

Soberanía Digital

Hacia una autonomía tecnológica real



La dependencia silenciosa

El hardware es tuyo. ¿Y el metadato?

Comparamos dispositivos y servicios creyendo que adquirimos control. La realidad, en lo personal y en lo empresarial, demuestra lo contrario:



Smart TVs

Capturan imágenes de pantalla cada 500 ms y las venden a terceros. En diciembre de 2025, Texas demandó a cinco grandes fabricantes.



Coches conectados

Telemetría y geolocalización enviadas a aseguradoras sin consentimiento claro. La FTC sancionó a GM/OnStar en 2025.



Mensajería y copilotos de IA

Metadatos de WhatsApp (3.500 M de cuentas enumeradas en 2025) y asistentes de IA que han accedido a correos confidenciales.



Los tres pilares de la soberanía digital



Infraestructura

Reducir la dependencia de nubes y procesadores externos. Iniciativas clave: Chips Act, directivas NIS2 y DORA.



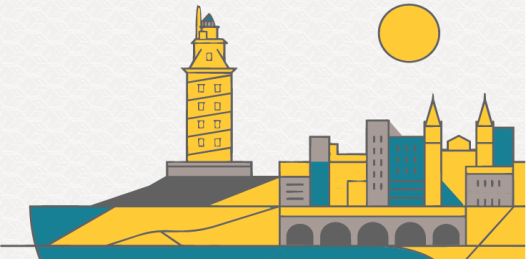
Datos

Lograr que los datos europeos circulen bajo nuestras reglas. Iniciativas clave: Data Act, Gaia-X y protección jurisdiccional.



Identidad

El pilar central que cohesiona el ecosistema: garantiza autoría, acceso y privacidad real para la persona.



La criptografía como **cimiento**

Bajo los tres pilares hay una misma base matemática. Sin ella, todo lo demás son buenas intenciones.



Firma digital

Atribución y confianza

Saber quién hizo qué y que nada se ha alterado. Base de la firma cualificada, eIDAS y las credenciales verificables.



Cifrado

Confidencialidad

Protege los datos en tránsito y en reposo, incluso frente al operador del cloud (computación confidencial).



Conocimiento cero (ZKP)

Privacidad por diseño

Demostrar una afirmación sin revelar el dato subyacente. Minimiza la exposición en cada verificación.



Post-cuántica (PQC)

Resiliencia a futuro

Identidad y datos deben durar décadas. La cripto-agilidad ya es un requisito arquitectónico.



“

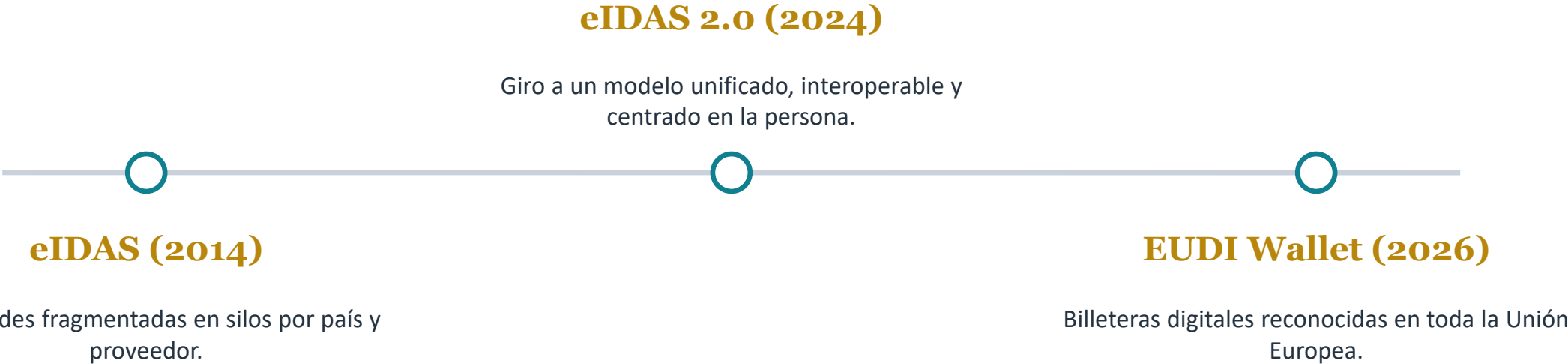
EL PILAR QUE SOSTIENE A LOS OTROS DOS

Datos sin identidad = contrato sin firma.
**Infraestructura sin identidad = caja fuerte con la
llave prestada.**

Por eso nos centramos en la identidad: es la cerradura que datos e infraestructura necesitan para que la soberanía sea real.



