Resolución sobre la Soberanía Digital en las Universidades

Aprobada por unanimidad en la 78.ª Asamblea General Ordinaria el 6 de noviembre de 2025.

Introducción

La universidad pública, en su condición de institución fundamental para el progreso social, la formación de la ciudadanía y la generación de conocimiento, se encuentra en una problemática acerca del uso de datos digitales de los miembros de su comunidad. La transformación digital ha dejado de ser un mero proceso de modernización de infraestructuras para convertirse en la base sobre la que se está construyendo el futuro de la educación superior, la investigación y la transferencia. Hoy en día la infraestructura digital no es un servicio accesorio, sino el pilar sobre el que se asientan todas las funciones esenciales de una universidad.

El marco teóricode esta resolución se basa en que la universidad pública, como custodiadora y generadora de conocimiento, tiene la obligación de garantizar que sus infraestructuras digitales reflejen y protejan sus valores fundamentales, como la autonomía, el acceso universal al conocimiento, la transparencia en la gestión y un compromiso con el servicio público. La transformación digital no puede entenderse como una simple «actualización tecnológica»; es, en su esencia, una cuestión de soberanía que determinará la capacidad de la universidad para cumplir su misión social en pleno siglo XXI, libre de interferencias externas y de la lógica de los mercados.

El control efectivo sobre los datos generados por la comunidad universitaria y sobre las herramientas digitales que median en los procesos de enseñanza, aprendizaje e investigación es un pilar fundamental de la libertad de cátedra y la autonomía universitaria consagrada en la legislación. Ceder este control a entidades privadas, cuyos objetivos comerciales no solo son ajenos, sino a menudo contrapuestos a la misión universitaria, supone una renuncia a la gobernanza de la institución y una amenaza directa a su independencia. Esta resolución se presenta como una hoja de ruta para que el Sistema Universitario Español (público) aborde esta problemática, no como consumidor pasivo de tecnología, sino como agente soberano, capaz él mismo de construir un ecosistema digital propio, abierto, colaborativo y sostenible, que sirva a los intereses de la comunidad universitaria, a la que realmente se debe, y garantice su relevancia y autonomía para las futuras generaciones.

La problemática digital de la Universidad Pública

Análisis del contexto

La digitalización de la educación superior es un proceso de largo recorrido que, sin embargo, ha experimentado una aceleración sin precedentes, provocada por la crisis sanitaria de la COVID-19. Esta situación forzó una transición abrupta y forzosa hacia modelos de docencia y trabajo a distancia, e intensificó de manera drástica la dependencia de las herramientas y plataformas digitales para la comunidad universitaria en la docencia, la investigación y la gestión administrativa. Lo que en muchos casos fue una respuesta reactiva y no planificada «estratégicamente», ha sentado las bases de una nueva normalidad en la que la «mediación tecnológica» está presente en todos lados.

Este cambio de paradigma, si bien ha abierto nuevas posibilidades, también ha expuesto a las universidades a nuevas y significativas vulnerabilidades. La urgencia por mantener la actividad académica llevó a la adopción masiva de soluciones tecnológicas ofrecidas por grandes corporaciones, a menudo bajo la apariencia de ofertas «gratuitas» o de bajo coste inicial. Esta dinámica ha facilitado una penetración profunda de actores comerciales en el núcleo de la actividad universitaria, sentando las bases para lo que podría considerarse una privatización encubierta de recursos, funciones y servicios públicos que son esenciales para la misión de la universidad. La dependencia de estas plataformas no es meramente técnica, sino que también afecta a los flujos internos de trabajo, las metodologías pedagógicas y, de forma crítica, a la gestión y almacenamiento de los datos generados por toda la comunidad universitaria.

La Infraestructura digital como activo estratégico

Es imperativo y urgente redefinir la idea que se tiene de la infraestructura digital universitaria. No puede ser considerada un servicio de «commodity» más, análogo al suministro eléctrico o propiamente la limpieza. La infraestructura digital (que, recordemos, abarca desde los centros de datos y el almacenamiento en la nube hasta las plataformas de aprendizaje (LMS), los sistemas de autenticación de usuarios y las herramientas de colaboración…) constituye un activo estratégico de suma importancia. Hoy en día es el núcleo a través del cual fluye cualquier activo de una universidad.

Quien controla la infraestructura, controla los flujos y canales de información, los datos de la comunidad universitaria y, en última instancia —aunque con la mayor importancia—, posee la capacidad de influir en la propia pedagogía, en las líneas de investigación y en la toma de decisiones institucionales. La pérdida de este control no es una mera decisión de externalización de un servicio técnico; dado que equivale a una cesión de soberanía con consecuencias profundas y a largo plazo. Cuando una universidad cede el almacenamiento de sus datos, las interacciones de su campus virtual o la gestión de las identidades de sus miembros

a una plataforma externa, está entregando las llaves de su activo «más preciado», a menudo sin una comprensión completa de las implicaciones futuras en términos de costes, seguridad, privacidad y autonomía estratégica. Por ello, la gobernanza de la infraestructura digital debe ser una prioridad al más alto nivel posible de la dirección universitaria, equiparable a la gestión académica, económica o propiamente de personal.

Marco normativo y estratégico

La Ley Orgánica del Sistema Universitario (LOSU)

La Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU) introduce un cambio de paradigma en su artículo 12, al consagrar explícitamente el conocimiento científico como un «bien común». Esta declaración tiene implicaciones prácticas directas. La ley obliga a las Administraciones Públicas y a las universidades a promover y contribuir activamente a la «Ciencia Abierta», lo que se materializa en el mandato para el personal docente e investigador de depositar una copia de la versión final de sus publicaciones y los datos de investigación asociados en repositorios institucionales o temáticos de acceso abierto, de forma simultánea a la fecha de publicación.

El apartado 5 de este mismo artículo de la LOSU dice «Los datos, entendidos como aquellas fuentes primarias necesarias para validar los resultados de las investigaciones, deberán seguir los principios FAIR (datos fáciles de encontrar, accesibles, interoperables y reutilizables) y, siempre que sea posible, difundirse en acceso abierto».

