian Mazza (ALAMI)**, quienes abordaron la aplicación de inteligencia artificial, la transformación de la atención sanitaria y los modelos de colaboración público-privada en el sector.

La mesa de soluciones digitales en salud contó con la participación de **Ángel Borque (Fundación Instituto de Investigación Sanitaria de Aragón)**, **Javier Mínguez (Bit & Brain)**, **Jaume Sellarès (Colegio Oficial de Médicos de Barcelona)** y **Sergi Iglesia (Sociedad Catalana de Salud Digital)**, moderada por **Josep Escoriza (director general de la Caja Andorrana de Seguridad Social)**.



Bloque IV: Educación

El bloque educativo reunió a **Félix García Lausín (SEGIB)** y **Esther Lucía Sánchez (Universidad Nacional de Cuyo y MetaRed)**, quienes presentaron iniciativas para impulsar la digitalización sostenible de la educación superior en el espacio iberoamericano.

En la mesa sobre incorporación de soluciones digitales en centros educativos participaron **Albert Maluquer (Gobierno de Andorra)**, **Fabrizio Gagliardi (Barcelona Supercomputing Centre)**, **Jaime García (INCAE Business School)**, **Marc Escolà (Universidad Europea de Andorra)** y **Pastora Martínez Samper (Universitat Oberta de Catalunya)**, moderada por **Juli Minoves (rector de la Universitat d'Andorra)**.



Bloque V: Ciberseguridad

En el bloque final intervinieron **Alejandro Kawabata (SEGIB)**, **Alberto Pinedo (Microsoft)**, **David Grout (Google)** y **Estefanía, representante del Centro Criptológico Nacional de España (CCN-CERT)**.

La mesa sobre protección de los países frente a amenazas digitales reunió a **Andreu Tomàs (Var Group Andorra)**, **Grete Raidma (INSAFE-INHOPE)**, **Jaroslav Ponder (Unión Internacional de Telecomunicaciones)**, **Jordi Celades** y **Tomás Clemente (Amazon Web Services)**, moderada por **Jordi Ubach (responsable de la Agencia de Ciberseguridad de Andorra)**.



03 BLOQUE ADMINISTRACIÓN PÚBLICA



De la identificación al acceso efectivo a derechos

La identidad digital se ha consolidado como el umbral a partir del cual se redefine la relación entre ciudadanía y Estado en el entorno digital. Funciona como infraestructura pública que habilita el ejercicio de derechos, el acceso a servicios y la construcción de confianza institucional. En este marco, la identidad deja de ser un componente técnico para convertirse en una pieza central del contrato entre administraciones y ciudadanos.

Su despliegue adquiere pleno sentido cuando se integra en arquitecturas públicas coherentes y de alcance sistémico. La experiencia acumulada muestra que los sistemas fragmentados, desarrollados por organismos aislados, tienden a reproducir barreras de acceso, duplicidades y desconfianza. La identidad digital opera de forma efectiva cuando se concibe como un activo común del Estado, reconocido transversalmente y sostenido en el tiempo.

La escala resulta determinante. Los modelos de identificación únicos permiten simplificar la interacción administrativa, reducir fricciones y habilitar servicios interoperables. Al mismo tiempo, plantean exigencias elevadas en materia de gobernanza del dato, seguridad y protección de la privacidad. La calidad de la infraestructura condiciona directamente la calidad de los servicios que se construyen sobre ella.

La identidad digital incorpora una dimensión jurídica insoslayable. Su capacidad transformadora depende del reconocimiento legal pleno en procedimientos administrativos y relaciones con terceros.

Sin ese reconocimiento, la digitalización queda limitada a una capa superficial que no altera la lógica de fondo de la administración. El valor jurídico de la identidad digital permite cerrar el ciclo entre reconocimiento, derecho y servicio.

La confianza emerge como resultado de este diseño institucional. La ciudadanía confía cuando comprende cómo funciona el sistema, qué datos se utilizan y con qué finalidad. La privacidad por diseño y el control efectivo del dato se convierten en condiciones estructurales para sostener esa confianza en el tiempo.



La identidad digital es una condición necesaria, pero no suficiente, si no está acompañada de un marco legal y de capacidades institucionales.

José Raúl Solares Chiu, viceministro de Comunicación, Gobierno de Guatemala

La transformación digital como capacidad del Estado

La digitalización de la administración pública se vincula de forma directa con la capacidad del Estado para responder a desafíos económicos y sociales persistentes. En contextos marcados por bajo crecimiento, informalidad y limitaciones fiscales, la transformación digital aparece como una palanca para mejorar eficiencia, transparencia y calidad institucional.

El impacto de la digitalización no se limita a la modernización de trámites. La interoperabilidad de sistemas, la trazabilidad de procesos y el uso estratégico de datos fortalecen la rendición de cuentas y reducen espacios de discrecionalidad. La administración digital refuerza así la legitimidad institucional y la confianza ciudadana.

La transición digital exige una visión por capas. Infraestructura, conectividad, habilidades digitales y servicios avanzados deben desarrollarse de forma simultánea. La introducción de tecnologías sofisticadas en entornos con brechas estructurales amplias corre el riesgo de reproducir desigualdades

existentes bajo formatos nuevos.

La capacidad estatal se expresa también en la continuidad de las políticas. La transformación digital requiere liderazgo político, estabilidad institucional y coordinación interadministrativa. Los avances sostenidos dependen menos de proyectos puntuales que de marcos estratégicos compartidos y evaluables.

La transformación del sector público es sistémica: arranca con el funcionariado, se consolida en la organización y culmina en un sistema público renovado, a través de competencias, cultura, procesos e infraestructura para la innovación.

Camila Medeiros, directora de Innovación, Escola Nacional de Administração Pública (ENAP), Brasil

Innovación pública, cooperación y desarrollo de capacidades

La innovación en el sector público se consolida como una condición necesaria para sostener la transformación digital. Esta innovación se articula en torno a personas, organizaciones y sistemas, y no únicamente a tecnologías. La formación de funcionarios, la cultura organizativa y la apertura a la experimentación determinan la capacidad de incorporar soluciones digitales con impacto real.

La colaboración con el sector privado y la academia amplía el acceso a conocimiento y capacidades que el Estado no concentra internamente. Esta cooperación adquiere sentido cuando se estructura en torno a objetivos públicos claros y reglas de gobernanza definidas. La innovación abierta permite incorporar soluciones externas sin diluir la responsabilidad institucional.

La contratación pública emerge como un instrumento estratégico. A través de los procesos de compra se definen estándares, escalabilidad e interoperabilidad. La forma en que el Estado contrata condiciona la arquitectura tecnológica que adopta y su capacidad para evolucionar en el tiempo. El desarrollo de capacidades internas resulta indispensable para evitar dependencias excesivas. La innovación pública sostenible combina acceso a

soluciones externas con fortalecimiento del conocimiento y la gestión dentro de la administración.

Datos, inteligencia artificial y responsabilidad institucional

La incorporación de inteligencia artificial en la administración pública desplaza el foco hacia la gobernanza de los datos. La calidad, contextualización e interoperabilidad de la información determinan el alcance real de estas tecnologías. Sin infraestructuras de datos sólidas, la inteligencia artificial amplifica sesgos y dependencias.

La escasez de datos representativos de los contextos iberoamericanos introduce riesgos adicionales. Los modelos entrenados con información ajena a la realidad local pueden generar decisiones poco ajustadas a las necesidades del territorio. La gobernanza del dato se convierte así en una cuestión de soberanía institucional.

La regulación de la inteligencia artificial plantea desafíos específicos. La proliferación de iniciativas y normativas inconexas puede generar fragmentación y dificultar la adopción responsable de tecnologías emergentes. Los enfoques graduales y sectoriales permiten adaptar las reglas a distintos niveles de madurez institucional.

La responsabilidad pública en el uso de inteligencia artificial exige transparencia, explicabilidad y capacidad de supervisión. La tecnología se integra en la administración como herramienta de apoyo a la decisión, no como sustituto del juicio institucional.

La calidad de los datos condiciona directamente la capacidad de ofrecer servicios digitales fiables y completos a la ciudadanía.

Albert Gomà, director del Departamento de Transformación Digital del Gobierno de Andorra

Gobernanza digital y cooperación regional

La gobernanza digital adquiere una dimensión regional en Iberoamérica. La fragmentación normativa y tecnológica limita la interoperabilidad y reduce el impacto de las inversiones. La cooperación entre países aparece como una vía para construir estándares comunes, compartir aprendizajes y evitar dependencias estructurales.

La región cuenta con activos diferenciales relevantes, como una comunidad lingüística amplia y una tradición de cooperación. Estos elementos ofrecen una base para articular posiciones comunes en debates globales sobre datos, inteligencia artificial y derechos digitales.

La gobernanza digital integra dimensiones tecnológicas, institucionales y económicas. Las decisiones sobre infraestructuras, centros de datos y modelos de desarrollo digital tienen implicaciones a largo plazo sobre competitividad y sostenibilidad. El liderazgo político resulta clave para orientar estas decisiones hacia objetivos públicos.

Iberoamérica tiene la capacidad de liderar la administración digital y posicionarse como referencia a nivel mundial.

Leo Van-Troi Mercedes, jefe de Gabinete, Oficina Gubernamental de Tecnologías de la Información y Comunicación, Gobierno de República Dominicana

Servicios públicos, experiencia ciudadana e inclusión

La transformación digital redefine la experiencia de la ciudadanía con la administración. La interoperabilidad entre sistemas permite reducir cargas administrativas y ofrecer servicios más simples y coherentes. La digitalización orientada al usuario se convierte en un criterio central de calidad institucional.

La inclusión atraviesa este proceso de forma transversal. La existencia de brechas digitales obliga a mantener canales presenciales y estrategias de acompañamiento. La administración digital amplía derechos cuando se diseña con criterios de accesibilidad y apoyo a los colectivos más

vulnerables. La relación futura entre ciudadanía y Estado se construye sobre confianza, capacidad institucional y equidad. La digitalización de la administración pública se consolida como una transformación estructural de su arquitectura y de su vínculo con la sociedad.

VISIÓN IBEROAMERICANA EN CLAVE DE PONENCIA

(BLOQUE I)

3.1 “La identidad digital: oportunidades en el ámbito de la administración electrónica” por Nacho Alamillo, director general, ASTREA

La identidad digital se ha convertido en el punto de acceso real a los derechos en el entorno digital. No es una capa técnica adicional ni un servicio más dentro del catálogo administrativo, sino la infraestructura que permite al ciudadano existir jurídicamente frente al Estado cuando la interacción deja de ser presencial. Sin identidad digital, la administración electrónica se queda en una digitalización superficial, incapaz de sostener servicios interoperables, fiables y escalables.

La clave no está únicamente en autenticar, sino en dar continuidad jurídica a la relación entre persona y administración. La identidad digital permite que el ciudadano no tenga que demostrar una y otra vez quién es, qué derechos tiene o qué información ya obra en poder del Estado. En ese sentido, la identidad funciona como un habilitador sistémico. Como se formuló con claridad durante la ponencia, “la identidad digital no es un servicio más, es la base sobre la que se construyen todos los demás”.

Esta base solo es sólida cuando se concibe como un bien público. Los sistemas fragmentados, desarrollados por organismos aislados, tienden a reproducir silos, duplicidades y fricción administrativa. La identidad digital, en cambio, exige una lógica de Estado, no de proyecto. Requiere gobernanza común, reconocimiento transversal y una arquitectura pensada para durar. Sin ese enfoque, lo digital se limita a replicar en línea los mismos obstáculos del mundo analógico.

El valor jurídico de la identidad es otro de los elementos centrales. La administración electrónica no puede apoyarse en soluciones que carezcan de efectos legales plenos. Si la identidad digital no

tiene reconocimiento jurídico, los trámites digitales quedan subordinados a verificaciones posteriores, certificados adicionales o pasos presenciales. En términos claros, “sin identidad digital con valor jurídico, lo digital se queda en una capa cosmética”.