Evolución regulatoria



La obligación no es solo para administraciones: bancos, telecom y grandes plataformas serán también partes confiantes.



El triángulo de confianza

Rompiendo el modelo cliente-servidor



Tecnologías descentralizadas



SSI

Identidad autosoberana

El usuario tiene la propiedad exclusiva, el control y la capacidad de portar su identidad, sin atarse a una plataforma corporativa.



VC

Credenciales verificables

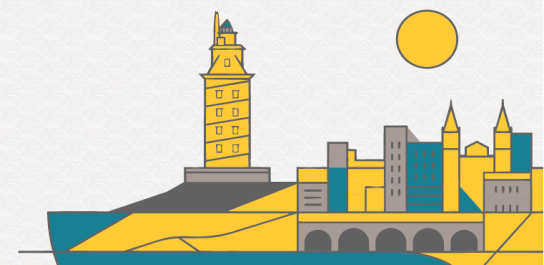
Documentos digitales firmados que el titular custodia y presenta. Comprobables al instante, sin contactar al emisor.



DID

Identificadores descentralizados

Identificadores únicos, persistentes y verificables que no requieren un registro central ni un proveedor de identidad.



Divulgación selectiva (ZKP)

Privacidad criptográfica por diseño: demostrar la validez de una afirmación sin revelar la información subyacente.



¿Eres mayor de edad?

Sí, sin revelar la fecha de nacimiento.



¿Tienes solvencia suficiente?

Sí, sin revelar el salario exacto.



¿Estás titulado en esto?

Sí, sin compartir el expediente entero.

Reduce drásticamente la exposición y la recolección excesiva de datos personales en verificaciones rutinarias.



La barrera de adopción empresarial

El choque entre el legado y la innovación: las organizaciones reales no parten de un lienzo en blanco.



PKI muy enraizadas

Infraestructuras de clave pública integradas en procesos críticos durante años.



IAM y directorios legacy

Gestión de identidad y directorios activos tradicionales en el corazón del negocio.



Sustitución inviable

Es económicamente inviable reemplazar sistemas críticos de la noche a la mañana.



El rol del integrador



Ecosistema SSI

Nuevos formatos de credenciales verificables, billeteras digitales EUDI e identificadores descentralizados.



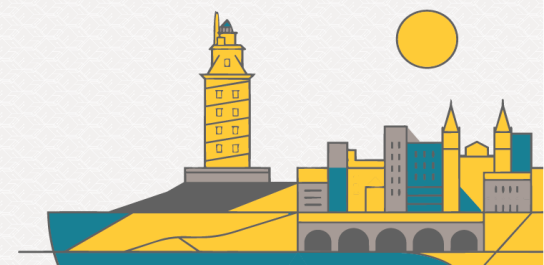
El puente

Perfiles que no solo vendan tecnología, sino que traduzcan y acoplen ambos mundos sin romper la operación.



Sistemas legacy

Infraestructura interna, control de accesos físico, portales corporativos y gestión de identidades tradicional.



Acompañamos desde el conocimiento aplicado a SSI y credenciales verificables.



Probamos eIDAS 2.0, SSI y credenciales verificables en entornos cerrados para anticipar los cuellos de botella.



Validamos emisión, custodia y verificación de credenciales de extremo a extremo antes de llevarlas a un cliente real.



Seguimos y validamos estándares emergentes como OpenID4VCI (emisión) y SD-JWT VC (divulgación selectiva).



Lo que viene: cadena de suministro e IA

Nuestro desarrollo más reciente lleva las credenciales verificables al terreno industrial, acelerado con agentes de IA.



Cadena de suministro verificable

Cada componente y producto lleva credenciales verificables: trazabilidad de extremo a extremo y base para el Pasaporte Digital de Producto europeo.



Desarrollo asistido por IA

Prototipamos emisión y verificación de credenciales con agentes de codificación, iterando sobre los estándares en días, no en meses.



Identidad para los agentes de IA

Cuando un agente de IA actúa en nombre de una organización, también necesita credenciales verificables. El triángulo de confianza se extiende a las máquinas.

Adecuar el esfuerzo al **negocio**



Diagnóstico de madurez

Evaluar el punto de partida tecnológico real del cliente antes de proponer nada.



Ruta escalonada

Adopción por fases que no sobredimensione la infraestructura ni genere deuda técnica.



Encaje por sector

Las preguntas no son iguales en banca, educación o industria: el acompañamiento se adapta.

No existe una solución universal. Cada organización requiere análisis de preventa y consultoría específica.



Gracias

No hay autonomía tecnológica sin identidad digital.

Axians · Innovación y ciberseguridad · www.axians.es