Esta obligación legal entra en una contradicción fundamental con el modelo de negocio de muchos proveedores de servicios en la nube privados. Estos modelos se basan, en gran medida, en la retención de los datos dentro de sus ecosistemas y en la imposición de altas barreras de salida, conocidas como costes de egreso de datos o *egress fees,* que penalizan económicamente la transferencia de grandes volúmenes de información fuera de su plataforma. Cuando los datos de investigación de una universidad se almacenan en una de estas nubes, cumplir con el mandato de la LOSU de depositarlos en repositorios de acceso abierto puede verse obstaculizado por costes prohibitivos o dificultades técnicas. La universidad no puede garantizar el conocimiento como «bien común» si los datos que lo sustentan están cautivos en una infraestructura privada con intereses comerciales, normalmente capitalistas y contrapuestos.

Protección de datos

El Reglamento General de Protección de Datos (RGPD), es una normativa de la Unión Europea que establece las reglas relativas a la protección de la privacidad, así como el tratamiento y circulación de los datos personales de sus residentes.

Esta normativa establece un marco riguroso para la protección de los datos personales de las personas físicas. En España, su aplicación se articula a través de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Para las universidades públicas, esto implica diversas obligaciones como «responsables del tratamiento» de los datos de toda su comunidad. Deben garantizar que cualquier tratamiento de datos sea lícito, leal y transparente, y que se apliquen las medidas técnicas y organizativas adecuadas para asegurar su confidencialidad e integridad.

La externalización de servicios a proveedores de nube, especialmente a aquellos cuyas sedes y centros de datos se encuentran fuera del Espacio Económico Europeo, introduce un riesgo significativo en el cumplimiento de esta normativa. La universidad sigue siendo la responsable última de los datos y debe asegurarse de que las transferencias internacionales de estos cumplen con las estrictas garantías exigidas por el RGPD. Mantener los datos en una infraestructura propia o federada bajo jurisdicción europea simplifica enormemente el cumplimiento y otorga a la institución un control directo y verificable sobre la protección de este derecho fundamental.

La ley de gobernanza de datos (DGA)

El Reglamento UE 2022/868, conocido como Ley de Gobernanza de Datos (DGA), tiene como objetivo facilitar la reutilización de determinadas categorías de datos en poder de organismos del sector público y fomentar el intercambio de datos en un entorno «de confianza».

Esta normativa es un respaldo directo al modelo de infraestructuras federadas/colaborativas como BOIRA[1]. Al establecer un marco para el intercambio seguro de datos del sector público, la DGA proporciona el paraguas ideal para que las universidades colaboren, compartan conjuntos de datos de investigación y creen sinergias, todo ello dentro de un marco soberano que refuerza la confianza y garantiza el control público.

Regulación de los mercados y servicios digitales (DMA y DSA)

El Reglamento de Mercados Digitales (DMA) y el Reglamento de Servicios Digitales (DSA) son dos pilares de la estrategia digital europea. La DMA (Reglamento UE 2022/2065) se dirige a las grandes plataformas *online* designadas como «guardianes de acceso» o «gatekeepers» (como Alphabet, Amazon, Apple, Meta o Microsoft), para evitar que abusen de su posición dominante. La DMA impone obligaciones, como garantizar la interoperabilidad con servicios de terceros y prohibir que impidan a los usuarios desinstalar servicios preinstalados. Esto ataca directamente el núcleo del problema del *vendor lock-in*[2], proporcionando a las

[1] Explicado en la página 13: "El proyecto BOIRA como ejemplo de colaboración interuniversitaria"

[2] Explicado en la página 7: "Modelo de negocio del «Vendor Lock-In»"

universidades una base legal para exigir a estos gigantes tecnológicos condiciones más justas y abiertas, y facilitando la migración a soluciones alternativas.

Por su parte, la DSA (Reglamento UE 2022/2065) establece normas sobre la moderación de contenidos y la transparencia de los servicios intermediarios. Aunque su impacto es más indirecto, los principios de transparencia y rendición de cuentas que exige a las plataformas son más fáciles de garantizar por parte de las universidades cuando estas operan sus propios servicios, que cuando dependen de las políticas opacas de un proveedor externo.

El Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, es de obligado cumplimiento para todas las Administraciones Públicas, incluidas las universidades.

El ENS establece una política de seguridad en el uso de medios electrónicos basada en un enfoque de proceso integral y una gestión continua de los riesgos. Uno de sus principios fundamentales es que la responsabilidad última sobre la seguridad de la información y de los servicios recae siempre en la entidad del sector público, incluso cuando la prestación de dichos servicios se externaliza a terceros.

La externalización de servicios críticos a proveedores de nube, especialmente aquellos cuyas sedes y jurisdicciones legales se encuentran fuera de la Unión Europea, introduce complejidades significativas en la gestión de riesgos y el cumplimiento del ENS. La evaluación de riesgos se complica por la falta de transparencia sobre la infraestructura subyacente, y la garantía de control de acceso y trazabilidad se delega en un tercero cuyos mecanismos de auditoría pueden ser opacos o insuficientes.

Una infraestructura propia o una federada, bajo el control directo de las universidades públicas, simplifica drásticamente la implementación de los principios del ENS. Permite una auditoría directa, un control granular de los accesos, una respuesta a incidentes coordinada y es una garantía de que los datos estén sujetos a la jurisdicción y a las normativas de protección de datos europeas. Este modelo se alinea perfectamente con los principios del ENS de seguridad integral, gestión de riesgos soberana y responsabilidad indelegable.

Alineación con estrategias superiores (Agenda España Digital y Europa)

Las universidades deberían inscribirse y alinearse con las estrategias de transformación digital a nivel nacional y europeo. La Agenda España Digital 2026, la Estrategia de Servicios en la Nube para las Administraciones Públicas y las iniciativas europeas como GAIA-X y la Estrategia Europea de Datos, comparten un diagnóstico y un objetivo común: que es la necesidad de promover la soberanía del

dato, la interoperabilidad y la autonomía tecnológica para el sector público europeo.