La confianza aparece así como una consecuencia, no como un punto de partida. No basta con pedir confianza al ciudadano; esta se construye mediante diseños comprensibles, reglas claras y control efectivo sobre los datos personales. La identidad digital debe incorporar privacidad por diseño y por defecto, garantizando que el ciudadano conserve el control sobre su información y entienda cómo y para qué se utiliza. En esa lógica, la identidad no solo habilita servicios, sino que redefine la relación de poder entre administración y ciudadanía.

Entendida de este modo, la identidad digital deja de ser una discusión tecnológica para convertirse en una decisión institucional. Es el mecanismo que permite al Estado reconocer al ciudadano de forma coherente en el entorno digital y, al mismo tiempo, ofrecer servicios más simples, más seguros y más justos. Sin ella, la administración electrónica no es transformadora.

3.2 “La transformación digital como palanca de progreso económico y social” por Alberto Gago, director de la Oficina España Digital 2030 e Internacionalización, Gobierno de España

La transformación digital del Estado solo adquiere sentido cuando se entiende como una herramienta para ampliar la capacidad institucional y no como un ejercicio de modernización tecnológica aislado. Digitalizar no equivale a innovar si no altera la forma en que el Estado recauda, invierte, regula y presta servicios. En contextos marcados por bajo crecimiento, informalidad persistente y limitaciones fiscales, la digitalización aparece como uno de los pocos vectores capaces de actuar simultáneamente sobre eficiencia administrativa, productividad y cohesión social.

El punto de partida es incómodo, pero necesario. Durante décadas, gran parte de América Latina ha mostrado dificultades para sostener trayectorias de crecimiento estables. A ello se suma una debilidad estructural del Estado para financiar transformaciones de largo plazo. En este marco, la transformación digital no puede presentarse como una solución mágica, pero sí como una condición

habilitante. Como se planteó durante la ponencia, “la transformación digital no va a resolver por sí sola los problemas estructurales, pero sin ella es imposible resolverlos”.

La clave está en abordar la transición digital por capas. Hablar de inteligencia artificial, automatización o servicios avanzados sin haber resuelto brechas básicas de conectividad y habilidades digitales implica construir sobre cimientos frágiles. La digitalización del Estado requiere simultáneamente infraestructura, alfabetización digital y rediseño de procesos. De lo contrario, corre el riesgo de reproducir desigualdades existentes bajo una apariencia tecnológica.

La administración pública digital también se vincula directamente con la calidad institucional. La interoperabilidad, la trazabilidad de los trámites y el uso inteligente de los datos reducen espacios de discrecionalidad y fortalecen la transparencia. En ese sentido, el *e-Government* no es solo una cuestión de eficiencia operativa, sino un componente central de legitimidad democrática y confianza ciudadana.

Entendida así, la transformación digital deja de ser un proyecto sectorial para convertirse en una política de Estado. Requiere liderazgo político, continuidad en el tiempo y coordinación entre niveles de gobierno. Solo desde esa lógica puede convertirse en una verdadera palanca de progreso económico y social.

3.3 “Innovación abierta e IA: una alianza público-privada en Brasil” por Camila Medeiros, Directora de Innovación, Escola Nacional de Administração Pública (ENAP), Brasil

La innovación en el sector público no ocurre por acumulación de tecnología, sino por transformación de capacidades. Digitalizar procesos sin transformar a las personas y a las organizaciones conduce, en el mejor de los casos, a mejoras marginales. La experiencia brasileña muestra que la innovación pública exige un enfoque sistémico que combine cultura organizativa, desarrollo de competencias y marcos normativos habilitantes.

Brasil ha construido en los últimos años un ecosistema amplio de innovación pública, con más de 200 laboratorios distribuidos en distintos niveles de gobierno. Estos espacios no funcionan como

unidades tecnológicas aisladas, sino como dispositivos para resolver problemas públicos desde la experimentación. La innovación se concibe como un proceso que “parte del individuo, pasa por la organización y alcanza al sistema público como un todo”.

En este marco, la inteligencia artificial ocupa un lugar relevante, pero subordinado a objetivos públicos claros. La IA no sustituye la capacidad del Estado; la amplifica cuando existe gobernanza, talento y supervisión. El punto de partida es reconocer una limitación estructural: “el Estado no tiene todo el conocimiento ni toda la tecnología”. De ahí la importancia de la cooperación con el mercado y la academia como principio estructural, no como excepción.

La innovación abierta permite al sector público acceder a soluciones desarrolladas fuera de la administración, siempre que existan reglas claras y capacidad interna para evaluarlas e integrarlas. Los contratos innovadores, las govtech y las startups se convierten así en aliados estratégicos, no en proveedores tradicionales. Esta lógica exige repensar la contratación pública y los mecanismos de compra como instrumentos de política pública.

Un Estado innovador no es el que adopta más tecnología, sino el que aprende, experimenta y coopera mejor. La innovación, entendida como capacidad institucional, no es un proyecto puntual, sino una condición que debe institucionalizarse para sostener la transformación digital en el tiempo.

3.4 “Sí, se puede implementar Data Governance en el mundo de Agentic AI sin tener que empezar de nuevo” por Manuel Gómez, arquitecto principal de TI, Informática INC

La expansión de la inteligencia artificial en el ámbito público ha desplazado el foco de los algoritmos hacia los datos. Sin datos de calidad, gobernados y contextualizados, la adopción de IA corre el riesgo de reproducir sesgos, dependencias y decisiones opacas. El reto principal no es técnico, sino institucional: gobernar cómo se producen, almacenan y utilizan los datos en el sector público.

Uno de los problemas más estructurales señalados es la invisibilidad cultural y lingüística. Menos del uno por ciento de los datos utilizados para entrenar grandes modelos lingüísticos proceden del español. Esto implica que muchos sistemas se entrenan con

realidades ajenas al contexto iberoamericano. Como se expresó con claridad, “no es que los modelos no entiendan el español; es que no tienen datos suficientes para entender nuestra realidad”.

La gobernanza de datos se convierte así en una condición previa para cualquier estrategia de inteligencia artificial responsable. No se trata únicamente de disponer de grandes volúmenes de información, sino de contar con datos curados, interoperables y sujetos a reglas claras de uso. Sin esta base, la IA puede amplificar desigualdades existentes o generar decisiones difíciles de auditar.

En el plano regulatorio, se advirtió sobre los riesgos de una aproximación precipitada. La proliferación de iniciativas legislativas inconexas puede frenar la innovación y generar fragmentación. La regulación de la IA no puede apoyarse en un único criterio, sino que debe adaptarse a sectores y niveles de madurez distintos. Regular sin resolver brechas estructurales puede terminar siendo contraproducente.

Gobernar la IA implica, en última instancia, tomar decisiones políticas sobre inversión, soberanía, sostenibilidad y modelo de desarrollo. La tecnología no es neutral y su adopción en el sector público exige liderazgo, capacidad institucional y visión de largo plazo.

3.5 “El futuro de la gobernanza digital en Iberoamérica” por Víctor Muñoz, fundador y socio, ARGIA

La gobernanza digital se ha convertido en uno de los principales desafíos estratégicos para Iberoamérica. La transformación digital avanza a ritmos desiguales y, sin coordinación, corre el riesgo de fragmentarse en marcos normativos incompatibles y arquitecturas tecnológicas inconexas. El problema no es la falta de iniciativas, sino su dispersión.

Reducir la gobernanza digital a un ejercicio regulatorio resulta insuficiente. La gobernanza incluye talento, infraestructura, sostenibilidad, financiamiento y cooperación internacional. Como se señaló durante la ponencia, “la gobernanza va mucho más allá de la regulación”. Centrarse exclusivamente en normas puede ocultar déficits estructurales que condicionan la adopción tecnológica real.

Uno de los riesgos más evidentes es la proliferación de marcos regulatorios inconexos, impulsados en

ocasiones por incentivos políticos de corto plazo. Este proceso puede desembocar en “un Frankenstein de modelos dispersos” que dificulta la interoperabilidad y la cooperación regional. Frente a ello, se plantea la necesidad de avanzar hacia principios comunes y estándares compartidos, adaptados a la realidad de la región.

Iberoamérica cuenta con activos diferenciales que pueden jugar a favor: una comunidad lingüística amplia, una tradición de cooperación y una visión que sitúa a las personas y los derechos en el centro del debate tecnológico. Estos elementos ofrecen una base sólida para construir posiciones comunes en discusiones globales sobre inteligencia artificial, datos y derechos digitales.

La gobernanza digital iberoamericana no se construye desde la competencia normativa, sino desde la colaboración. Las alianzas público-privadas, la cooperación internacional y el papel de los bancos de desarrollo aparecen como mecanismos clave para movilizar inversión y capacidades. Traducir tecnología en desarrollo y cohesión social exige una visión compartida y sostenida en el tiempo.

04 BLOQUE SERVICIOS FINANCIEROS



Un sistema financiero bajo presión estructural

El sistema financiero se encuentra en una fase de transformación acelerada impulsada por la digitalización de los medios de pago, la aparición de nuevos intermediarios y la incorporación de tecnologías que alteran la forma en que se intercambia valor. Esta transformación no responde a una evolución incremental, sino a una

reconfiguración de la infraestructura financiera que sostiene la actividad económica cotidiana.

Los servicios financieros se sitúan en un punto de fricción permanente entre innovación, regulación e inclusión. La velocidad del cambio tecnológico convive con marcos normativos diseñados para otros ritmos y con realidades sociales marcadas por desigualdades persistentes. En este contexto, la cuestión central gira en torno a la capacidad de gobernar la transición sin comprometer estabilidad, acceso y confianza.

Una de cada dos personas a las que atendemos tiene algún grado de pobreza digital. O bien no tienen acceso a un dispositivo, o no saben utilizarlo, o no tienen recursos para acceder a un plan de datos.

Gabriela Eguidazu, directora de Innovación para el crecimiento inclusivo, Fundación Microfinanzas BBVA

La arquitectura de los pagos y la experiencia del usuario

La evolución de los sistemas de pago ilustra con claridad esta transformación estructural. La proliferación de métodos, plataformas y dispositivos ha ampliado las opciones disponibles para usuarios y comercios, pero también ha incrementado la complejidad operativa del ecosistema. Pagos instantáneos, *wallets*, transferencias basadas en cuenta, tarjetas virtuales y soluciones biométricas conviven en paralelo, generando fricciones y costes ocultos.

La tendencia dominante apunta hacia modelos de orquestación, donde distintas soluciones se integran de forma transparente. La experiencia del usuario se consolida como criterio central de diseño. La tecnología aporta valor cuando reduce pasos, simplifica decisiones y opera de manera casi invisible. La fragmentación, en cambio, penaliza la adopción y limita la escalabilidad.

La identidad digital emerge como un componente estructural de esta arquitectura. La capacidad de autenticar de forma segura y reutilizable condiciona la interoperabilidad entre plataformas y la movilidad

del usuario dentro del sistema financiero digital. El control de la identidad se vincula así con el control de la experiencia y de los datos asociados a las transacciones.

Wallets, plataformas y finanzas integradas

Los *wallets* han evolucionado desde instrumentos de pago hacia plataformas multifuncionales que integran finanzas, consumo y servicios. Esta convergencia redefine la relación entre usuario y sistema financiero, desplazando el punto de acceso desde entidades tradicionales hacia entornos digitales más amplios.

En algunos mercados, esta lógica ha cristalizado en modelos de superapps. En otros, el avance es más gradual, pero la dirección es clara: las finanzas se integran en la vida cotidiana y dejan de presentarse como un destino específico. Esta integración reduce fricciones y amplía el alcance de los servicios financieros, aunque introduce nuevos retos en términos de gobernanza y competencia.