Estos documentos reconocen que la dependencia excesiva de un número reducido de proveedores tecnológicos no europeos no es solo un riesgo económico, sino también una vulnerabilidad geopolítica. La Estrategia Cloud nacional, establece explícitamente la «soberanía del dato» como un pilar fundamental y promueve un modelo de nube híbrida[3] y multi-proveedor para evitar la dependencia o el *vendor lock-in*. A nivel europeo, GAIA-X busca crear una infraestructura de datos federada, abierta y soberana para Europa, basada en valores como la transparencia, la interoperabilidad y el control de los datos por parte de sus generadores.

Las universidades, como uno de los principales centros de generación de conocimiento e innovación de Europa, no pueden permanecer al margen de esta estrategia. Deben ser protagonistas y no meros consumidores en la construcción de este ecosistema digital soberano. Adoptar un modelo propio y federado no solo les beneficia y responde a sus necesidades internas, sino que contribuye directamente a los objetivos estratégicos de España y de la Unión Europea, reforzando así la autonomía tecnológica.

La LOSU exige apertura y control público del conocimiento. El ENS exige control y responsabilidad sobre la seguridad de la infraestructura tecnológica. Las estrategias nacionales y europeas identifican la dependencia tecnológica como una vulnerabilidad estratégica. La externalización masiva a hiperescalares[4] no europeos contraviene simultáneamente estos tres frentes, dado que dificulta el acceso abierto por los costes de egreso, complica la soberanía de la seguridad por las jurisdicciones extranjeras y profundiza la dependencia estratégica. La adopción de un modelo soberano no es una opción ideológica, sino la vía coherente y responsable para que las universidades públicas cumplan con el marco legal y estratégico que las rige.

La amenaza de la externalización privada

La transición hacia la digitalización ha llevado a muchas universidades a adoptar soluciones tecnológicas privadas de terceros, a menudo sin una evaluación exhaustiva de los riesgos estratégicos a largo plazo. Si bien la externalización puede ofrecer ventajas aparentes en términos de costes iniciales y agilidad de despliegue, esconde un modelo de negocio que, a la larga, resulta perjudicial para

[3] Explicado en la página 12: "Modelos de infraestructuras viables: Infraestructura híbrida"

[4] Los hiperescalaeres son grandes corporaciones que ofrecen servicios de computación en la nube a una escala masiva, utilizando una infraestructura de miles de servidores en centros de datos, como Google Cloud, Microsoft Azure o Amazon Web Services.

los intereses de una institución pública, socavando así su autonomía financiera, su control sobre los datos y su capacidad de innovación.

Análisis de la situación actual

La situación actual en el Sistema Universitario Español (público) es heterogénea. El informe *Universitic2022*, elaborado por CRUE, señala que la externalización de servicios ha retrocedido gracias a una mejora de los procesos de digitalización y de gobiernos internos. Sin embargo, esta visión puede ocultar una realidad más matizada. La pandemia del COVID-19 actuó como catalizador para la adopción acelerada de soluciones «gratuitas» o de bajo coste inicial ofrecidas por las grandes corporaciones tecnológicas, que aprovecharon la crisis para consolidar su posición «privada» en el ecosistema universitario.

Esta penetración se ha producido a menudo a través de la provisión de cuentas institucionales para correo electrónico, almacenamiento en la nube, y herramientas de colaboración. Aunque nominalmente gratuitas o de bajo coste, estas soluciones integran a toda la comunidad universitaria en un ecosistema tecnológico cerrado, generando así una dependencia de facto que los informes de madurez digital, centrados en la implementación de tecnología, pueden no capturar en toda su dimensión estratégica. La gratuidad inicial es, en realidad, el primer paso de una estrategia calculada para asegurar la dependencia a largo plazo.

Modelo de negocio del «Vendor Lock-In»

El principal riesgo estratégico de la externalización masiva a un único proveedor es el fenómeno conocido como «vendor lock-in» o dependencia del proveedor. Se trata de una situación en la que el coste de cambiar de un proveedor a otro es tan prohibitivamente alto (económica, técnica y temporalmente hablando) que el cliente queda efectivamente cautivo, forzado a continuar con el proveedor original independientemente de la calidad del servicio o de los aumentos de precio. Este modelo no es un efecto secundario indeseado, sino el núcleo de una estrategia de negocio de muchos grandes proveedores de servicios en la nube.

Las tácticas usadas para generar esta dependencia son sistemáticas y siguen un patrón bien definido.

Precios de captación y adaptación masiva

La estrategia comienza con ofertas iniciales extremadamente atractivas, a menudo gratuitas para el sector educativo o con descuentos significativos. El objetivo es eliminar las barreras económicas de entrada y fomentar una adopción masiva y rápida. Una vez que la universidad migra sus servicios esenciales (correo, almacenamiento, LMS) y sus datos a la plataforma, el primer anclaje está fijado.

Aumento exponencial y unilateral de precios

Tras un periodo inicial, y una vez que la institución ha integrado profundamente el servicio en sus operaciones diarias y depende de él para funcionar, los precios de renovación se incrementan de forma drástica y, a menudo, unilateral. El proveedor es consciente de que la universidad ya no tiene una alternativa fácil. Los recientes y anunciados aumentos de precios en las licencias de Microsoft 365 y Google Workspace, que afectan directamente al sector educativo, son una prueba fehaciente de esta práctica. La universidad se encuentra entonces ante una disyuntiva: aceptar precios que puedan duplicarse o triplicarse o afrontar el coste y el trastorno masivo de una migración que normalmente tiene obstáculos y trabas.

Creación de barreras a la migración

Para asegurar que la migración sea lo más difícil posible, los agentes involucrados implementan una serie de barreras técnicas y económicas:

Coste de egreso: se aplican tarifas elevadas por transferir datos de la universidad fuera de la nube del proveedor. Para una institución con petabytes de datos de investigación, académicos y administrativos, estos costes pueden ascender a cientos de miles o incluso millones de euros, haciendo la migración económica inviable.

Formatos de datos propietarios: los datos se almacenan a menudo en formatos específicos del proveedor, que no son fácilmente compatibles con otros sistemas. Esto requiere complejos y costosos procesos de conversión de datos para poder utilizarlos en una plataforma alternativa.

Dependencia de servicios específicos: las aplicaciones y los flujos de trabajo se construyen utilizando APIs y servicios que son exclusivos del ecosistema del proveedor. Migrar a otro entorno implica reescribir y rediseñar gran parte de las aplicaciones dependientes, algo que es un esfuerzo técnico ingente.