La inclusión de pequeños comercios en este ecosistema sigue siendo un desafío relevante. Barreras de coste, complejidad tecnológica y conocimiento limitan la adopción, especialmente en economías con alta informalidad. Soluciones que convierten dispositivos comunes en terminales de pago reducen estas barreras, pero no las eliminan por completo.

Fintech más allá del relato: penetración limitada, impacto desigual

El sector fintech ocupa un lugar destacado en el discurso sobre transformación financiera, aunque su peso real en el conjunto del sistema sigue siendo limitado. Su impacto se concentra en segmentos específicos, especialmente pagos, inversión y ciertos nichos de crédito, mientras otros ámbitos permanecen prácticamente inalterados. La penetración desigual del modelo fintech obliga a matizar los relatos de disrupción total. La innovación financiera introduce eficiencia y especialización, pero convive con estructuras tradicionales que mantienen un papel central. La relación entre banca y fintech evoluciona hacia esquemas de complementariedad y colaboración, más que de sustitución.

Latinoamérica aparece como un espacio

especialmente dinámico en este proceso. La menor bancarización histórica ha facilitado la adopción de soluciones digitales, impulsada por la necesidad de acceso más que por la sofisticación tecnológica. Esta expansión convive con retos significativos en regulación, escalabilidad y sostenibilidad del modelo.

Regulación como habilitador (o freno) de la innovación

La regulación atraviesa de forma transversal la transformación de los servicios financieros. Los marcos normativos condicionan la velocidad, la dirección y el alcance de la innovación. Lejos de actuar únicamente como freno, la regulación define perímetros de actuación y aporta certidumbre al ecosistema.

La experiencia comparada muestra que la claridad normativa facilita la adopción responsable de nuevas soluciones. Regímenes de licencias, *sandboxes* regulatorios y marcos específicos para activos digitales permiten canalizar la innovación dentro de límites definidos. La heterogeneidad del ecosistema financiero exige aproximaciones diferenciadas según riesgos, escala y tipo de actividad.

La protección del consumidor adquiere especial relevancia en entornos digitalizados. Interfaces simplificadas y procesos automatizados pueden ocultar riesgos difíciles de evaluar para el usuario medio. La supervisión debe adaptarse a estas dinámicas para preservar la confianza sin limitar el acceso.

Inclusión financiera: tecnología sin alfabetización no es inclusión

La inclusión financiera constituye uno de los principales argumentos a favor de la digitalización de los servicios financieros. El acceso a medios de pago digitales, cuentas básicas y productos financieros adaptados amplía las oportunidades económicas de amplios sectores de la población. Sin embargo, la tecnología no garantiza inclusión por sí misma.

La brecha digital introduce límites claros. Falta de conectividad, dispositivos adecuados y competencias digitales condicionan la capacidad de participar en la economía digital. La alfabetización financiera y digital se consolida como dimensión inseparable de cualquier estrategia de inclusión.

Las experiencias compartidas muestran que el diseño centrado en el usuario y el acompañamiento en la adopción resultan determinantes. Soluciones basadas en interfaces simples, asistencia automatizada y adaptación a contextos locales amplían el impacto de la digitalización sin sacrificar sofisticación tecnológica.

Criptomonedas estables (Stablecoins): eficiencia, adopción real y tensiones geopolíticas

La expansión de las criptomonedas estables introduce una capa adicional de complejidad en el sistema financiero digital. Estos instrumentos han superado el ámbito especulativo y se utilizan de forma creciente para transferencias de valor cotidianas, especialmente en contextos de alta inflación o restricciones cambiarias.

El crecimiento de las criptomonedas estables plantea implicaciones directas para la soberanía monetaria y la política económica. La hegemonía de determinadas divisas en el entorno digital refuerza asimetrías existentes y desplaza el control del valor hacia infraestructuras privadas globales. Las economías con monedas menos estables enfrentan riesgos adicionales de sustitución monetaria.

La respuesta institucional a este fenómeno sigue abierta. Las iniciativas de monedas digitales de bancos centrales avanzan a ritmos desiguales y conviven con soluciones privadas ya operativas. El equilibrio entre eficiencia, control y estabilidad constituye uno de los grandes dilemas de la transición financiera digital.

Tokenización y nuevos mercados de activos

La tokenización de activos reales aparece como uno de los vectores con mayor potencial transformador a medio plazo. La representación digital de activos financieros y no financieros abre la puerta a mercados más líquidos, accesibles y transparentes. Este proceso puede alterar la forma en que se construyen señales económicas y se canaliza la inversión. La posibilidad de fraccionar activos, reducir intermediación y ampliar la base de inversores introduce dinámicas nuevas en la relación entre economía real y sistema financiero.

La adopción de estos modelos depende de marcos regulatorios claros, infraestructuras seguras y capacidad institucional para supervisar mercados

emergentes. La tokenización amplía oportunidades, pero también exige una gobernanza adaptada a su complejidad.



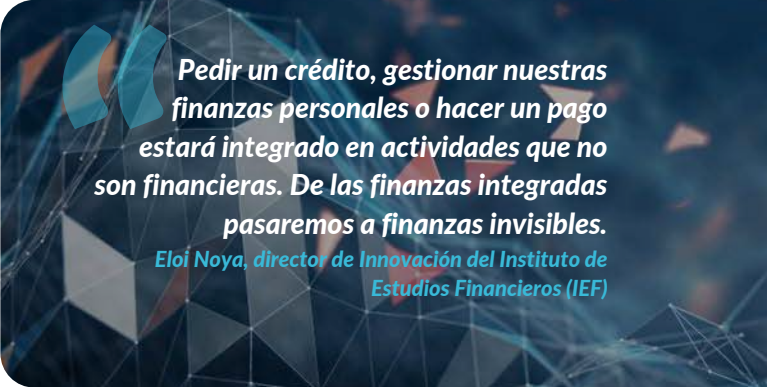
La banca tradicional tiene la gran oportunidad de actuar como puente entre estos dos mundos: el financiero tradicional y la nueva economía digital. Dar entrada a la nueva riqueza digital hacia el mundo tradicional y viceversa.

*Carlos Salinas, director de Activos Digitales y Fintech
MoraBanc*

Finanzas integradas e invisibles: el desplazamiento del banco como interfaz

La evolución del sistema financiero apunta hacia una integración progresiva de las finanzas en otras actividades económicas y sociales. Los servicios financieros se incorporan como capas funcionales dentro de plataformas no financieras, reduciendo su visibilidad como productos independientes.

Este desplazamiento redefine el papel de los intermediarios tradicionales. La banca mantiene un rol relevante en segmentos especializados, mientras que las operaciones cotidianas se integran en entornos digitales más amplios. La confianza, la gestión del riesgo y la regulación continúan siendo funciones centrales, aunque ejercidas en arquitecturas distintas.



Pedir un crédito, gestionar nuestras finanzas personales o hacer un pago estará integrado en actividades que no son financieras. De las finanzas integradas pasaremos a finanzas invisibles.

Eloi Noya, director de Innovación del Instituto de Estudios Financieros (IEF)

Gobernar la transición financiera digital

El Bloque II converge en una idea central: la transformación digital de los servicios financieros avanza más rápido que los marcos de gobernanza

que deberían acompañarla. Innovación, inclusión y soberanía monetaria se entrelazan en un equilibrio aún inestable.

El desafío no reside en frenar la transformación, sino en orientarla. La capacidad para articular regulación, infraestructura y diseño centrado en el usuario determinará si la digitalización financiera refuerza la estabilidad y la equidad o amplifica desigualdades existentes.

VISIÓN IBEROAMERICANA EN CLAVE DE PONENCIA

(BLOQUE II)

4.1 “Fintech en Iberoamérica: regulación, retos y oportunidades” por Francisco del Olmo, director general de Estrategia y Asuntos Internacionales, CNMV

La transformación digital de los servicios financieros ha desplazado el centro del debate desde la innovación tecnológica hacia la capacidad de los marcos regulatorios para ordenar un ecosistema cada vez más complejo. La fintech ya no es un fenómeno emergente, sino un actor integrado en el sistema financiero, aunque con un peso real todavía limitado. Su impacto no se mide tanto por volumen como por su capacidad para tensionar reglas, tiempos y responsabilidades.

Uno de los elementos clave es la asimetría entre velocidad tecnológica y capacidad regulatoria. La innovación avanza de forma exponencial, mientras que la regulación opera por definición de manera incremental. Esta brecha genera un espacio de fricción permanente que obliga a los supervisores a equilibrar dos objetivos en tensión: proteger la estabilidad del sistema y no sofocar la innovación. En este contexto, la regulación deja de ser un freno y se convierte en un instrumento de ordenación. “Regular no es impedir que las cosas pasen, es decidir cómo pasan”.

La experiencia europea muestra que la claridad normativa puede actuar como un habilitador. Marcos como MiCA, los *sandboxes* regulatorios o los regímenes de licencias específicas permiten canalizar la innovación dentro de perímetros definidos. Sin embargo, se advierte contra la ilusión de una regulación única aplicable a todos los casos. El ecosistema fintech es heterogéneo por

naturaleza y requiere aproximaciones diferenciadas según riesgos, escala y tipo de actividad.

Otro punto central es la protección del consumidor. La digitalización amplía el acceso, pero también introduce nuevas opacidades. Productos financieros complejos, interfaces simplificadas y procesos automatizados pueden ocultar riesgos difíciles de evaluar para el usuario medio. De ahí la insistencia en que “la innovación no puede ir por delante de la comprensión”, especialmente en contextos de inclusión financiera.

Desde una perspectiva iberoamericana, la cooperación entre supervisores emerge como una necesidad estratégica. La fragmentación regulatoria puede generar arbitrajes indeseados y limitar la escalabilidad de soluciones útiles. En este sentido, la regulación fintech se plantea como un ejercicio de gobernanza compartida, donde la coordinación internacional resulta tan relevante como la normativa nacional.

4.2 “El futuro de los pagos digitales: innovación y tendencias” por Alejandro Banegas, Director de Desarrollo de Negocio, Mastercard

El sistema de pagos se encuentra en el epicentro de la transformación financiera digital. Lejos de tratarse únicamente de un cambio en los medios de pago, lo que está en juego es la arquitectura misma que sostiene el intercambio de valor en la economía digital. La proliferación de nuevos métodos, plataformas y dispositivos ha ampliado las opciones disponibles, pero también ha introducido una complejidad creciente.

Uno de los fenómenos más visibles es la fragmentación del ecosistema. Pagos instantáneos, *wallets*, tarjetas virtuales, biometría y transferencias basadas en cuenta conviven en paralelo, generando fricción para comercios y usuarios. Frente a esta dispersión, se plantea la necesidad de avanzar hacia modelos de orquestación, donde distintas soluciones se integren de forma transparente. “El reto no es crear más métodos de pago, sino conseguir que todos funcionen juntos”.

La experiencia del usuario se convierte así en el criterio central. La tecnología solo aporta valor cuando simplifica. En este sentido, el avance de la tokenización, la biometría y la autenticación pasiva apunta hacia un modelo donde el pago se diluye en

la experiencia, reduciendo pasos y aumentando seguridad. La idea de que “la mejor tecnología es la que no se ve” atraviesa toda la reflexión.

Sin embargo, la innovación no es homogénea. Millones de pequeños comercios siguen fuera del ecosistema digital, no por falta de interés, sino por barreras de coste, complejidad o conocimiento. Soluciones como *Tap to Pay* buscan reducir estas barreras, convirtiendo dispositivos cotidianos en puntos de acceso al sistema financiero.

El futuro de los pagos digitales se define, por tanto, en la intersección entre innovación tecnológica, interoperabilidad y diseño centrado en el usuario. No se trata solo de eficiencia, sino de construir infraestructuras de confianza que permitan participar en la economía digital sin fricciones ni exclusiones.

4.3 “Tendencias en fintech” por Adrián Peribáñez, director de Innovación y Transformación Digital, Andbank

El ecosistema fintech ha alcanzado un grado de madurez que obliga a revisar muchos de los supuestos iniciales sobre disrupción y cambio sistémico. Lejos de sustituir al sistema financiero tradicional, la fintech opera como una capa que introduce eficiencia, especialización y nuevas lógicas de relación con el usuario, aunque con un peso agregado todavía limitado.

Uno de los datos más reveladores es la penetración real del sector. A pesar de su visibilidad, la fintech representa alrededor del 3% del mercado financiero global. Esta cifra invita a relativizar el discurso de ruptura total y a centrar el análisis en los segmentos donde su impacto es más tangible, especialmente en pagos, inversión y ciertos nichos de crédito. “La fintech no ha cambiado todo, pero ha cambiado cosas muy concretas”. Latinoamérica aparece como un espacio especialmente dinámico. La menor bancarización histórica ha facilitado la adopción de soluciones digitales, no tanto por innovación pura, sino por necesidad. Allí donde la banca tradicional no llegaba, la fintech ha encontrado espacio para operar. Sin embargo, esta expansión convive con desafíos relevantes en materia de regulación, escalabilidad y sostenibilidad del modelo.

Otro eje clave es la evolución hacia las finanzas embebidas. Los servicios financieros dejan de

presentarse como productos independientes y se integran en otras experiencias digitales. El usuario no “va al banco”, sino que accede a funciones financieras dentro de plataformas de comercio, movilidad o servicios. Esta invisibilización redefine el papel de las entidades financieras y desplaza el foco desde el producto hacia la experiencia.

Las tendencias fintech apuntan así a una mayor integración, especialización y colaboración con el sistema tradicional. El desafío es articular un ecosistema donde ambos aporten valor sin generar nuevas exclusiones.

05 BLOQUE SERVICIOS DE SALUD



La salud como frontera crítica de la transformación digital

La digitalización de la salud se ha convertido en uno de los terrenos más sensibles y estratégicos de la transición digital. A diferencia de otros sectores, aquí la innovación no se mide únicamente en términos de eficiencia o productividad, sino por su capacidad para mejorar resultados clínicos, reducir desigualdades y sostener sistemas sanitarios sometidos a una presión creciente. El debate se desplaza hacia las condiciones bajo las cuales la tecnología puede incorporarse sin fragmentar el sistema, sin generar exclusión y sin debilitar el control público.

Las intervenciones del Bloque III convergen en un diagnóstico compartido: los sistemas de salud arrastran problemas estructurales previos a la digitalización. Envejecimiento poblacional, aumento de la cronicidad, escasez de profesionales sanitarios

y presión financiera configuran un escenario en el que los modelos tradicionales muestran límites evidentes. En este contexto, la tecnología aparece como una palanca necesaria, aunque incapaz de resolver por sí sola estas tensiones.

La digitalización de la salud requiere una aproximación sistémica, apoyada en gobernanza del dato y en una redefinición profunda de los procesos asistenciales. La tecnología adquiere sentido cuando forma parte del diseño estructural del sistema y no como respuesta puntual a déficits acumulados.

La ética es un concepto que no debemos perder de vista ante esta avalancha de tecnología.

Jaume Sellarès, vicepresidente del Colegio Oficial de Médicos de Barcelona (CoMB)

De los datos clínicos al conocimiento accionable

Uno de los ejes centrales del bloque fue el papel del dato sanitario como activo estratégico. La salud genera volúmenes masivos de información, cuyo valor depende de la capacidad para integrarla, interpretarla y utilizarla en la toma de decisiones. La fragmentación de sistemas, la falta de interoperabilidad y la persistencia de silos organizativos continúan siendo barreras estructurales.

El desafío trasciende lo técnico. La integración de datos clínicos, administrativos y poblacionales plantea cuestiones de gobernanza, privacidad y legitimidad de uso. El foco se desplaza hacia la capacidad de disponer de información pertinente en el momento adecuado y orientada a decisiones concretas. La inteligencia artificial y la analítica avanzada amplifican este potencial, al tiempo que elevan los riesgos en ausencia de reglas claras.

La transformación de los datos en conocimiento clínico y organizativo emerge como un factor crítico para la sostenibilidad del sistema. La predicción de riesgos, la gestión poblacional y la personalización de tratamientos dependen de infraestructuras de datos robustas y compartidas. Sin estas condiciones, la innovación queda confinada a experiencias

aisladas sin impacto sistémico.

Cuando quieres ayudar al paciente, necesitas comprender que la tecnología la tiene que utilizar él, y aquí hay una enorme brecha digital que tienes que ser capaz de cerrar.

Javier Mínguez, cofundador de Bit & Brain

Inteligencia artificial en salud: promesa clínica y responsabilidad institucional

La inteligencia artificial ocupa un lugar creciente en la agenda de la salud digital. Sus aplicaciones abarcan desde el apoyo al diagnóstico hasta la optimización de flujos asistenciales. Este potencial convive con la necesidad de evitar enfoques simplificadores que atribuyen a la tecnología capacidades que exceden su alcance real.

La IA no reemplaza al profesional sanitario ni corrige automáticamente los déficits estructurales del sistema. Su valor se expresa cuando contribuye a liberar tiempo clínico, mejorar la calidad de la decisión y reducir variabilidades injustificadas en la práctica asistencial. La tecnología resulta pertinente cuando refuerza la capacidad de cuidado y no cuando introduce nuevas capas de complejidad operativa.

La adopción de IA en salud exige marcos claros de responsabilidad institucional. La trazabilidad de las decisiones, la explicabilidad de los modelos y la validación clínica constituyen condiciones imprescindibles. La dependencia de modelos entrenados con datos externos introduce riesgos de sesgo y desalineación con los contextos locales, lo que refuerza la centralidad de la gobernanza del dato como condición previa.

El hecho de que el paciente se sienta parte del equipo también puede beneficiar a la hora de conseguir los objetivos terapéuticos que se buscan.

Santiago Sánchez, analista del área de Sistemas de Información, SAAS - Servei Andorrà Atenció Sanitària

Interoperabilidad y continuidad asistencial

La continuidad asistencial representa uno de los principales desafíos de los sistemas de salud contemporáneos. La fragmentación entre niveles asistenciales, proveedores y territorios dificulta una atención centrada en el paciente. La digitalización ofrece herramientas para reducir esta brecha cuando se apoya en estándares compartidos y en una voluntad institucional sostenida.

Las historias clínicas electrónicas, los sistemas de receta digital y las plataformas de intercambio de información constituyen avances relevantes. Su impacto depende de la integración en una lógica de sistema que permita articular la atención a lo largo del tiempo y entre distintos actores. La interoperabilidad incorpora una dimensión organizativa y política que exige acuerdos, redefinición de competencias y alineación de incentivos.

La experiencia acumulada muestra que, sin interoperabilidad, los sistemas tienden a fragmentarse en islas funcionales. Los principales obstáculos no suelen ser tecnológicos, sino culturales y regulatorios, y su superación requiere liderazgo público y una visión clara del beneficio colectivo.

Innovación público-privada: entre la colaboración y la dependencia

La transformación digital de la salud se apoya de forma creciente en la colaboración con actores privados. Plataformas tecnológicas, proveedores de servicios en la nube y desarrolladores de soluciones digitales aportan capacidades que el sector público no siempre concentra internamente. Esta colaboración resulta necesaria, aunque introduce tensiones relacionadas con la dependencia tecnológica y el control del dato.

El diseño de relaciones equilibradas emerge como un elemento central. El sector público necesita preservar su capacidad de decisión estratégica y orientar la innovación hacia objetivos de interés general. La colaboración adquiere valor cuando contribuye a desarrollar capacidades internas y a fortalecer el sistema en su conjunto, sin trasladar la gobernanza a terceros.

En este marco, instrumentos como los PERTE se

presentan como mecanismos para articular inversión, innovación y política industrial en torno a prioridades públicas. La salud digital se configura así como un espacio de convergencia entre política sanitaria, transformación digital y estrategia económica.



Hablar de salud digital no es hablar de la digitalización del sistema sanitario: es hablar de salud, y por tanto, de la persona y del paciente.

Sergi Iglesias, Vicepresidente de la Sociedad Catalana de Salud Digital

Escalabilidad, equidad y adopción real

Uno de los riesgos recurrentes en la salud digital es la proliferación de pilotos con escasa capacidad de escalado. Soluciones técnicamente sólidas encuentran dificultades al integrarse en la práctica clínica cotidiana. La adopción efectiva depende de factores como la usabilidad, la integración en los flujos de trabajo y la aceptación por parte de profesionales y pacientes.

La equidad atraviesa este debate de forma transversal. La digitalización puede ampliar el acceso a servicios sanitarios, especialmente en territorios remotos, pero también puede excluir a quienes carecen de competencias digitales o conectividad suficiente. La brecha tecnológica se traduce en desigualdades con impacto directo en los resultados de salud.

El diseño centrado en el usuario, la formación y el acompañamiento se consolidan como elementos clave para evitar una sanidad a dos velocidades. La tecnología alcanza su potencial cuando se adapta a las personas y a sus contextos de uso.



Si no resolvemos la brecha digital no vamos a poder poner la inteligencia artificial al servicio de nuestros pacientes para su propio beneficio.

Ángel Borque, Fundación Instituto de Investigación Sanitaria de Aragón

Gobernar la salud digital como política de Estado

El Bloque III converge en que la salud digital se configura como una política pública de largo plazo. Su desarrollo depende menos de soluciones concretas que de la capacidad para articular gobernanza, datos, profesionales y ciudadanía en torno a un modelo compartido.

La transición digital en salud exige coherencia estratégica, continuidad institucional y una comprensión realista de los límites y posibilidades de la tecnología. En un sector donde las decisiones tienen un impacto humano directo, la innovación debe avanzar con ambición y prudencia.

La salud digital deja de presentarse como una promesa futura y se consolida como una necesidad presente. La cuestión central reside en si esta transformación será capaz de reforzar el carácter público, equitativo y sostenible de los sistemas sanitarios.

VISIÓN IBEROAMERICANA EN CLAVE DE PONENCIA

(BLOQUE III)

5.1 “La transformación digital en el sector social y sanitario: oportunidades para una mejor atención sanitaria” por Jesús Domínguez, ingeniero de soluciones, Salesforce

La incorporación de inteligencia artificial en los sistemas sanitarios se ha desplazado desde la experimentación hacia la necesidad estructural. La presión asistencial, la escasez de profesionales y el crecimiento de la demanda obligan a repensar cómo se organiza el trabajo clínico y administrativo. En este contexto, la IA aparece como una herramienta para liberar capacidad, no para sustituir criterio médico.

El valor principal de la inteligencia artificial en salud no reside en automatizar decisiones clínicas complejas, sino en optimizar procesos que hoy consumen tiempo y energía del profesional. La gestión de citas, la priorización de casos, la preparación de información clínica o el seguimiento de pacientes crónicos son ámbitos donde la tecnología puede aportar impacto inmediato. Como se expresó durante la ponencia, “la tecnología tiene sentido cuando devuelve tiempo al profesional

para cuidar”. Este enfoque desplaza el foco desde la sofisticación del algoritmo hacia su integración en los flujos reales de trabajo. Las soluciones que no se adaptan a la práctica clínica cotidiana tienden a generar rechazo, incluso cuando son técnicamente avanzadas. La adopción depende, en gran medida, de que la tecnología sea invisible y no añada fricción al proceso asistencial.

La gobernanza del dato emerge como una condición previa. Los modelos de IA solo son tan fiables como los datos que los alimentan. La fragmentación de sistemas, la baja interoperabilidad y la falta de estándares comunes limitan su potencial. En este sentido, se subrayó que “sin datos integrados no hay inteligencia artificial útil”. La calidad, trazabilidad y contexto del dato son tan relevantes como la capacidad de cálculo.