Consecuencias para la universidad pública

La sumisión a este modelo de negocio tiene consecuencias devastadoras para una institución pública.

Erosión de la autonomía financiera y estratégica

La universidad pierde por completo el control sobre una partida presupuestaria cada vez más crítica. La planificación financiera a largo plazo se vuelve imposible, ya que los presupuestos de TI quedan a merced de las decisiones de precios de corporaciones multinacionales cuyo único objetivo es maximizar el beneficio de sus accionistas. La capacidad de la universidad para invertir en sus propias prioridades estratégicas se ve mermada por la necesidad de hacer frente a costes de licencias cada vez más crecientes e impredecibles.

Riesgos para la propiedad intelectual y privacidad

Almacenar los datos de una universidad (especialmente los más sensibles como investigaciones en curso, datos de estudiantes, evaluaciones, comunicaciones internas), en plataformas y servicios de terceros, crea una «caja negra». Los términos de servicio, a menudo largos y ambiguos, pueden otorgar al proveedor derecho sobre el uso y análisis de estos datos para sus propios fines comerciales. Esto supone una amenaza directa a la propiedad intelectual generada en la universidad y a la privacidad y los derechos fundamentales de toda la comunidad universitaria.

Además, los datos pueden quedar sujetos a legislaciones de terceros países, como la CLOUD Act de EE.UU., que podría permitir el acceso a los mismos por parte de autoridades extranjeras.

Pérdida de capacidades técnicas internas

La externalización sistemática de la gestión de la infraestructura y de los servicios digitales conduce a la «atrofia» del talento propio. La universidad deja de ser un lugar donde se crea y gestiona tecnología para convertirse en un mero consumidor. Esta pérdida de conocimiento interno hace a la institución aún más dependiente de los proveedores externos para cualquier necesidad futura, perdiendo la capacidad de innovar, de adaptar las herramientas a sus necesidades pedagógicas específicas y de formar sus propios técnicos expertos.

Comparativa de modelos de provisión de servicios TI

La dependencia de un proveedor no solo es un problema de costes presentes, sino que hipoteca la capacidad de la universidad para adoptar futuras tecnologías o modelos pedagógicos que no sean compatibles con el ecosistema del proveedor. Si una universidad queda atrapada en el ecosistema de un proveedor, todos sus procesos, datos y la formación de su personal se adaptan a ese ecosistema. Si surge una nueva tecnología o metodología pedagógica prometedora basada en un estándar abierto u ofrecida por un sistema no compatible con el sistema del proveedor, la universidad no puede adaptarla fácilmente porque los costes y la complejidad de la migración desde el proveedor actual son prohibitivos. El resultado es que la universidad se ve forzada a esperar a que su proveedor dominante decida (o no) incorporar una versión similar de esa innovación, perdiendo agilidad y quedando rezagada. El *vendor lock-in* actúa como un impuesto a la innovación futura, ahogando así la capacidad de la universidad para evolucionar de forma autónoma.

Característica	Modelo Soberano (Propio/Federado)	Modelo Externalizado (Proveedor Privado)
Coste Total de Propiedad (TCO)	Inversión inicial en hardware/personal más alta;	Coste inicial bajo; costes recurrentes impredecibles y

	costes operativos predecibles y controlados a largo plazo.	crecientes (riesgo de subidas de precios).
Control y Propiedad de los Datos	Total y sin ambigüedades. Los datos residen en infraestructura propia y bajo jurisdicción nacional/europea.	Control cedido. Sujeto a los términos de servicio del proveedor y a jurisdicciones extranjeras (ej. CLOUD Act). Riesgo de explotación de datos.
Soberanía Digital	Máxima. La institución define la tecnología, las políticas de acceso y la evolución de los servicios.	Nula o muy baja. Dependencia total de la hoja de ruta, tecnología y políticas del proveedor.
Riesgo de Dependencia (Lock-in)	Mínimo. Basado en estándares abiertos y software libre que garantizan la portabilidad e interoperabilidad.	Máximo. Diseñado para crear barreras técnicas y económicas a la salida.
Flexibilidad y Adaptabilidad	Alta. Las soluciones se pueden adaptar a las necesidades pedagógicas y de investigación específicas de la universidad.	Baja. La institución se adapta a la oferta estandarizada del proveedor. La personalización es limitada o costosa.
Cumplimiento Normativo (ENS/RGPD)	Directo y verificable. La auditoría y el control están bajo la gestión directa de la institución.	Complejo y delegado. Requiere confianza en el proveedor y auditorías de terceros. Complejidad jurídica transfronteriza.

Hacia un modelo soberano

Frente al modelo de dependencia y riesgo que supone la externalización «acrítica», es necesario articular una alternativa robusta, viable y alineada con la misión de la universidad pública. Este modelo soberano no implica un rechazo a la tecnología, sino una apropiación estratégica de la misma, que se basa en principios de control públicos, estándares abiertos y la inversión en capacidades propias.

Principios fundamentales de la gobernanza de datos, la transparencia y el control público

El pilar de un modelo soberano es una gobernanza de datos sólida y bien definida. Esto implica establecer un marco institucional que defina claramente quién es el propietario de los datos generados u obtenidos por la universidad, quién puede acceder a ellos y bajo qué condiciones. Se debe implementar un sistema de roles y responsabilidades, como los definidos en el marco de la ENS, que distinga entre el «Responsable de la información» (quien establece los requisitos de seguridad y uso). El «Responsable de servicio» (quien garantiza su prestación) y el «Responsable de seguridad» (quien vela por el cumplimiento de políticas).

Sin embargo, la mera definición de estos roles resulta insuficiente y fácilmente quebrantable si los datos y servicios residen en infraestructuras externas, especialmente aquellas sujetas a jurisdicciones extranjeras o construidas sobre hardware de proveedores que plantean riesgos para la soberanía digital. Por ello, en los casos en los que, de forma excepcional y transitoria, sea estrictamente necesario utilizar servicios externos, se deben definir contractualmente y auditar de forma rigurosa estos roles, como establece el ENS. Estas soluciones deben entenderse siempre como temporales y no como parte de la estrategia de infraestructura a largo plazo de la universidad.

Este modelo de gobernanza debe ser transparente y basarse en los valores académicos de la universidad, no en los intereses comerciales de un proveedor. Esto implica clasificar los datos según su nivel de criticidad y sensibilidad, y aplicar políticas de acceso y uso diferenciadas. Los datos de investigación, los expedientes académicos, o la información personal de la comunidad universitaria deben ser tratados con el máximo nivel de protección, en infraestructuras que garanticen su control real y residencia bajo jurisdicción europea.

Software libre y estándares abiertos

Una de las herramientas más poderosas para construir un ecosistema digital soberano es la adopción estratégica de software libre (Open Source) y estándares abiertos. Es crucial desmitificar la percepción errónea de que el software libre es inherentemente menos seguro que el software propietario. Por el contrario, cuando está respaldado por una comunidad de desarrollo activa y es gestionado por un equipo técnico competente, el software libre puede ser significativamente más seguro. Su principal ventaja es la transparencia, porque el código fuente es público y puede ser auditado por la propia institución o por expertos independientes para detectar vulnerabilidades, algo imposible en el software propietario de «caja negra».

Prevención del *Vendor Lock-In*

Al basarse en estándares abiertos, garantiza la interoperabilidad y la portabilidad de los datos, eliminando las barreras de salida y permitiendo a la universidad cambiar de solución o de proveedor de soporte sin quedar cautiva.

Flexibilidad y adaptabilidad

El software libre puede ser modificado y adaptado para satisfacer las necesidades pedagógicas, de investigación o de gestión específicas de la universidad. En lugar de adaptar sus procesos a una herramienta rígida, la universidad puede adaptar la herramienta a sus procesos.

Fomento de la colaboración y el conocimiento

El uso de software libre promueve una cultura de colaboración, tanto dentro de la universidad como con otras instituciones. Los equipos técnicos no son meros administradores de licencias, sino que pueden contribuir al desarrollo de las herramientas, generando un conocimiento valioso que se retiene en la universidad.

Inversión estratégica en capital humano (priorizar el personal propio)

Esta resolución aboga por un cambio de paradigma fundamental en la gestión de los recursos universitarios: considerar el gasto en personal técnico altamente cualificado no como un coste operativo, sino como una inversión estratégica en la capacidad y soberanía de la universidad. La tendencia a reducir las plantillas de personal propio en favor de la subcontratación de servicios es una estrategia cortoplacista que, a la larga, debilita a la institución.

Se insta a los equipos de gobierno a priorizar la contratación, formación continua y retención de personal técnico especializado en la creación, despliegue y mantenimiento de los servicios digitales. Un equipo técnico robusto y competente es la garantía última de la soberanía digital. Es este capital humano el que permite a la universidad gestionar su propia infraestructura, adaptar el software libre a sus necesidades, responder con agilidad a los nuevos retos y, en definitiva, ser dueña de su futuro digital. Esta inversión no solo asegura la soberanía, sino que crea empleo de alta cualificación, retiene el conocimiento técnico crítico dentro de los muros de la universidad y refuerza su papel como motor de innovación.

Modelos de infraestructuras viables

La implementación de un modelo soberano no implica necesariamente que cada universidad debe construir y mantener un gran centro de datos de forma aislada. Existen varios modelos de infraestructura viables que pueden adaptarse a la escala y las capacidades de cada institución.

Infraestructura propia

En este modelo, cada universidad gestiona su propio centro de datos para alojar sus servicios críticos. Es el modelo de máxima soberanía, pero puede requerir una inversión inicial significativa y una masa crítica de personal técnico.

Infraestructura híbrida

Este modelo combina el uso de recursos propios (nube privada) para los datos y aplicaciones más críticos y sensibles, con el uso de servicios de nube pública para cargas de trabajo menos sensibles, picos de demanda o aplicaciones específicas. La clave de un modelo híbrido soberano es que la gobernanza, la orquestación y el

control permanezcan en manos de la universidad, utilizando la nube pública como un recurso flexible, pero no como el depositario de sus activos estratégicos.

Un modelo híbrido soberano, en línea con la Estrategia Cloud nacional, debe basarse en un marco de interoperabilidad que garantice la reversibilidad de las cargas de trabajo. Esto se consigue mediante el uso de estándares abiertos y componentes reutilizables que permitan mover datos y aplicaciones entre la nube privada y la pública sin «fricciones técnicas» ni costes prohibitivos. El uso de proveedores de nube pública debe limitarse a cargas de trabajo no sensibles o picos temporales de demanda, asegurando que los datos críticos y las aplicaciones esenciales residan siempre en la infraestructura propia, bajo el control directo de la universidad. Este enfoque evita que la nube pública se convierta en una vía de un solo sentido y preserva la autonomía estratégica de la institución.

Infraestructura federada/colaborativa

Este es, quizás, el modelo más prometedor y eficiente para el Sistema Universitario Español (Público). Consiste en que múltiples universidades agrupen sus recursos (financieros, técnicos y de hardware) para crear y gestionar una infraestructura de nube compartida. Este enfoque permite alcanzar importantes economías de escala, compartir costes de inversión y mantenimiento, y crear un equipo técnico de alto nivel al servicio de todas las instituciones participantes, todo ello sin ceder el control a un tercer comercial. Es un modelo que une las ventajas de la nube (elasticidad y eficiencia) con los principios del servicio público y la soberanía.

Casos de éxito y modelos de referencia

El proyecto BOIRA como ejemplo de colaboración interuniversitaria

El proyecto BOIRA es la prueba de concepto de que el modelo de infraestructura federada/colaborativa es una de las soluciones más estratégicas y eficientes para el Sistema Universitario Español público. Nacido de una propuesta de la Universidad de Zaragoza en el marco de los proyectos Unidigital, BOIRA es una infraestructura de nube compartida entre varias universidades públicas españolas, inicialmente la propia Universidad de Zaragoza, la Universidad de Almería y la Universidad del País Vasco.

Su principal fortaleza reside en su concepción soberana desde el origen, porque está construida íntegramente sobre hardware propio de las universidades y gestionada exclusivamente con software libre. Esta elección tecnológica garantiza la independencia total de proveedores comerciales y el control absoluto sobre las plataformas.