Finalmente, la ponencia sitúa la responsabilidad institucional en el centro del debate. La adopción de IA en salud requiere marcos claros de responsabilidad, explicabilidad y validación clínica. La tecnología no puede avanzar más rápido que la capacidad del sistema para gobernarla. Solo desde esta lógica la inteligencia artificial puede convertirse en una palanca real de transformación sanitaria.

5.2 “La inteligencia artificial en sanidad: ganando tiempo para una atención más humana” por José Rodríguez, director de Oracle Health

La transformación digital de la salud descansa sobre una infraestructura tecnológica que suele permanecer fuera del debate público: la gestión del dato y la capacidad de cómputo. Sin una base sólida, la innovación clínica y organizativa queda limitada a iniciativas aisladas. La infraestructura cloud se presenta como un habilitador clave para escalar soluciones digitales de forma segura y sostenible.

El principal desafío no es tecnológico, sino de arquitectura. Los sistemas sanitarios han crecido de forma fragmentada, con múltiples aplicaciones y bases de datos que no dialogan entre sí. Esta fragmentación dificulta tanto la atención clínica integrada como la explotación avanzada de la información. Como se señaló durante la ponencia, “el problema no es la falta de datos, sino que están dispersos y no se pueden usar”.

La nube permite abordar esta fragmentación desde una lógica de integración y escalabilidad. Facilita el

acceso seguro a la información, la interoperabilidad entre sistemas y el despliegue de analítica avanzada. Sin embargo, su adopción en salud plantea interrogantes legítimos sobre soberanía del dato, seguridad y cumplimiento normativo.

La respuesta no pasa por rechazar la tecnología, sino por gobernarla. Se insistió en la necesidad de modelos híbridos, donde el sector público mantenga el control estratégico del dato, independientemente del proveedor tecnológico. “La nube no es perder control, es cambiar la forma de ejercerlo”, se afirmó, subrayando que la clave está en los contratos, los estándares y la supervisión.

La infraestructura, entendida de este modo, deja de ser un elemento técnico para convertirse en una decisión de política pública. La capacidad de almacenar, procesar y proteger datos sanitarios condiciona la viabilidad de cualquier estrategia de salud digital. Sin esta base, la innovación queda reducida a un conjunto de promesas difíciles de materializar.

5.3 “El PERTE para la Salud de Vanguardia: impulsando la innovación en salud” por Silvia López, directora de División Técnica del Comisionado del PERTE para la Salud de Vanguardia, Gobierno de España

La salud digital no es solo una cuestión asistencial, sino también una oportunidad de política industrial. La articulación de capacidades tecnológicas, investigación biomédica y sistema sanitario convierte a la salud en un vector estratégico de desarrollo económico. En este marco se sitúa el PERTE Salud de Vanguardia, concebido como un instrumento para alinear inversión pública, innovación y objetivos sanitarios.

El enfoque parte de una premisa clara: la transformación del sistema de salud requiere escala y coordinación. Las iniciativas fragmentadas no generan impacto estructural. El PERTE busca precisamente superar esta lógica, impulsando proyectos tractores que conecten investigación, industria y prestación de servicios. Como se señaló, “no se trata de financiar tecnología, sino de transformar el sistema”.

La digitalización ocupa un lugar central en esta estrategia. El uso avanzado de datos, la inteligencia artificial, la medicina personalizada y la interoperabilidad aparecen como ámbitos

prioritarios. Sin embargo, el énfasis no está únicamente en la tecnología, sino en la capacidad del sistema para absorberla. La formación de profesionales, la adaptación organizativa y la gobernanza del dato son elementos inseparables de la inversión.

El PERTE se plantea también como una herramienta para reducir dependencias externas. Fortalecer capacidades industriales y tecnológicas propias permite al sistema sanitario ganar resiliencia y autonomía estratégica. En este sentido, la salud digital se vincula directamente con la soberanía tecnológica y la competitividad del país.

La ponencia subraya que la transformación sanitaria exige continuidad en el tiempo. Los ciclos políticos cortos no son compatibles con los plazos de maduración de la innovación en salud. El PERTE se presenta así como un intento de institucionalizar una visión de largo plazo, donde la digitalización refuerce tanto la calidad asistencial como el tejido productivo.

5.4 “Reestructuración de los Sistemas de salud en Iberoamérica: innovación, equidad y alianzas público-privadas” por Cristian Mazza, presidente de la Asociación Latinoamericana de Sistemas Privados de Salud (ALAMI)

La digitalización de la salud en América Latina se desarrolla en un contexto marcado por desigualdades estructurales. La región combina avances tecnológicos significativos con brechas persistentes en acceso, financiación y capacidades institucionales. En este escenario, la salud digital aparece como una oportunidad condicionada: puede ampliar el acceso o profundizar exclusiones existentes.

Uno de los principales desafíos es la heterogeneidad de los sistemas sanitarios. La fragmentación institucional y territorial dificulta la adopción de soluciones digitales a escala. Como se señaló durante la ponencia, “no existe una única salud digital para América Latina, existen muchas realidades distintas”. Esta diversidad obliga a diseñar estrategias adaptadas, alejadas de modelos importados sin contextualización.

La inclusión emerge como criterio central. La tecnología puede acercar servicios a poblaciones rurales o remotas, pero solo si se acompaña de políticas de conectividad, alfabetización digital y

financiamiento sostenible. De lo contrario, el riesgo es construir sistemas paralelos accesibles solo para una parte de la población.

La cooperación regional aparece como una vía para compartir aprendizajes y reducir asimetrías. El intercambio de experiencias, estándares comunes y proyectos colaborativos puede acelerar la adopción de soluciones efectivas. En este sentido, se destacó la importancia de articular alianzas público-privadas que respeten las prioridades sanitarias de cada país. La salud digital, en el contexto latinoamericano, no puede desligarse de la agenda de equidad. Su éxito no se medirá por el número de aplicaciones o plataformas, sino por su capacidad para mejorar resultados de salud en los colectivos más vulnerables. La tecnología, concluye la ponencia, solo tiene sentido si contribuye a fortalecer sistemas sanitarios más justos y resilientes.

06 BLOQUE EDUCACIÓN



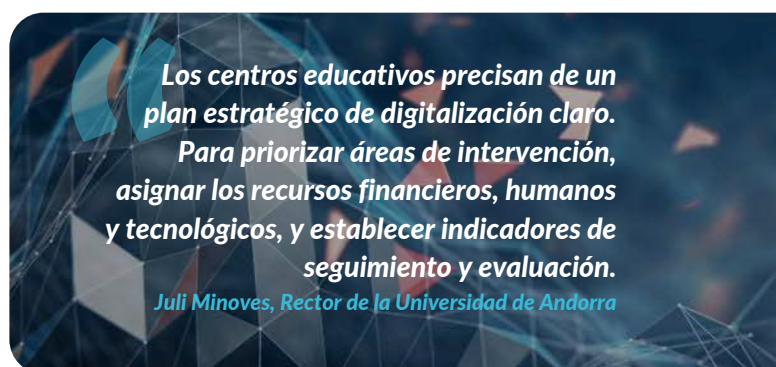
La educación superior ante una reconfiguración acelerada del conocimiento

La educación superior se encuentra en un proceso de reconfiguración profunda, impulsado por la convergencia entre inteligencia artificial, digitalización de procesos y transformación de los modelos de producción del conocimiento. Este cambio no se manifiesta como una transición gradual, sino como una superposición de dinámicas que ya están transformando la docencia, la investigación, la evaluación académica y la gobernanza institucional.

Las universidades operan hoy en un entorno donde las tecnologías digitales intervienen de forma directa en la generación, validación y circulación del

conocimiento. Esta intervención no es periférica. Afecta a cómo aprenden los estudiantes, cómo evalúan los docentes, cómo se revisa la producción científica y cómo se toman decisiones organizativas. La universidad actúa, en este contexto, como un puente entre transformaciones tecnológicas globales y realidades sociales, económicas y territoriales específicas.

Esta posición intermedia expone a las instituciones universitarias a una tensión constante entre velocidad de cambio y capacidad de adaptación. Las prácticas evolucionan más rápido que los marcos normativos, culturales y organizativos que deberían gobernarlas. La transformación digital universitaria se desarrolla, así, en un espacio donde la innovación cotidiana convive con estructuras diseñadas para otros ritmos.



Los centros educativos precisan de un plan estratégico de digitalización claro. Para priorizar áreas de intervención, asignar los recursos financieros, humanos y tecnológicos, y establecer indicadores de seguimiento y evaluación.

Juli Minoves, Rector de la Universidad de Andorra

La inteligencia artificial ya forma parte del sistema universitario

La inteligencia artificial se ha integrado de facto en el funcionamiento cotidiano del sistema universitario. Su presencia atraviesa el ciclo completo del conocimiento: desde la elaboración de trabajos académicos hasta los procesos de evaluación, desde el apoyo a la investigación hasta la revisión por pares. Este fenómeno no responde a una adopción institucional planificada, sino a una incorporación progresiva impulsada por estudiantes, docentes e investigadores en su práctica diaria.

La consecuencia inmediata es un desplazamiento de los debates tradicionales sobre uso permitido o prohibido. La inteligencia artificial permanece y se adapta, incluso cuando se intenta limitar su utilización. El foco se traslada hacia la capacidad institucional para redefinir criterios de autoría, integridad académica, evaluación del aprendizaje y responsabilidad científica. La cuestión central deja de ser la detección del uso tecnológico y pasa a ser

la formación del criterio para entenderlo, evaluarlo y gobernarlo.

Este escenario exige una alfabetización académica ampliada, que incorpore la comprensión crítica de los sistemas de inteligencia artificial como parte de las competencias universitarias básicas. La universidad se enfrenta al reto de formar personas capaces de pensar con tecnología sin delegar en ella el juicio intelectual.

Gobernanza institucional y medición de la madurez digital

La transformación digital universitaria adquiere coherencia cuando se articula desde la gobernanza. Las experiencias compartidas muestran que los avances más consistentes se producen en aquellas instituciones que han integrado la digitalización en su planificación estratégica, dotándose de estructuras de liderazgo claras y mecanismos de seguimiento.

La medición de la madurez digital se consolida como una herramienta clave para orientar decisiones. Evaluar procesos, capacidades y resultados permite identificar brechas reales y priorizar intervenciones con mayor impacto. Esta lógica desplaza la transformación digital del terreno de la intuición al de la gestión basada en evidencia.

La madurez digital se entiende como un proceso continuo. Cada avance abre nuevas exigencias en competencias, infraestructura y cultura organizativa. Esta visión resulta especialmente relevante en sistemas universitarios heterogéneos, donde los ritmos de transformación varían de forma significativa entre instituciones y territorios.

docencia y en el rol del profesorado. Una parte significativa del cuerpo docente ha incorporado tecnologías en su práctica cotidiana, mientras que una proporción menor impulsa transformaciones metodológicas más profundas.

Esta diferencia condiciona la capacidad de escalar la innovación educativa. La adopción tecnológica sin cambios pedagógicos estructurales tiende a reproducir modelos tradicionales en formatos nuevos. El liderazgo pedagógico aparece como un factor crítico para traducir la digitalización en mejoras reales del aprendizaje.

La evolución del rol docente se conecta también con la transformación del mercado laboral. La aceleración tecnológica reduce la vigencia de los conocimientos y refuerza el valor del aprendizaje a lo largo de la vida. La universidad amplía su función formativa, ofreciendo itinerarios flexibles, actualización continua y desarrollo de competencias transversales. La digitalización facilita esta expansión siempre que se apoye en modelos pedagógicos coherentes y criterios de calidad compartidos.

Nuestra verdadera obsesión es disponer de un sistema de evaluación que pueda acreditar ante la sociedad que aquellas personas a las que damos un título universitario realmente tienen las competencias que se dice en el plan de estudios que deben tener.