Desde un punto de vista técnico, su arquitectura es robusta y abierta. Utiliza tecnologías estándar y de código abierto como OpenNebula para la gestión y orquestación de la nube, y Ceph como sistema de almacenamiento distribuido, escalable y resiliente. La interconexión entre las tres sedes universitarias se realiza a través de la red académica y de investigación española, RedIRIS, que garantiza una comunicación de alta capacidad, segura y al margen de las redes comerciales.

Este diseño distribuido no solo asegura la soberanía, sino que también proporciona una alta disponibilidad y continuidad de servicio para las aplicaciones críticas alojadas en la plataforma, ya que permite el despliegue de instancias replicadas en diferentes sedes.

El proyecto, además de ser una realidad operativa, tiene una clara visión de futuro, con planes para establecer un dominio propio y alinearse con proyectos estratégicos europeos de infraestructura en la nube (IPCEI-CIS).

Moodle como estándar abierto para la docencia

Moodle es otro ejemplo de una solución de software libre que ha alcanzado un nivel de madurez, robustez y funcionalidad que lo convierte en el estándar de facto para la gestión del aprendizaje (LMS) en la mayoría de las universidades españolas. Sin embargo, el verdadero potencial soberano de Moodle solo se materializa cuando se despliega en una infraestructura controlada por la propia universidad, ya sea en un servidor local o en una nube federada como BOIRA.

Una implementación autogestionada de Moodle otorga a la institución el control total sobre la plataforma de enseñanza-aprendizaje, específicamente de los datos de los estudiantes, las interacciones pedagógicas, las calificaciones y los contenidos. Permite una personalización profunda de la plataforma para adaptarla a modelos pedagógicos específicos (o los que prevea la propia universidad), integrar herramientas de terceros de forma segura y desarrollar internamente nuevas funcionalidades que respondan a las necesidades de la comunidad docente e investigadora. Este modelo contrasta radicalmente con la cesión de la plataforma LMS a un proveedor externo, donde la universidad se convierte en un simple inquilino de una plataforma cerrada y sus datos en un activo para el proveedor.

El Consorci de Serveis Universitaris de Catalunya (CSUC)

El CSUC representa un modelo consolidado y de gran escala de colaboración interuniversitaria que va más allá de una única infraestructura. Este consorcio, que agrupa a las universidades catalanas, mancomuna una amplia gama de servicios académicos, científicos y de gestión. Entre ellos se incluyen la conectividad de alta capacidad (Anella Científica), servicios en la nube, acceso a supercomputación, repositorios para la ciencia abierta y, de forma muy relevante, la realización de compras conjuntas de software y equipamiento TIC.

La experiencia del CSUC demuestra que la colaboración institucional a nivel regional puede generar enormes eficiencias, optimizar la inversión pública y, crucialmente, fortalecer la posición negociadora de las universidades frente a los proveedores tecnológicos. Al actuar como un bloque unificado, las universidades pueden obtener mejores condiciones y exigir estándares más altos de apertura y seguridad.

Iniciativas inspiradas en la administración pública

Barcelona y la plataforma DECIDIM

El Ayuntamiento de Barcelona ha impulsado el desarrollo de Decidim, una plataforma de participación ciudadana basada íntegramente en software libre. Este proyecto demuestra cómo una institución pública puede liderar la creación de su propia infraestructura digital soberana para una función democrática crítica, y cómo esta solución, al ser abierta, puede ser adoptada y mejorada por cientos de otras instituciones en todo el mundo.

Estrategia cloud nacional

La propia Estrategia de servicios en la nube híbrida para las Administraciones Públicas del Gobierno de España promueve un modelo multi-nube e interoperable, que reconoce explícitamente la necesidad de garantizar la «soberanía del dato» y de diseñar un sistema capaz de evitar la estrategia de negocio *vendor lock-in*.

Conclusión

Síntesis

En esta resolución se puede comprobar cómo el Sistema Universitario Español (público) se enfrenta a una decisión estratégica de gran importancia con respecto al futuro digital de sus universidades. La trayectoria actual, marcada por una creciente externalización de servicios de infraestructura digital a un número reducido de grandes proveedores comerciales, representa una amenaza para la autonomía, la sostenibilidad financiera y la misión pública de la universidad. Este modelo conduce a la dependencia del proveedor (*vendor lock-in*), a la pérdida de control sobre los datos y la propiedad intelectual, y a la erosión de las capacidades técnicas internas.

Se ha demostrado que esta deriva no solo es estratégicamente imprudente, sino que contraviene el espíritu del marco legal y estratégico vigente. La Ley Orgánica del Sistema Universitario, con su defensa del conocimiento como bien común y la Ciencia Abierta; el Esquema Nacional de Seguridad, con su exigencia de control y responsabilidad indelegable; y las estrategias digitales de España y la Unión

Europea, con su llamada a la soberanía del dato y la autonomía tecnológica, nos hacen entender que debe de producirse un importante cambio de rumbo.

Frente a este modelo de riesgo, existe una alternativa soberana, viable y alineada con los valores universitarios. Un modelo basado en la colaboración interuniversitaria, la adopción de software libre y estándares abiertos, y una inversión decidida en el capital humano propio. La viabilidad técnica, económica y organizativa de este modelo no es una hipótesis, sino una realidad demostrada por casos de éxito como el Proyecto BOIRA, la gestión autónoma de plataformas como Moodle y la de consorcios como el CSUC.

Soluciones

Las universidades públicas deben realizar una auditoría estratégica de sus servicios e infraestructuras digitales. Dicha auditoría deberá evaluar el nivel de dependencia de proveedores externos, cuantificar los riesgos asociados al *vendor lock-in* (incluyendo costes de egreso de datos y barreras técnicas a la migración) y analizar la conformidad de los contratos vigentes con la legislación en materia de protección de datos, seguridad y ciencia abierta.

Se debe realizar un cambio estructural en las políticas de personal de las universidades públicas para que se reconozca y priorice la contratación, estabilización y formación continua de personal técnico especializado en la gestión de infraestructuras, seguridad y servicios digitales. Este personal debe ser considerado una inversión estratégica en la capacidad y autonomía de la institución, frente al modelo de subcontratación sistemática.

Si a últimas instancias, y en casos excepcionales y transitorios en los que sea imprescindible recurrir a servicios externos, se han de empezar procesos de nueva contratación o renovación de servicios digitales (plataformas de aprendizaje, servicios de almacenamiento en la nube, sistemas de autenticación, herramientas de colaboración), los pliegos de condiciones técnicas y administrativas deben priorizar de forma explícita y vinculante las soluciones basadas en software libre y estándares abiertos. Se deberá exigir a los licitadores garantías contractuales de portabilidad total de los datos en formatos estándar y de reversibilidad completa del servicio sin costes penalizadores. Se deberá exigir también contractualmente la definición explícita y la auditoría rigurosa de los roles y responsabilidades conforme a lo establecido en el ENS, garantizando que la responsabilidad última y el control efectivo permanezcan en la universidad.

Es necesario elaborar y dotar presupuestariamente un Plan Estratégico Nacional para la Soberanía Digital del Sistema Universitario Español. Este plan deberá fomentar y financiar la creación de nuevas federaciones de infraestructura compartida, siguiendo el modelo del Proyecto BOIRA, con el objetivo de extender esta red a todas las universidades públicas del territorio nacional.

Promover activamente entre la comunidad universitaria la adopción, el desarrollo y la mejora continua de plataformas autogestionadas como Moodle, desplegadas sobre infraestructuras soberanas (propias o federadas).

Se debe declarar en la Ley Orgánica del Sistema Universitario la soberanía digital como un principio rector, irrenunciable de la universidad, indisociable de la autonomía universitaria.

Bibliografía y fuentes documentales

ABD. (2025). *Microsoft actualiza precios y facturación*. ABD. https://www.abd.es/2025/01/microsoft-actualiza-precios-y-facturacion/

Agencia Estatal de Investigación. (2022). *Modelo Convenio Colaboración subprograma infraestructuras*. Ministerio de Ciencia e Innovación. https://www.aei.gob.es/sites/default/files/convocatory_info/2022-08/Modelo_Convenio_Colaboracion_subprograma_infraestructuras%20fin.doc

Ajuntament de Barcelona. (s.f.). *Barcelona se convierte en capital mundial de las tecnologías abiertas con la primera Open Tech Week*. Participació Ciutadana. https://ajuntament.barcelona.cat/participaciociutadana/es/noticia/barcelona-se-convierte-en-capital-mundial-de-las-tecnologias-abiertas-con-la-primera-open-tech-week_1558305

Amazon Web Services. (2021). *Caso de éxito: Cómo el Monasterio de São Bento de Río de Janeiro adaptó su plataforma EAD Moodle para asistir a clases 100% en línea debido a COVID-19*. AWS. https://aws.amazon.com/es/blogs/aws-spanish/caso-de-exito-como-el-monasterio-de-sao-bento-de-rio-de-janeiro-adapto-su-plataforma-ead-moodle-para-asistir-a-clases-100-en-linea-debido-a-covid-19/

Boira. (s.f.). *Página de inicio*. Boira. https://boira.es/

Buendata. (s.f.). *Moodle en la Educación Superior: Transformando el Aprendizaje en Universidades y Centros de Educación*. Buendata. https://buendata.com/moodle-en-la-educacion-superior-transformando-el-aprendizaje-en-universidades-y-centros-de-educacion/

Cast AI. (2023). *Vendor Lock-In and How To Break Free*. Cast.ai. https://cast.ai/blog/vendor-lock-in-and-how-to-break-free/

Cloudflare. (s.f.). *What is vendor lock-in?*. Cloudflare. https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/

Comisión Europea. (s.f.). *Una Europa adaptada a la era digital*. Comisión Europea. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es

Comisión Europea. (s.f.). *Capacidades digitales*. Estrategia Digital Europea. https://digital-strategy.ec.europa.eu/es/policies/digital-skills

Comisión Europea. (2020). *Estrategia Europea sobre Software de Código Abierto 2020-2023*. Datos.gob.es. https://datos.gob.es/es/blog/nueva-estrategia-europea-sobre-software-de-codigo-abierto-2020-2023

Consorci de Serveis Universitaris de Catalunya. (s.f.). *Página de inicio*. CSUC. https://www.csuc.cat/es

Crue Universidades Españolas. (2023). *Informe UNIVERSITIC 2022: Análisis de las TIC en las Universidades Españolas*. Crue. https://www.crue.org/wp-content/uploads/2023/11/Universitic-2022-Crue.pdf

Delgado, M., & Oliver, R. (2006). *La aplicación de las tecnologías de la información y la comunicación en la educación superior*. RED. Revista de Educación a Distancia. https://www.um.es/ead/red/17/delgado_oliver.pdf

European University Association. (s.f.). *Digital transition*. EUA. https://www.eua.eu/our-work/topics/digital-transition.html

European University Association. (2024). *Safeguarding academic and digital sovereignty: A model for action*. EUA. https://www.eua.eu/our-work/expert-voices/safeguarding-academic-and-digital-sovereignty-a-model-for-action.html

Gaia-X España. (s.f.). *Iniciativa de los espacios de datos*. Gaia-X Spain. https://www.gaiax-spain.com/iniciativa-de-los-espacios-de-datos/

Gobierno de España. (2022). *España Digital 2026*. España Digital. https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

Gobierno de España. (s.f.). *Ley Orgánica del Sistema Universitario (LOSU)*. Ministerio de Ciencia e Innovación. https://www.ciencia.gob.es/Estrategias-y-Planes/GobernanzaEstrategica/LOSU.html

Gobierno de España. (2022). *Universidades presenta la Ley Orgánica del Sistema Universitario con un amplio consenso de la comunidad educativa y científica*. Ministerio de Ciencia e Innovación. https://www.ciencia.gob.es/site-web/Noticias/2022/Mayo/universidades-presenta-ley-organica-sistema-universitario.html

Gobierno Vasco. (2023). *Estrategia de Gobernanza de los Datos de Euskadi*. Euskadi.eus. https://www.euskadi.eus/contenidos/informacion/estrateg_gobernanza_del_dato2/es_def/adjuntos/estrategia_de_gobernanza_de_los_datos_es.pdf

Goom Spain. (s.f.). *Incremento de los precios de servicios cloud de Microsoft*. Goom Spain. https://www.goomspain.com/en/incremento-de-los-precios-de-servicios-cloud-de-microsoft/

Google Cloud. (s.f.). *¿Qué es el gobierno de datos?*. Google Cloud. https://cloud.google.com/learn/what-is-data-governance?hl=es

Google. (s.f.). *Controlar qué servicios de Google están disponibles para los usuarios*. Ayuda de Administrador de Google Workspace. https://support.google.com/a/answer/14206754?hl=es

Gros, B., & Contijoch, M. (2021). *Pandemia y privatización en la Educación Superior. Tecnologías de la educación y reforma de la universidad*. RedCLADE. https://redclade.org/noticias/pandemia-y-privatizacion-en-la-educacion-superior-tecnologias-de-la-educacion-y-reforma-de-la-universidad/

Harraca, M. (2025). *Martín Harraca: "Soberanía digital y el rol de las universidades"*. Noticias UNSAM. https://noticias.unsam.edu.ar/2025/08/27/martin-harraca-soberania-digital-y-el-rol-de-las-universidades/

Hernández, V. M., & Cabrera, L. (2021). *Transformación Digital en Educación Superior*. Revista Latinoamericana de Difusión Científica. https://revistalatam.digital/article/22tr03/

IBM. (s.f.). *¿Qué es el gobierno de datos?*. IBM. https://www.ibm.com/mx-es/think/topics/data-governance

Jefatura del Estado. (2022). *Ley 11/2022, de 28 de junio, General de Telecomunicaciones*. Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

KPMG. (2023). *Principales novedades de la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario*. KPMG. https://assets.kpmg.com/content/dam/kpmg/es/pdf/2023/05/legal-alert-novedades-LO-2-2023-Sistema-Universitario.pdf

MasterBorn. (2023). *Cloud Vendor Lock-in: 4 Real-Life Scenarios and Lessons Learned*. MasterBorn. https://www.masterborn.com/blog/cloud-vendor-lock-in-4-real-life-scenarios-and-lessons-learned

Moodle. (s.f.). *Educación más alta*. Moodle. https://moodle.com/es/noticias/categoria-19/historias-de-exito/educacion-mas-alta/

Nubens. (2023). *Suben los precios de Google Workspace*. Nubens. https://nubens.com/noticias/suben-precios-google-workspace/

Open IT. (s.f.). *Reduzca el gasto recurrente en software mediante la optimización de licencias*. Open IT. https://openit.com/es/reduce-recurrent-software-spend-through-license-optimization/

Plataforma de Contratación del Sector Público. (2023). *Anuncio de formalización de contratos de: Presidencia de la Agencia Estatal de Administración Tributaria*. Contrataciondelestado.es.

https://contrataciondelestado.es/wps/wcm/connect/PLACE_es/Site/area/docAccCmpnt?srv=cmpnt&cmpntname=GetDocumentsById&source=library&DocumentIdParam=81216788-4a61-4550-b1d3-ff623fcd4449

Pohle, J., & Teh, B. (2022). *Soberanía digital*. EconStor. https://www.econstor.eu/bitstream/10419/264177/1/Full-text-article-Pohle-et-al-Soberania-digital.pdf

Real Instituto Elcano. (2021). *El reto de la soberanía tecnológica: hacia un ecosistema digital europeo propio*. Real Instituto Elcano. https://www.realinstitutoelcano.org/analisis/el-reto-de-la-soberania-tecnologica-hacia-un-ecosistema-digital-europeo-propio/

RedIRIS. (2024). *Proyecto Boira*. Jornadas Técnicas RedIRIS 2024. https://rediris.es/jt/jt2024/programa/ponencias/?id=jt2024-jt--a17b3c4.Proyecto%20Boira%20-%20JJTT%202024.pdf

Rovira, C., & Fernández, S. (2021). *El desafío de las universidades en la era digital*. Trayectorias Universitarias. https://revistas.unlp.edu.ar/TrayectoriasUniversitarias/article/download/12566/11351/42645

Secretaría General de Administración Digital. (2022). *Estrategia Cloud de la Administración General del Estado*. PAe. https://administracionelectronica.gob.es/pae_Home/dam/jcr:f9ceb19b-882b-4221-8476-10d59305ff10/2022_12_Estrategia_Cloud_AAPP.pdf

Tecnozero. (2025). *Aumento de precios en Microsoft 365 para el 1 de abril de 2025: ¡Descubre cómo te afectará!*. Tecnozero. https://www.tecnozero.com/blog/aumento-de-precios-en-microsoft-365-para-el-1-de-abril-de-2025-descubre-como-te-afectara/

Universidad de Ámsterdam. (s.f.). *Preserving digital sovereignty of universities and researchers*. Universiteit van Amsterdam. https://www.uva.nl/en/about-the-uva/policy-and-regulations/general/preserving-digital-sovereignty-of-universities-and-researchers/preserving-digital-sovereignty-of-universities-and-researchers.html

Universidad de Cantabria. (2023). *La UC participa en el informe 'Universitic 2022', el estudio de referencia sobre las TIC en las universidades españolas*. Web Unican. https://web.unican.es/noticias/Paginas/2023/11/informe-Universitic-2022-.aspx

Universidad de Murcia. (s.f.). *Proyecto Nube Colaborativa BOIRA*. Unidigital. https://unidigital.um.es/proyectos/nube-colaborativa-boira/

Universidad de Valladolid. (2020). *Política de Seguridad de la Información*. Secretaría General UVa. https://secretariageneral.uva.es/_documentos/II.14.-Politica-Seguridad-UVa.pdf

Universidad de Zaragoza. (s.f.). *Esquema Nacional de Seguridad*. ENS Unizar. https://ens.unizar.es/

Vera, J. (2002). *El proceso de investigación*. REDALYC. https://www.redalyc.org/pdf/547/54701701.pdf

Wikipedia. (s.f.). *Consorcio de Servicios Universitarios de Cataluña*. Wikipedia. https://es.wikipedia.org/wiki/Consorcio_de_Servicios_Universitarios_de_Catalu%C3%B1a

Wikipedia. (s.f.). *Soberanía digital*. Wikipedia. https://es.wikipedia.org/wiki/Soberan%C3%ADa_digital