Marc Escolà, protonotario académico de la Universidad Europea de Andorra

Cuando hablamos de infraestructura se nos olvida muchas veces que la capacitación continua y el soporte técnico también tienen que estar dentro de la presupuestación, si no la tecnología se vuelve obsoleta.

Jaime García, director e investigador Senior del Índice de Progreso Social de INCAE Business School

Docencia, profesorado y liderazgo pedagógico

La digitalización impacta de manera directa en la

Infraestructura, energía y soberanía del conocimiento

El debate sobre educación digital incorpora una dimensión material que condiciona de forma directa la autonomía académica y científica. La capacidad de cómputo, el acceso a energía y la disponibilidad de infraestructuras tecnológicas determinan quién puede desarrollar investigación avanzada, entrenar modelos de inteligencia artificial y gestionar grandes volúmenes de datos.

Las diferencias en costes energéticos y capacidad instalada introducen asimetrías relevantes entre regiones e instituciones. Estas brechas no son

únicamente presupuestarias; afectan a la capacidad de decidir sobre tecnologías críticas y a la dependencia de infraestructuras externas. La soberanía del conocimiento se vincula, en este contexto, con la capacidad de sostener infraestructuras propias o compartidas bajo criterios públicos.

La cooperación entre instituciones con afinidad estratégica emerge como una respuesta pragmática. Compartir recursos, capacidades y conocimientos permite mitigar limitaciones individuales y sostener proyectos que, de otro modo, resultarían inviables. La cooperación adquiere así un carácter operativo, orientado a mantener capacidades reales en un entorno de creciente concentración tecnológica.

Las competencias digitales ya no son de uso de los instrumentos, sino de cómo comportarse con estos instrumentos, del respeto, la convivencia, el sentido crítico y la ciudadanía democrática en el espacio digital.

Albert Maluquer, director de Sistemas de Educación y Relaciones Internacionales del Gobierno de Andorra

Cooperación iberoamericana y aprendizaje en red

La diversidad de los sistemas universitarios iberoamericanos refuerza el valor de la cooperación estructurada. Compartir experiencias, metodologías y modelos de gobernanza permite acelerar aprendizajes y reducir la duplicación de esfuerzos. La transformación digital universitaria avanza con mayor solidez cuando se apoya en redes de colaboración que convierten experiencias locales en referencias transferibles.

Esta lógica de aprendizaje en red resulta especialmente relevante en contextos de recursos limitados. La cooperación permite ganar escala sin imponer uniformidad, respetando las especificidades institucionales y territoriales. La universidad amplía, de este modo, su capacidad de incidencia más allá de sus fronteras inmediatas.

La articulación con gobiernos, sector productivo y sociedad civil refuerza este enfoque. La

digital universitaria se inscribe en ecosistemas más amplios de desarrollo, donde la educación superior actúa como nodo de innovación social, científica y económica.

No lo estamos haciendo solos, lo estamos haciendo con otros para llegar más lejos, trabajando en torno a tres ejes que son inseparables: conocimiento, tecnología y alianzas.

Pastora Martínez Samper, Comisionada para la acción internacional, Universitat Oberta de Catalunya (UOC)

Inclusión, acceso y responsabilidad pública

La digitalización amplía el alcance potencial de la educación superior, pero introduce riesgos de exclusión si no se acompaña de políticas específicas. El acceso desigual a conectividad, dispositivos y competencias digitales condiciona la capacidad de amplios sectores de la población para beneficiarse de la transformación educativa.

La universidad mantiene una responsabilidad pública en este ámbito. Diseñar estrategias que integren inclusión digital y educativa resulta indispensable para evitar una educación superior segmentada. La tecnología puede acercar la universidad a nuevos públicos siempre que se adapte a contextos diversos y se acompañe de formación y apoyo.

El vínculo con el territorio refuerza esta dimensión. La transformación digital facilita nuevas formas de transferencia de conocimiento, innovación aplicada y desarrollo local. Esta conexión territorial fortalece la legitimidad social de la universidad en un entorno de cambio acelerado.

Gobernar la transformación universitaria

La transformación digital universitaria se configura como un proceso estructural que exige liderazgo, continuidad y visión de largo plazo. La inteligencia artificial, los datos y la infraestructura ya están reconfigurando la forma en que se enseña, se investiga y se valida el conocimiento.

La universidad enfrenta el desafío de adaptarse sin perder su función crítica ni su autonomía intelectual. Su capacidad para gobernar esta transición

determinará si sigue siendo un activo colectivo central en la construcción del futuro del conocimiento en Iberoamérica.

Más que una adaptación técnica, la transformación digital de la educación superior redefine el papel de la universidad en la sociedad contemporánea y su contribución al desarrollo sostenible, la cohesión social y la producción de conocimiento con sentido público.

“Los problemas complejos —como la adaptación de la IA a la educación— requieren un enfoque multiactor, incluyendo agencias de financiación, reguladores, sector público, empresas privadas y organizaciones con objetivos afines.

Fabrizio Gagliardi, asesor senior de la dirección del Barcelona Supercomputing Centre (BSC)

VISIÓN IBEROAMERICANA EN CLAVE DE PONENCIA

(BLOQUE IV)

6.1 “La estrategia iberoamericana para la transformación digital de la educación superior” por Félix García Lausín, coordinador del Espacio del Conocimiento Iberoamericano, SEGIB

La transformación digital de la educación superior interpela directamente el papel de la universidad en Iberoamérica. Las instituciones universitarias operan como nodos donde convergen formación, ciencia, innovación, políticas públicas, mercado laboral y ciudadanía. En ese cruce, la digitalización está redefiniendo funciones, responsabilidades y expectativas sociales.

En ese contexto, la universidad se consolida como una infraestructura social estratégica: forma capital humano, produce conocimiento y articula capacidades colectivas en un contexto caracterizado por la aceleración tecnológica y la fragilidad institucional. En ese marco, la transformación digital se vincula con la capacidad de anticipar cambios y de formar agentes capaces de intervenir en realidades complejas. Las universidades son un puente que posibilita transformaciones necesarias para ese futuro posible.

La cooperación iberoamericana emerge como una

condición estructural para avanzar. La heterogeneidad de los sistemas universitarios, de los niveles de madurez digital y de los recursos disponibles hace inviable cualquier enfoque aislado. Plataformas de colaboración como MetaRed, permiten compartir aprendizajes, contrastar modelos y transformar experiencias locales en referencias transferibles. Compartir casos de éxito y hacerlos aplicables responde a una lógica de escala más que a un ejercicio de visibilidad institucional.

La transformación digital debe entenderse como un proceso organizativo y cultural. La adopción de tecnologías digitales modifica la forma en que las universidades gobiernan, evalúan su desempeño y toman decisiones. La gestión basada en datos adquiere un papel central, al permitir identificar brechas reales y orientar prioridades estratégicas.

La sostenibilidad atraviesa este proceso. La incorporación de tecnologías emergentes, incluida la inteligencia artificial, plantea implicaciones energéticas, éticas y sociales que requieren marcos adecuados de gobernanza. La universidad está llamada a integrar innovación y responsabilidad dentro de una misma agenda, liderando desde el ejemplo y reforzando su función pública en la transición digital iberoamericana.

6.2 “Transformación Digital Sostenible en Educación Superior. El rol de MetaRed” por Esther Lucía Sánchez, rectora de la Universidad Nacional de Cuyo y presidenta de MetaRed

La transformación digital universitaria se inscribe en un contexto marcado por crisis ambientales, cambios tecnológicos acelerados y redefinición de los modelos de conocimiento. En este escenario, la universidad se ve obligada a revisar su forma de organizarse, de enseñar y de vincularse con su entorno.

La experiencia institucional presentada sitúa la digitalización como un proceso estratégico que afecta a la gobernanza, la cultura organizativa y la planificación a largo plazo. La creación de estructuras específicas para liderar esta transformación refleja una comprensión clara del desafío. “La transformación digital es un cambio cultural” resume la idea de que la tecnología actúa como catalizador de decisiones más profundas.

Los datos adquieren un papel central como activo institucional. Medir la madurez digital permite abandonar aproximaciones intuitivas y avanzar con

con criterio. Modelos como U-Digital ofrecen marcos de referencia que facilitan diagnósticos comparables y planes de acción graduales. La madurez digital se concibe como un recorrido progresivo, donde cada etapa habilita la siguiente.

La formación del profesorado aparece como uno de los vectores críticos. El diagnóstico presentado muestra avances significativos en el uso de herramientas digitales, junto con una brecha clara en liderazgo pedagógico y estratégico. Este contraste orienta políticas de capacitación más focalizadas, entendiendo que el rol docente evoluciona en paralelo a la transformación institucional.

La sostenibilidad atraviesa toda la reflexión. La adopción de inteligencia artificial y tecnologías exponenciales implica decisiones con impacto energético y ambiental. Desde esta perspectiva, la universidad asume la responsabilidad de integrar transición digital y transición ecológica en una misma visión. “Hacer vivible el futuro” se convierte en una formulación que conecta innovación, ética y desarrollo.

La transformación digital universitaria aparece así como una condición para seguir cumpliendo la función pública de la universidad en un mundo en mutación, reforzando su vínculo con el territorio y su capacidad de generar valor social.

07 BLOQUE CIBERSEGURIDAD



La ciberseguridad se consolida como uno de los pilares estructurales de la transformación digital. A diferencia de otras dimensiones, su relevancia no depende del grado de digitalización alcanzado, sino de la exposición acumulada que generan la interconexión, la automatización y la dependencia tecnológica. En este contexto, la ciberseguridad deja de ser un ámbito técnico para convertirse en una

cuestión de soberanía, estabilidad institucional y confianza social.

Las intervenciones del bloque coinciden en un diagnóstico claro: el perímetro clásico de seguridad ha desaparecido. Estados, administraciones públicas, infraestructuras críticas y empresas privadas operan en un ecosistema donde las fronteras digitales son difusas y donde los ataques no distinguen entre sectores ni tamaños. La asimetría entre atacantes y defensores se amplifica por la velocidad de adopción tecnológica y por la sofisticación creciente de las amenazas.

La ciberseguridad se configura así como una política pública transversal, que afecta a la continuidad de los servicios esenciales, a la protección de derechos fundamentales y a la capacidad de los países para sostener su transformación digital sin comprometer su resiliencia.



Amenazas persistentes y evolución del riesgo

El panorama de amenazas descrito en el bloque muestra una evolución clara en tácticas, vectores y actores. La explotación de vulnerabilidades en dispositivos de borde, infraestructuras críticas y cadenas de suministro se consolida como uno de los principales puntos de entrada. Estos entornos, tradicionalmente menos monitorizados que los sistemas corporativos, concentran hoy una parte relevante del riesgo.

La distinción entre actores estatales y criminales pierde nitidez. Técnicas desarrolladas por actores avanzados son rápidamente adoptadas por redes criminales con capacidad financiera creciente. La monetización del cibercrimen, a través de *ransomware*, extorsión o robo de información, alimenta un ecosistema cada vez más profesionalizado y persistente.

La ciberseguridad deja de ser un problema excepcional para convertirse en una condición permanente del entorno digital. La exposición no responde únicamente a fallos técnicos, sino a decisiones organizativas, carencias de gobernanza y déficits de capacidades internas.

Uno de los grandes desafíos es seguir avanzando en concienciación y formación, y el otro es la limitación presupuestaria: el mercado de la ciberseguridad es igual de caro independientemente del tamaño del país.

Andreu Tomàs, Director de Var Group Andorra

Inteligencia artificial y ciberseguridad: doble filo estratégico

La inteligencia artificial introduce una transformación profunda en el ámbito de la ciberseguridad. Su uso por parte de los atacantes acelera la automatización de campañas, la personalización de ingeniería social y la explotación de vulnerabilidades a escala. Al mismo tiempo, refuerza las capacidades defensivas mediante detección avanzada, análisis de comportamiento y respuesta automatizada.

El bloque subraya que esta dinámica genera una carrera tecnológica continua. La defensa no puede prescindir de la IA sin asumir una desventaja estructural. La ciberseguridad incorpora así una dimensión de innovación constante, donde la actualización de capacidades se convierte en un requisito operativo.

Este escenario introduce nuevos riesgos asociados a los propios sistemas de inteligencia artificial. La protección de modelos, datos de entrenamiento y flujos de decisión adquiere un peso estratégico. La seguridad de la IA se integra como una capa adicional dentro de la arquitectura global de ciberseguridad.

La inteligencia artificial es una cuestión de supervivencia: si los defensores de la ciberseguridad no usan IA, quedan en desventaja frente a la ciberdelincuencia.

Tomás Clemente, arquitecto principal de seguridad de Amazon Web Services (AWS)

Identidad, trazabilidad y control en entornos automatizados

La proliferación de agentes digitales y sistemas automatizados redefine el concepto de identidad en los entornos digitales. La capacidad de asignar identidades claras, roles y permisos a sistemas no humanos emerge como una condición crítica para mantener trazabilidad y control.

La gestión de identidades se convierte en un eje estructural de la seguridad. Sin mecanismos que permitan auditar acciones, aplicar privilegios mínimos y monitorizar comportamientos, la automatización amplifica el riesgo en lugar de mitigarlo. La identidad deja de ser un atributo exclusivamente humano para integrarse en la gobernanza técnica de los sistemas.

Esta evolución refuerza la necesidad de marcos de seguridad que contemplen la complejidad creciente de los entornos digitales y que integren la automatización sin perder capacidad de supervisión.

El abuso infantil en Internet no tiene fronteras: el material puede estar subido en un país, alojado en otro y llegar a todo el mundo en segundos. La colaboración internacional y una legislación actualizada son imprescindibles.

Grete Raidma, INSAFE-INHOPE

Regulación, cumplimiento y vigilancia continua

El bloque pone de relieve la densidad creciente del marco regulatorio en materia de ciberseguridad. Normativas nacionales, europeas e internacionales configuran un entorno exigente, donde el cumplimiento formal resulta insuficiente sin mecanismos de supervisión continua.

La ciberseguridad regulatoria se desplaza hacia modelos dinámicos, basados en evaluación permanente, evidencias y capacidad de respuesta. La acumulación normativa plantea desafíos de implementación, especialmente para administraciones y organizaciones con recursos limitados.

La capacidad de traducir requisitos legales en

controles técnicos operativos se convierte en un factor crítico. La regulación actúa como marco habilitador cuando se integra en la gestión diaria y no como un ejercicio puntual de auditoría.

Sin entender claramente en qué punto se encuentra cada país en materia de ciberseguridad, es imposible que los organismos internacionales, el sector privado o las agencias de desarrollo actúen de forma eficaz.

Jaroslav Ponder, director de la Oficina de Europa de la Unión Internacional de Telecomunicaciones (UIT)

Infraestructuras críticas, servicios esenciales y resiliencia

La protección de infraestructuras críticas ocupa un lugar central en el bloque. Energía, telecomunicaciones, agua, transporte y servicios sanitarios concentran riesgos sistémicos cuyo impacto trasciende el ámbito digital. Los ataques a estos entornos buscan desestabilizar, extorsionar o influir en contextos geopolíticos.

La resiliencia se construye a partir de arquitecturas robustas, planes de continuidad y capacidad de recuperación. La ciberseguridad se integra como un componente estructural de la gestión del riesgo país, no como una función aislada.

La migración a entornos *cloud* introduce oportunidades de escalabilidad y visibilidad, siempre que se acompañe de modelos claros de responsabilidad compartida y de gobernanza técnica adecuada.

Cooperación internacional y construcción de capacidades

La dimensión transfronteriza de la ciberseguridad atraviesa todo el bloque. Las amenazas no respetan jurisdicciones y la respuesta efectiva exige cooperación internacional, intercambio de información y alineación de estándares.

La construcción de capacidades nacionales aparece como una prioridad estratégica. Formación de

profesionales, simulacros, ejercicios conjuntos y participación en foros internacionales fortalecen la capacidad de respuesta colectiva. La cooperación técnica se convierte en un complemento indispensable de la regulación. La ciberseguridad se consolida así como un ámbito donde la acción nacional y la coordinación internacional resultan inseparables.

Concienciación, liderazgo y cultura organizativa

El bloque concluye subrayando el papel del liderazgo y la cultura organizativa. La concienciación de las capas directivas se identifica como un factor determinante para priorizar inversiones, adoptar decisiones estratégicas y sostener políticas de seguridad coherentes.

La escasez de talento especializado y las limitaciones presupuestarias refuerzan la necesidad de enfoques pragmáticos, colaboración público-privada y democratización del acceso a soluciones de seguridad. La gestión del cambio emerge como un desafío transversal. La ciberseguridad deja de ser una cuestión técnica para convertirse en una responsabilidad compartida entre instituciones, empresas y ciudadanía.

VISIÓN IBEROAMERICANA EN CLAVE DE PONENCIA

(BLOQUE V)

7.1 “Implementación de la Carta Iberoamericana de Principios y Derechos de los Entornos Digitales (CIPDED)” por Alejandro Kawabata, Director de Asuntos Jurídicos e Institucionales, SEGIB

La transformación digital en América Latina se sostiene sobre una desigualdad estructural que condiciona su alcance y sus efectos. Hay 244 millones de personas que no tienen acceso a Internet, lo que limita de forma directa el acceso a educación, empleo, servicios públicos y participación cívica. Esta brecha no se agota en la cobertura. Afecta también a la calidad —el 55% de los usuarios se quejan de la baja calidad—, a la asequibilidad y a las capacidades, con menos del 30% de la población con competencias digitales básicas.

La digitalización, en este contexto, no opera como mecanismo de integración, sino como un factor que puede profundizar las desigualdades existentes.

La Carta Iberoamericana de Principios y Derechos en los Entornos Digitales emerge como un marco de alineación política para ordenar este proceso. Su legitimidad reside en su adopción por jefes de Estado y de Gobierno y en un consenso articulado en torno a tres principios operativos: la transformación digital debe estar centrada en las personas, los derechos fundamentales deben ser garantizados en entornos digitales y este proceso no debe “dejar a nadie atrás”. Estos principios establecen una base común para orientar decisiones públicas en un entorno marcado por la fragmentación y la velocidad del cambio tecnológico.

La arquitectura del instrumento traduce ese consenso en una estructura operativa compuesta por diez capítulos temáticos y 58 compromisos de política pública, concebidos para guiar tanto la adaptación normativa como el diseño de políticas públicas. Su alcance abarca la totalidad del proceso de transformación digital, integrando dimensiones como conectividad, gobernanza, derechos y tecnologías emergentes.

La implementación se configura como el núcleo del planteamiento. Se organiza en torno a cuatro ámbitos prioritarios —conectividad e inclusión digital, protección de datos y ciberseguridad, gobierno digital y tecnologías emergentes— y se articula mediante producción de conocimiento, desarrollo de estándares comunes y mecanismos de cooperación regional. La generación de capacidades compartidas se plantea como condición para reducir la fragmentación normativa y avanzar hacia una mayor coherencia regional.

En este marco, adquieren relevancia instrumentos concretos orientados a sostener esa implementación: repositorios normativos validados por los Estados, sistemas de indicadores para medir la evolución de la digitalización, encuestas regionales para identificar necesidades y programas de capacitación dirigidos a cerrar brechas de habilidades. A ello se suma el desarrollo de estándares en ámbitos críticos como la protección de datos, los derechos del consumidor en entornos digitales o la interoperabilidad de los servicios públicos.

La inteligencia artificial se incorpora como un ámbito que exige criterios específicos de gobernanza. Se plantea el desarrollo de modelos “transparentes,

Te puede interesar:

Descarga la Carta de Principios y Derechos para entornos digitales.



inclusivos y representativos lingüísticamente” y la definición de estándares comunes para su uso ético y seguro. Esta aproximación parte de una premisa operativa: “el proceso de transformación digital va mucho más rápido que las decisiones de política pública”, lo que desplaza el foco regulatorio hacia el uso de las tecnologías.

El conjunto configura una visión de la transformación digital como proceso político y operativo, donde la coordinación regional, la producción de conocimiento y la definición de estándares comunes funcionan como condiciones necesarias para sostener su desarrollo y limitar sus efectos excluyentes.

7.2 “Nación Frontera: IA y Ciberseguridad” por Alberto Pinedo, National Technology and Security Lead, Microsoft

La adopción de la inteligencia artificial se consolida como una realidad transversal en las organizaciones, con un alto porcentaje de empresas ya operando en entornos que integran estas capacidades y una rápida evolución hacia modelos más avanzados basados en agentes. Este desarrollo no responde a una dinámica coyuntural, sino a una transformación estructural en la forma en que se organiza el trabajo, donde los sistemas dejan de limitarse a asistir y comienzan a ejecutar tareas de forma autónoma bajo supervisión humana.

Este cambio introduce un nuevo modelo operativo en el que las organizaciones se orientan al trabajo más que a estructuras jerárquicas, apoyándose en agentes capaces de asumir funciones específicas.

La inteligencia artificial permite descargar tareas repetitivas o de bajo valor, concentrando la intervención humana en actividades estratégicas. Lejos de sustituir al humano, el objetivo es “potenciar aquel trabajo que es poco productivo, descargarlo y yo centrarme en lo que realmente aporta valor”.

Este escenario amplía de forma significativa los riesgos asociados al uso de la tecnología. La gestión de la información se convierte en un punto crítico, especialmente en contextos donde se manejan datos sensibles o clasificados. A ello se suma la creciente complejidad normativa, con marcos regulatorios que exigen un control preciso sobre el uso, acceso y tratamiento de los datos. La dificultad no reside únicamente en la existencia de normas, sino en su implementación efectiva dentro de sistemas tecnológicos complejos.

La inteligencia artificial también incrementa la capacidad de los actores maliciosos, generando un entorno en el que las amenazas evolucionan con mayor rapidez. En palabras del propio planteamiento, “la IA nos ayuda mucho, también potencia y ayuda a los malos”, lo que obliga a las organizaciones a incorporar estas mismas capacidades en sus mecanismos de defensa. En este contexto, la gestión de identidades adquiere un papel central. La incorporación de agentes en los procesos exige que estos dispongan de identidades propias que permitan aplicar controles de acceso, establecer trazabilidad y garantizar la supervisión de sus acciones. Sin este elemento, la protección de los sistemas se vuelve incompleta.

La respuesta pasa por desarrollar capacidades que permitan descubrir y clasificar los activos de información, controlar el uso de herramientas de inteligencia artificial, monitorizar riesgos en tiempo real y asegurar el cumplimiento normativo de forma continua. La ciberseguridad se articula así como un sistema integrado de control, visibilidad y respuesta, orientado a sostener el uso seguro de la inteligencia artificial en entornos organizativos cada vez más complejos.

7.3 “Más allá del cumplimiento: seguridad en productos y servicios TIC” por Estefanía, Centro Criptológico Nacional de España (CCN-CERT), Ministerio de Defensa del Gobierno de España

El incremento sostenido de vulnerabilidades en productos y servicios tecnológicos responde a una transformación marcada por la creciente interconexión de sistemas y la adopción de tecnologías cada vez más complejas. La exposición al riesgo deja de estar vinculada únicamente a la operación de los sistemas para situarse también en la calidad de los componentes que los integran. Tal como se evidencia en los análisis realizados, “el

número de vulnerabilidades detectadas en productos y servicios era cada vez mayor”, en parte por una mayor capacidad de detección, pero también por una ampliación real de la superficie de exposición.

La seguridad se articula sobre tres pilares fundamentales —personas, procesos y tecnología—, aunque el foco se desplaza hacia esta última, en particular hacia la garantía de que los productos y servicios utilizados cumplen requisitos verificables. La tendencia a centrarse en arquitecturas seguras ha dejado en segundo plano la evaluación de los propios componentes, generando situaciones en las que sistemas aparentemente robustos incorporan elementos con debilidades estructurales.

En este contexto, el catálogo de productos y servicios de seguridad desarrollado por el Centro Criptológico Nacional se configura como un mecanismo clave para introducir criterios homogéneos en la adquisición tecnológica del sector público. Este catálogo incluye únicamente aquellos productos y servicios que han superado procesos de evaluación y certificación, garantizando que cumplen un conjunto definido de requisitos de seguridad. La lógica no se limita a validar lo declarado por el fabricante, sino a establecer de forma independiente qué funcionalidades deben formar parte de la certificación, evitando así una “falsa sensación de seguridad” derivada de certificaciones incompletas.

La evidencia empírica refuerza esta necesidad. En los primeros procesos de evaluación, se detectó que “el 16% de los requisitos... no los implementaban directamente” y que “el 19% lo hacían con vulnerabilidades”. La corrección de estas deficiencias supone una mejora significativa en la seguridad global de los sistemas, al reducir el número de vulnerabilidades explotables dentro de una misma arquitectura.

El modelo evoluciona hacia esquemas de evaluación continua que permiten mantener actualizadas las garantías de seguridad en entornos donde los ciclos de desarrollo son cada vez más cortos. Metodologías como Lince o los nuevos enfoques para entornos cloud introducen mecanismos de certificación adaptados a esta realidad, incorporando evaluaciones periódicas y monitorización constante. En esta línea, el desarrollo de nuevas metodologías como Ciclón apunta hacia sistemas de certificación

dinámicos, capaces de reflejar en tiempo real el nivel de garantía de los servicios. La seguridad de los productos y servicios TIC se configura así como un elemento estructural en la gestión del riesgo, basado en evaluación rigurosa, control continuo y adaptación a la evolución tecnológica.

7.4 “Panorama de las amenazas cibernéticas: relatos desde la trinchera” por David Grout, CTO EMEA y Director Técnico, Google

El análisis de miles de horas de respuesta a incidentes a nivel global permite identificar un cambio claro en las dinámicas de ataque: los adversarios priorizan puntos de entrada menos protegidos, combinan técnicas avanzadas con vectores de bajo coste y operan con una creciente capacidad de adaptación. En este contexto, los dispositivos de borde de red —*firewalls*, VPNs y sistemas de acceso— se consolidan como uno de los principales focos de explotación, al constituir “blind spots” en muchas arquitecturas de seguridad. A diferencia de los entornos *endpoint*, ampliamente monitorizados en la última década, estos sistemas presentan menores niveles de visibilidad y control.

La explotación de vulnerabilidades *zero-day* en estos dispositivos se ha intensificado, especialmente por parte de actores estatales, aunque rápidamente ha sido adoptada también por grupos criminales. El acceso a estos puntos permite escalar dentro de las redes, obtener credenciales y desplegar operaciones de extorsión o *ransomware*. Esta convergencia de técnicas refleja una difusión acelerada del conocimiento operativo entre distintos tipos de atacantes.

En paralelo, emergen perfiles menos sofisticados en términos técnicos, pero altamente efectivos en la ejecución. Los denominados “*advanced persistent teenagers*” operan mediante esquemas de ingeniería social apoyados en información obtenida a través de *malware* tipo *infostealer*. La combinación de datos personales, urgencia y manipulación emocional permite comprometer procesos internos, como los servicios de soporte, y obtener acceso legítimo a sistemas críticos. Estos ataques no dependen de vulnerabilidades técnicas, sino de la explotación de dinámicas organizativas.

El alcance de las amenazas se extiende también a infraestructuras críticas e industriales, donde las

capacidades de protección son más limitadas y los sistemas presentan mayores restricciones operativas. A ello se suma el interés creciente por cadenas de suministro y servicios SaaS, donde un único punto de compromiso puede escalar a múltiples organizaciones.

La inteligencia artificial introduce un doble vector. En el corto plazo, su uso por parte de los atacantes se concentra en la mejora de campañas de desinformación, traducción y generación de contenido para *phishing*. Sin embargo, la progresiva reducción de barreras de acceso —con herramientas disponibles a bajo coste— anticipa una expansión hacia capacidades más complejas, incluyendo desarrollo de *malware* o automatización de ataques.

De cara al futuro, se prevé la persistencia del *ransomware* como modelo dominante, el aumento de operaciones sobre telecomunicaciones y una mayor instrumentalización del ciberespacio en contextos geopolíticos. Al mismo tiempo, la inteligencia artificial ofrece ventajas claras para la defensa, especialmente en la detección automatizada de vulnerabilidades y la aceleración de la respuesta operativa.

08 CONCLUSIONES PARA EL AVANCE DIGITAL IBEROAMERICANO

El **II Foro Digital de Andorra** confirma que la transición digital en Iberoamérica ha entrado en una fase decisiva. El debate central ya no gira en torno a la adopción tecnológica, sino a la capacidad de los Estados, las empresas y las instituciones para gobernar este proceso en un contexto marcado por la aceleración tecnológica, la fragmentación geopolítica y el cuestionamiento de los marcos multilaterales. La digitalización se ha convertido en una infraestructura política, económica y social que determina la prestación de servicios públicos, el acceso a derechos y la distribución de riesgos. No puede abordarse como una suma de proyectos sectoriales, sino como una agenda estratégica de país y de región.

01 GOBERNAR LA DIGITALIZACIÓN COMO POLÍTICA PÚBLICA ESTRUCTURAL

La transformación digital exige liderazgo público sostenido, capaz de articular visión, prioridades y mecanismos de coordinación interinstitucional. No se trata solo de impulsar innovación, sino de alinear tecnología, regulación, capacidades y recursos en torno a objetivos claros de desarrollo, inclusión y sostenibilidad. La ausencia de dirección política genera fragmentación, dependencia tecnológica y pérdida de capacidad institucional. Sin orientación pública, la digitalización tiende a reproducir desigualdades y consolidar dependencias. Gobernar implica asumir decisiones sobre datos, infraestructuras, estándares, interoperabilidad y modelos de colaboración con una mirada de largo plazo.

02 IDENTIDAD DIGITAL Y DATOS COMO INFRAESTRUCTURA DEL ESTADO DIGITAL

La identidad digital emerge como pilar del Estado digital: no solo como mecanismo de autenticación, sino como infraestructura que permite ejercer derechos, acceder a servicios y construir confianza entre ciudadanía y administración. Los sistemas de identidad robustos facilitan la interoperabilidad, reducen fricciones y habilitan nuevos modelos de servicio público.

Ligada a la identidad, la gestión del dato se consolida como activo estratégico. Los sistemas públicos generan volúmenes crecientes de información, pero su valor depende de la capacidad para integrarla y convertirla en conocimiento accionable. La fragmentación de bases de datos y la ausencia de marcos de gobernanza limitan el impacto de la digitalización. La gobernanza del dato no es un desafío técnico: involucra decisiones sobre privacidad, uso legítimo, responsabilidad y control democrático, especialmente donde la inteligencia artificial comienza a integrarse en procesos clave.

03 INTELIGENCIA ARTIFICIAL: OPORTUNIDAD, RIESGO Y RESPONSABILIDAD PÚBLICA

La inteligencia artificial atraviesa todos los bloques temáticos del Foro. Su potencial para mejorar la eficiencia, apoyar la toma de decisiones y personalizar servicios es ampliamente reconocido, pero su incorporación sin marcos claros de gobernanza introduce riesgos significativos. Su valor depende de la calidad de los datos, la claridad en la asignación de responsabilidades y la posibilidad de supervisar y corregir decisiones automatizadas. Donde estos elementos faltan, la IA amplifica errores y opacidades. El Foro apunta a la necesidad de modelos de adopción responsables que integren evaluación de impacto, explicabilidad, trazabilidad y control humano significativo. La inteligencia artificial se consolida como herramienta de política pública que exige criterios éticos, jurídicos y organizativos.

04 CIBERSEGURIDAD COMO CONDICIÓN DE GOVERNABILIDAD DIGITAL

En un entorno de amenazas persistentes e infraestructuras interconectadas, la seguridad deja de ser una función periférica para convertirse en un elemento central de la gobernanza. El principal riesgo ya no reside en los incidentes puntuales, sino en la erosión progresiva de la capacidad de control. La dependencia tecnológica y la opacidad de sistemas complejos debilitan la autonomía de los Estados y la confianza ciudadana.

La hoja de ruta apunta hacia una ciberseguridad integrada desde el diseño, apoyada en estándares, certificación, cooperación público-privada y desarrollo de capacidades internas, construyendo la resiliencia como proceso continuo.

05 SERVICIOS FINANCIEROS DIGITALES E INCLUSIÓN ECONÓMICA

La digitalización financiera es uno de los vectores más potentes de inclusión económica. La expansión de pagos digitales, fintech y nuevos modelos de intermediación abre oportunidades para ampliar el acceso a servicios, especialmente en contextos de informalidad. Sin embargo, el Foro advierte que la innovación financiera sin marcos adecuados puede generar nuevas exclusiones y riesgos sistémicos. La regulación, la supervisión y la educación financiera son elementos clave para asegurar que la digitalización contribuya a la estabilidad y al bienestar. La colaboración entre reguladores, entidades financieras tradicionales y nuevos actores tecnológicos es el factor crítico para construir ecosistemas financieros sólidos y confiables.

06 SALUD DIGITAL: SOSTENIBILIDAD, EQUITAD Y CALIDAD ASISTENCIAL

La digitalización de la salud se presenta como una de las fronteras más críticas de la transformación digital. Los sistemas sanitarios enfrentan desafíos estructurales previos a la tecnología —envejecimiento poblacional, cronicidad, presión financiera— y la tecnología aparece como palanca para mejorar la eficiencia y la continuidad asistencial. Su impacto depende de una visión sistémica: la interoperabilidad, la gobernanza del dato clínico y la integración en los procesos asistenciales son condiciones para evitar soluciones fragmentadas. La equidad atraviesa este debate: la salud digital puede ampliar el acceso, pero también profundizar brechas si no se acompaña de políticas de inclusión digital, formación y diseño centrado en las personas.

07 EDUCACIÓN Y UNIVERSIDADES COMO INFRAESTRUCTURA DEL FUTURO DIGITAL

El Foro sitúa a la educación superior como infraestructura estratégica de la transición digital. Las universidades forman talento, producen conocimiento y articulan capacidades colectivas en un contexto de cambio acelerado. Su transformación digital se vincula a la capacidad de anticipar necesidades, adaptar modelos formativos y reforzar su función pública. La cooperación iberoamericana emerge como condición estructural para avanzar, dada la heterogeneidad de sistemas y recursos. Compartir modelos, métricas y aprendizajes permite escalar experiencias y evitar enfoques aislados. La sostenibilidad se incorpora como eje transversal, conectando la digitalización educativa con la responsabilidad ambiental, ética y social de las instituciones.

08 MULTILATERALISMO, COOPERACIÓN Y ACCIÓN COMPARTIDA

Finalmente, el Foro refuerza el valor de los espacios de diálogo multilateral en un contexto donde estos marcos están siendo cuestionados. La experiencia de Andorra muestra que la cooperación público-privada e internacional sigue siendo una herramienta eficaz cuando se orienta a resultados concretos.

El II Foro Digital de Andorra se consolida así como una plataforma de acción, más que como un espacio de reflexión. Las conclusiones apuntan a la necesidad de pasar del diagnóstico a la ejecución, de las alianzas declarativas a los proyectos compartidos, y de la innovación dispersa a la estrategia coordinada.



FORO DE ANDORRA
Alianzas Público-Privadas
para la Transición Digital

Con el apoyo de:

