Material docente para la formación del PDI

Autor:
SANTOS MANUEL CAVERO LÓPEZ

FACULTAD DE COMERCIO Y TURISMO
UNIVERSIDAD COMPLUTENSE DE MADRID

UNIVERSIDAD COMPLUTENSE MADRID

RESPONSABILIDAD LEGAL Y ÉTICA DE LA TECNOLOGÍA EN EL AULA EN LA FACULTAD DE COMERCIO Y TURISMO

UNIVERSIDAD COMPLUTENSE MADRID

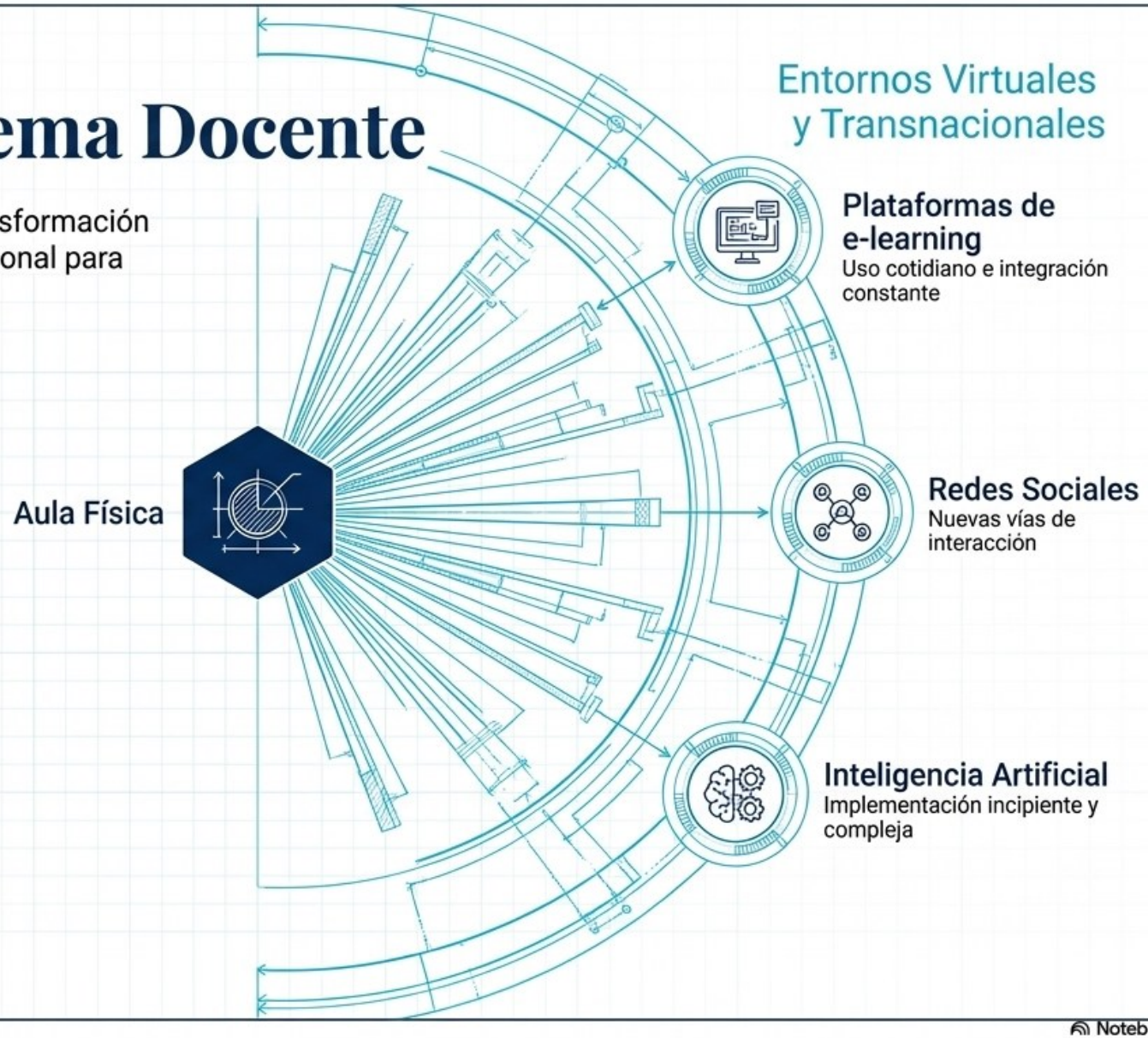
RESPONSABILIDAD LEGAL Y ÉTICA DE LA TECNOLOGÍA EN EL AULA EN LA FACULTAD DE COMERCIO Y TURISMO

Este curso aborda las responsabilidades que surgen al integrar herramientas tecnológicas en la docencia, desde plataformas de e-learning y redes sociales hasta la inteligencia artificial. El objetivo es proporcionar un marco de actuación seguro para proteger tanto a los alumnos como al propio docente.

Sección	**Contenido**
1ª Parte	El caso de "la app de calificaciones" y debate inicial.
2ª Parte	Los cuatro pilares de la responsabilidad digital (RGPD, Propiedad, Accesibilidad, IA).
3ª Parte	Simulacro de crisis.

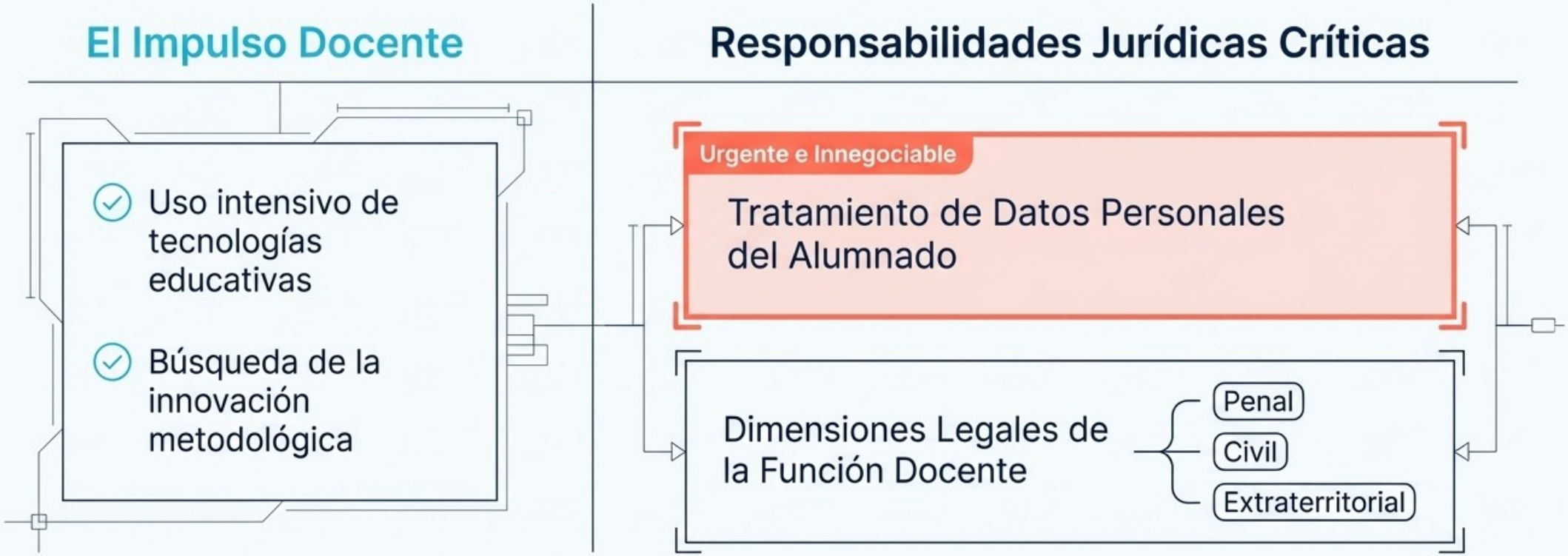
El Nuevo Ecosistema Docente

La labor docente ha experimentado una transformación profunda, trascendiendo el aula física tradicional para consolidarse en una realidad ineludible, enriquecedora y compleja.



Estos recursos enriquecen significativamente el proceso de enseñanza-aprendizaje y fomentan la innovación metodológica.

La Paradoja de la Innovación: Retos y Vulnerabilidades



La adopción tecnológica no está exenta de vulnerabilidades. Exige una reflexión profunda sobre las implicaciones de nuestras decisiones operativas.

Nuestro Objetivo: Un Marco de Actuación Seguro

Ciclo 1 / 4º Seminario: Responsabilidad legal y ética del uso de la tecnología (Facultad de Comercio y Turismo)

Ponente: Santos Cavero | **Duración:** 2 horas

A través de marcos normativos actualizados y la resolución de casos prácticos, esta sesión dota al profesorado de las herramientas necesarias para innovar sin cruzar los límites legales.

PRIMERA PARTE

INCIDENTE_REF: UCM-CCT-11-202X

Anatomía de una Crisis Digital

El Caso de la “App de Calificaciones”

REPORTE DE INCIDENTE: SHADOW IT Y VULNERACIÓN DE DATOS (RGPD)

Imaginemos por un momento una situación cotidiana en nuestra propia Facultad de Comercio y Turismo de la Universidad Complutense de Madrid: estamos a mediados de noviembre, en el pico más alto del cuatrimestre, y las entregas de trabajos se acumulan, las tutorías se multiplican y la presión por ofrecer una docencia de calidad, interactiva y moderna es constante.

En este contexto, pongámosle rostro a nuestro protagonista: llamémosle Carlos, un profesor titular, profundamente comprometido con su alumnado y siempre dispuesto a mejorar sus metodologías.

EXPEDIENTE: ANTECEDENTES_01

El Protagonista y el Dilema Operativo

ESTADO ACTUAL
Campus Virtual UCM (Moodle)

- Percibido por Carlos (Profesor Titular) como **tosco**, lento y poco intuitivo.
- Presión máxima a mediados de noviembre por entregas acumuladas.

LA VISIÓN
Innovación Deseada

- Feedback dinámico y corrección ágil.
- Comunicación de notas en tiempo real directo al **smartphone** del alumno.

CONTEXTO: 150 estudiantes. Asignatura con evaluación continua semanal.

Investigando en foros de innovación educativa, descubre una aplicación externa, una app de origen estadounidense que está ganando muchísima popularidad entre docentes de todo el mundo, debido a que su interfaz es brillante, promete una analítica de datos espectacular sobre el rendimiento del aula y, lo mejor de todo, es gratuita.

Matriz de Decisión: El Espejismo de la Innovación

Dimensión	Moodle Oficial	App Externa ('De Moda')
Experiencia de Usuario (UX)	Lenta / Tradicional	Brillante / Analítica espectacular
Coste Económico	Incluido	Gratuita
Ubicación de Servidores	Red UCM / Unión Europea	Estados Unidos (Fuera de la UE)
Auditoría y Contrato RGPD	Aprobado por IT	Inexistente (Shadow IT)

CONCLUSIÓN DIAGNÓSTICA: La decisión se basó únicamente en la capa visible (UX y coste), ignorando por completo la infraestructura legal subyacente y el riesgo catastrófico.

Investigando en foros de innovación educativa, descubre una aplicación externa, una app de origen estadounidense que está ganando muchísima popularidad entre docentes de todo el mundo, debido a que su interfaz es brillante, promete una analítica de datos espectacular sobre el rendimiento del aula y, lo mejor de todo, es gratuita.

EXPEDIENTE: VECTOR_DE_ATAQUE_03

La Anatomía del “Shadow IT”

SHADOW IT: Uso de tecnología en la sombra. Operar en la clandestinidad digital sin el filtro, auditoría ni firma de un contrato de Encargado de Tratamiento por parte de los servicios informáticos.

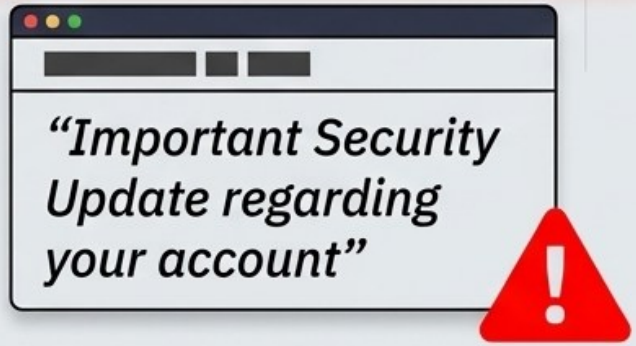
EXPEDIENTE: TIMELINE_INCIDENTE_04

El Punto de Inflexión: La Trampa Temporal

Mes 1 y 2: Funcionamiento Perfecto

Viernes por la Tarde

- Agilización de notas y feedback.
- Gráficos detallados de evolución.
- Transformación digital aparente.



LA REALIDAD: Brecha de seguridad masiva. Hackers vulneran los servidores estadounidenses de la compañía.

EXPEDIENTE: AUDITORIA_DE_DAÑOS_05

Nivel de Exposición: ¿Qué se filtró a la Dark Web?

NIVEL DEVASTADOR

NIVEL CRÍTICO

AMBER BAUGE

NIVEL DEVASTADOR: Evaluaciones Subjetivas

Comentarios privados de evaluación del profesor sobre el rendimiento, actitud y capacidad individual de cada estudiante.

NIVEL CRÍTICO: Base de Datos Académica

Historial académico detallado de la clase, registro de calificaciones continuas y listado de suspensos.

NIVEL BÁSICO: Datos de Registro

Nombres, apellidos, correos electrónicos universitarios y fotografías de perfil de 150 alumnos.

ESTADO ACTUAL:
Dominio Público.
Cero capacidad de contención.

EXPEDIENTE: IMPACTO_MULTILATERAL_06

El Impacto: Lunes por la Mañana

08:01 | 08:15

FRENTE 1: MEDIOS DE COMUNICACIÓN

La noticia salta a **medios tecnológicos** durante el fin de semana. **Daño reputacional inmediato.**

08:32 | 08:45

FRENTE 2: ALUMNADO

150 estudiantes asustados al ver sus **datos personales y académicos expuestos.** Pánico generalizado en el aula.

08:01 | 08:15

FRENTE 3: FAMILIAS

Quejas formales y exigencias de responsabilidades legales por parte de los **padres** (especialmente de alumnos menores/jóvenes).

08:22 | 08:45

FRENTE 4: INSTITUCIÓN

Citación urgente y bloqueo institucional. Remitentes: Decanato y Delegado de Protección de Datos (DPD).

Antes de poder procesar la situación, la bandeja de entrada colapsa. La crisis técnica es ahora una crisis humana e institucional.

EXPEDIENTE: AUTOPSIA_LEGAL_07

Análisis de Crisis I: Responsabilidad Legal y Económica

El Origen de la Culpa

CONCEPTO: Transferencia no autorizada

Aunque la falla técnica es de la empresa externa, la realidad legal dicta que el docente obligó o incentivó la cesión de datos a un tercero sin garantías. Es una vulneración directa del RGPD al enviar datos de ciudadanos europeos a servidores desconocidos.

¿Quién asume la Sanción?

CONCEPTO: Responsabilidad Subsidiaria

La universidad, como empleadora, responde subsidiariamente frente a la Agencia Española de Protección de Datos (AEPD). Sin embargo, ante una negligencia clara, el patrimonio personal del profesor podría estar en riesgo mediante acciones de repetición internas.

EXPEDIENTE: AUTOPSIA_ÉTICA_08

Análisis de Crisis II: El Daño Moral y Ético

Datos Altamente Sensibles

Las calificaciones y los fracasos académicos (suspensos) no son datos triviales; **definen el historial y la intimidad** del estudiante.

Daño Psicológico Severo

Revelar públicamente comentarios críticos genera estrés agudo, ansiedad y daño irreparable a la reputación y reputación y autoestima del alumno.

Quiebra de Confianza

Destrucción total del aula como un entorno de aprendizaje seguro, privado y confidencial.

Más allá de las multas y los expedientes, el factor humano revela el verdadero abismo: ¿Cómo se repara el daño psicológico de 150 alumnos traicionados por una "innovación" negligente?

EXPEDIENTE: PROTOCOLO_ACTUACIÓN_09

Protocolo de Emergencia: La Regla de las 72 Horas

[72:00:00]

01. Descubrimiento

El profesor detecta la pérdida, sustracción o hackeo de los datos de la plataforma.

02. Notificación Inmediata

Comunicación urgente e ineludible al Delegado de Protección de Datos (DPD) de la universidad.

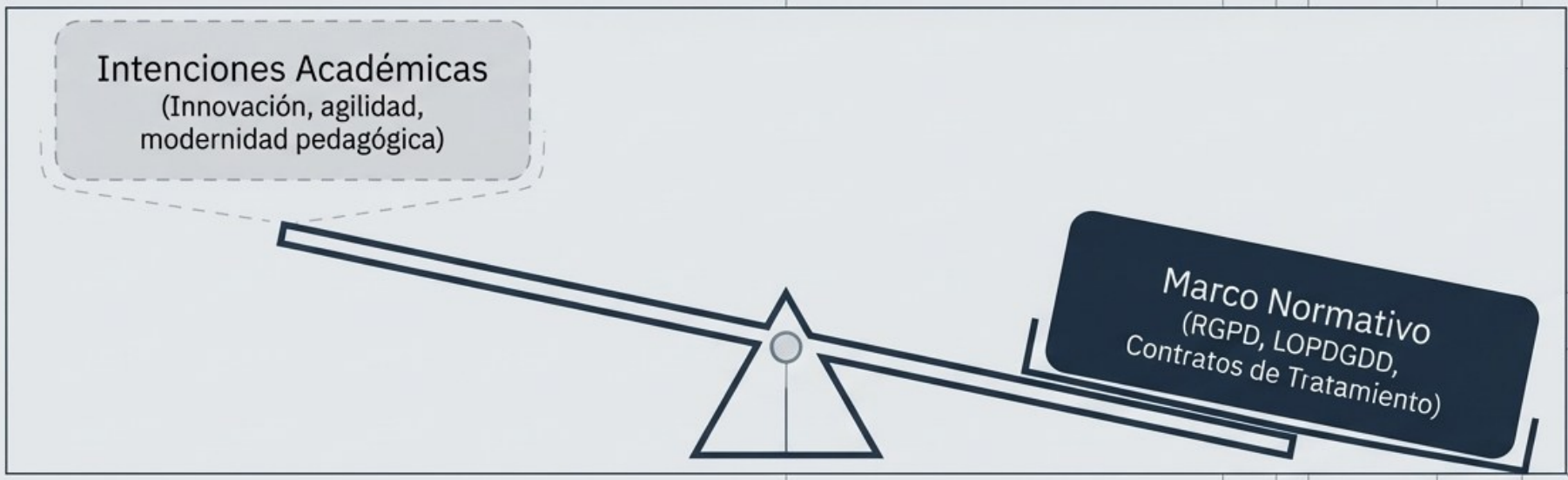
03. Aviso a la Autoridad

La institución tiene un plazo legal estricto de 72 horas para notificar la brecha a la AEPD.

NORMATIVA CRUE: La suspensión de los plazos administrativos NO afecta a las quiebras de seguridad. El reloj no se detiene en fines de semana.

EXPEDIENTE: SÍNTESIS_FINAL_10

La Paradoja de las Buenas Intenciones



En el entorno digital, las buenas intenciones pedagógicas nunca anulan el marco normativo.

La innovación tecnológica sin una red de seguridad jurídica no es transformación digital; es una negligencia que expone tanto al estudiante como a la institución.

1. Datos: El Marco LOPDGDD

Ley Orgánica 3/2018 (LOPDGDD) - Título X: Derechos digitales en el entorno educativo.

El Ecosistema RGPD

La AEPD sanciona prácticas negligentes; el uso de estos canales institucionales es de obligado cumplimiento.

2. Propiedad Intelectual: La frontera legal

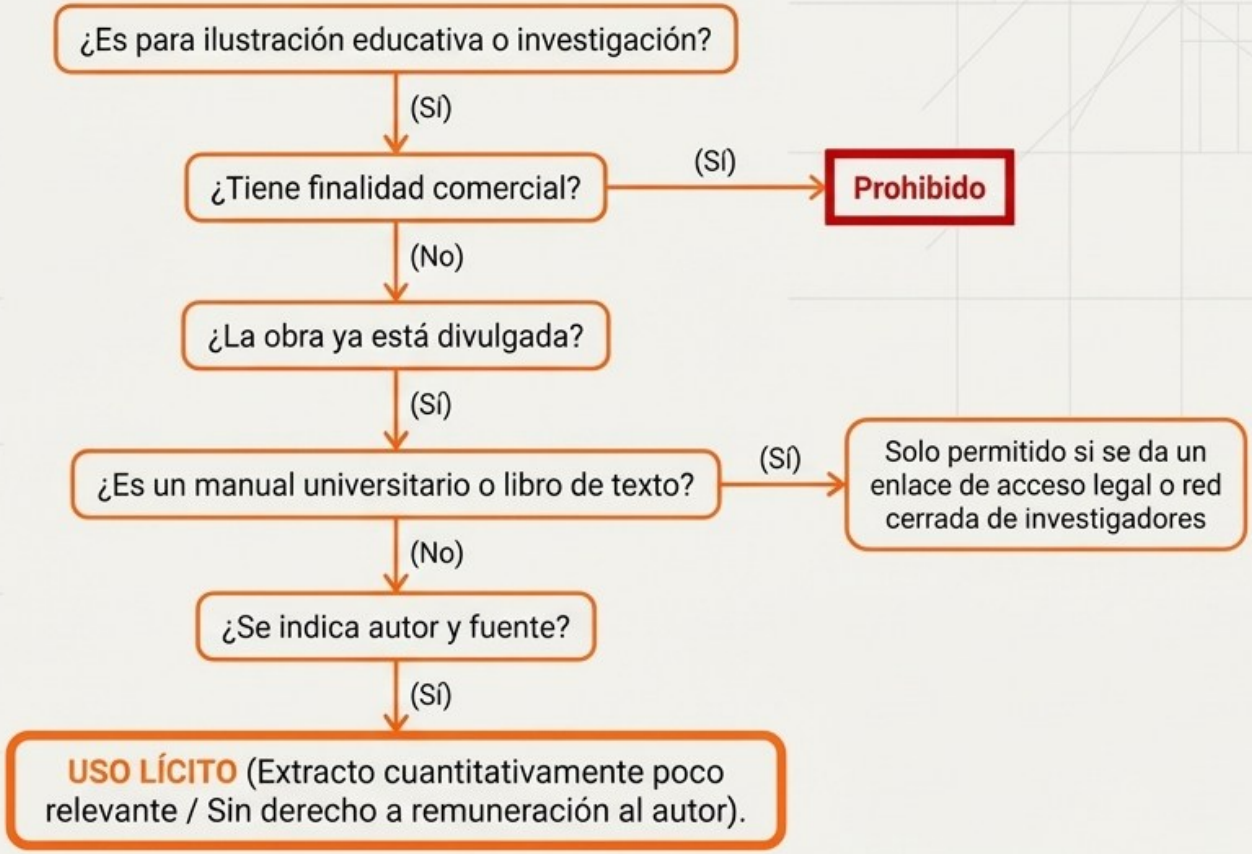
Texto Refundido de la Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996).

INFRACCIÓN DIRECTA: Subir obras completas o manuales escaneados al campus virtual sin permiso.

LA EXCEPCIÓN DOCENTE (Art. 32.3): "Ilustración con fines educativos". Permite usar pequeños fragmentos de obras ajenas sin pedir permiso al autor, sujeto a condiciones estrictas.

Validando el Artículo 32.3: Pequeños Fragmentos

Árbol de Decisión Visual



La Regla del 10% (Artículo 32.4)

Reproducción parcial sin autorización limitada a un capítulo de libro, artículo de revista o extensión equivalente al 10% del total de la obra.

La Regla del 10%

ON 1. ¿Realizado en la Universidad, por su personal y con medios propios?

ON 2. ¿Distribuido exclusivamente entre alumnos matriculados y PDI del centro?

ON 3. ¿Alojado en redes internas y cerradas (Campus Virtual)?

⚠ Si no se cumplen estas condiciones, los autores/editores tienen derecho irrenunciable a remuneración equitativa (CEDRO).

3. Accesibilidad: La obligación de no dejar a nadie atrás

RD 1112/2018 (Accesibilidad de sitios web públicos) y **RD Legislativo 1/2013** (Diseño **Universal**).

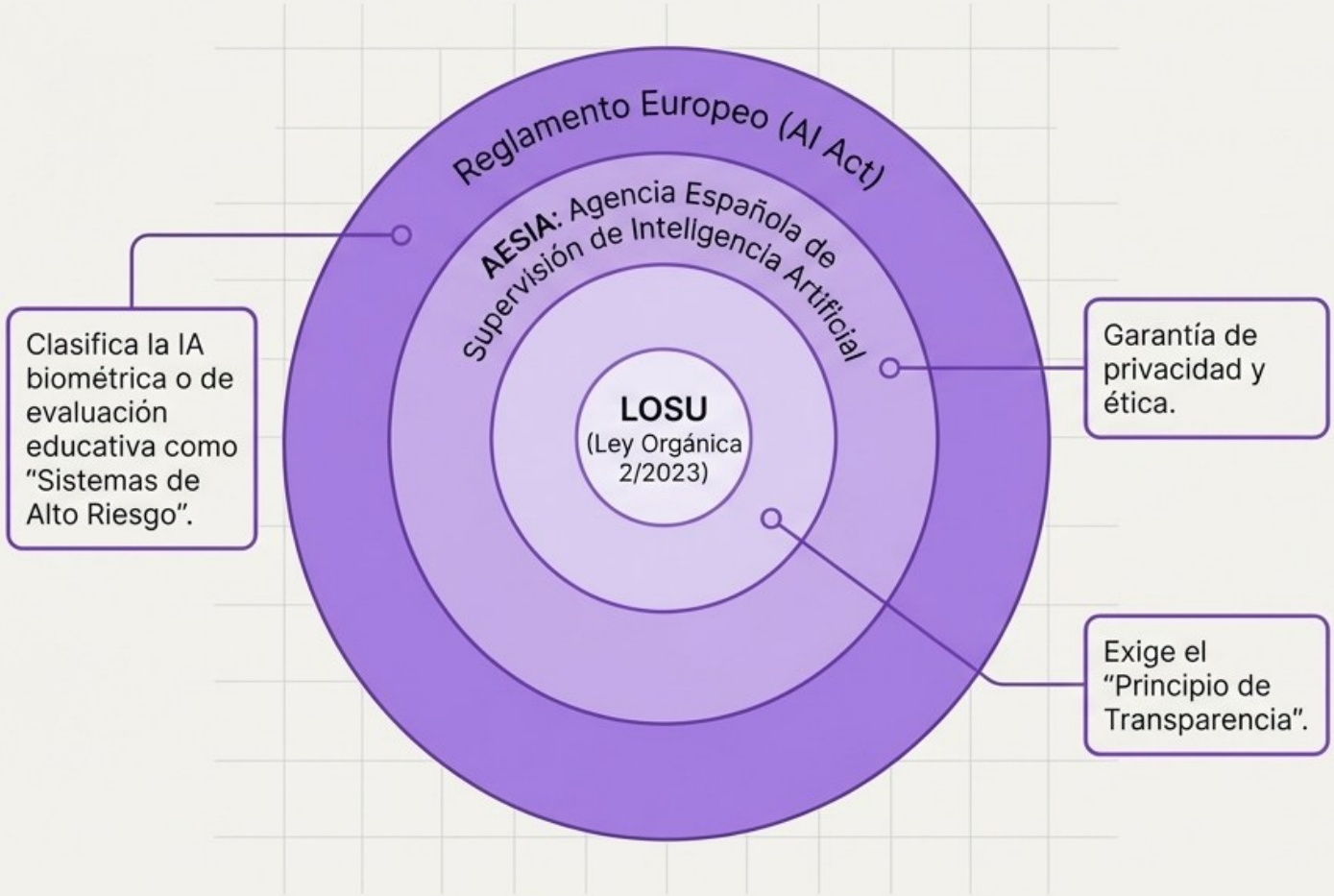
Vulnerar esta legislación es atentar contra la igualdad de oportunidades.

Los contenidos digitales obligatoriamente deben ser:

- Perceptibles
- Operables
- Comprensibles
- Robustos

El Embudo de la Accesibilidad

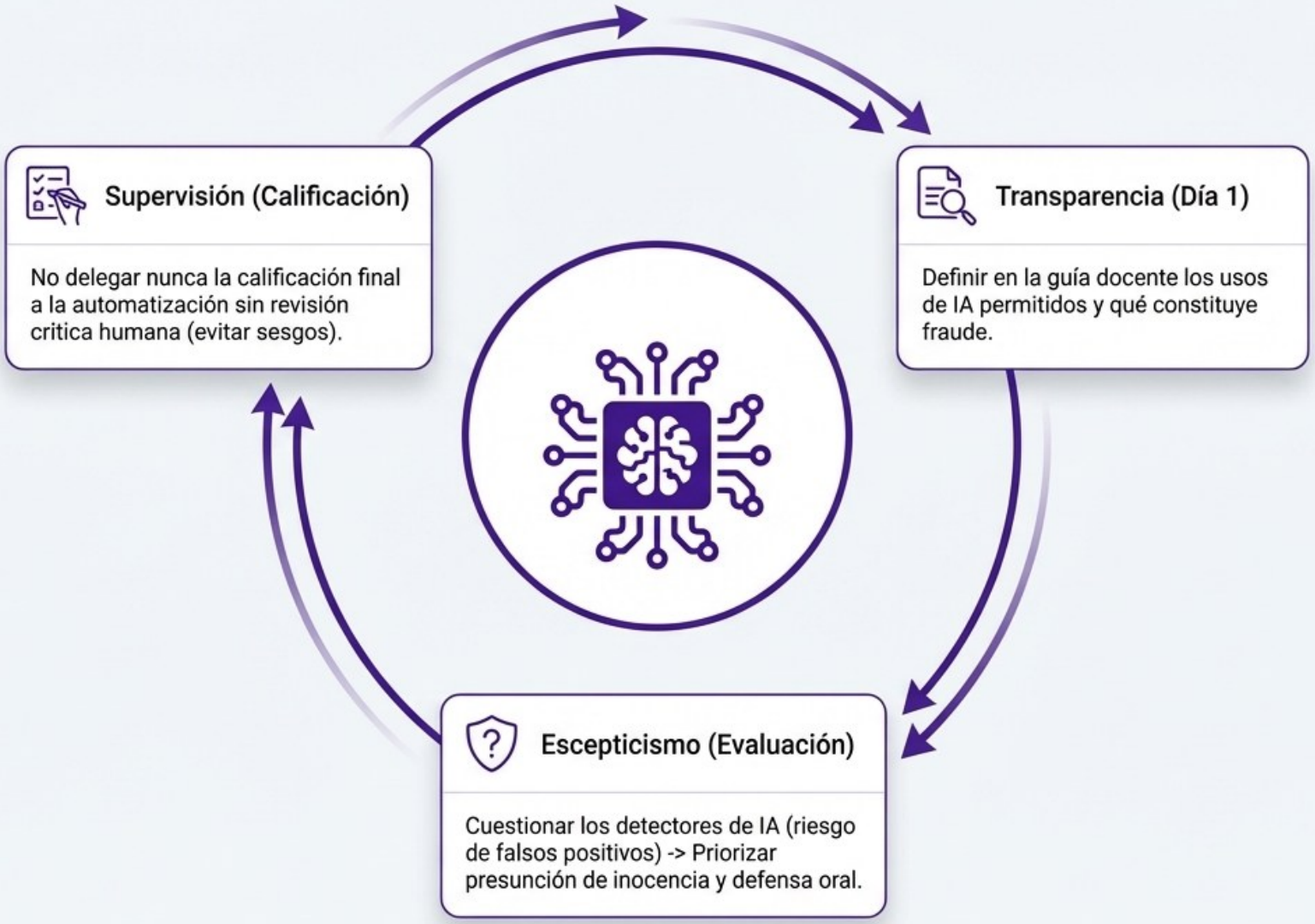
4. Inteligencia Artificial: La nueva frontera regulatoria



Es obligatorio detallar claramente en las Guías Docentes el uso permitido de herramientas IA para garantizar la equidad académica.

Matriz de Integración Normativa: El "Cheat Sheet" del Docente

Pilar Legal	Normativa Clave	Límite Práctico Docente	Canal / Herramienta Segura
Protección de Datos	LOPDGDD / RGPD	Prohibido exponer datos (ej. DNI completo, emails personales) sin base legal.	Plataformas institucionales auditadas / Canales AEPD.
Propiedad Intelectual	LPI (Art. 32)	Regla del 10% o pequeño fragmento para fines docentes.	Campus Virtual (red cerrada).
Accesibilidad	RD 1112/2018	Prohibido software incompatible o PDFs ilegibles.	Diseño universal (Perceptible y Operable).
Inteligencia Artificial	AI Act / LOSU	IA de evaluación es "alto riesgo".	Transparencia obligatoria en la Guía Docente.

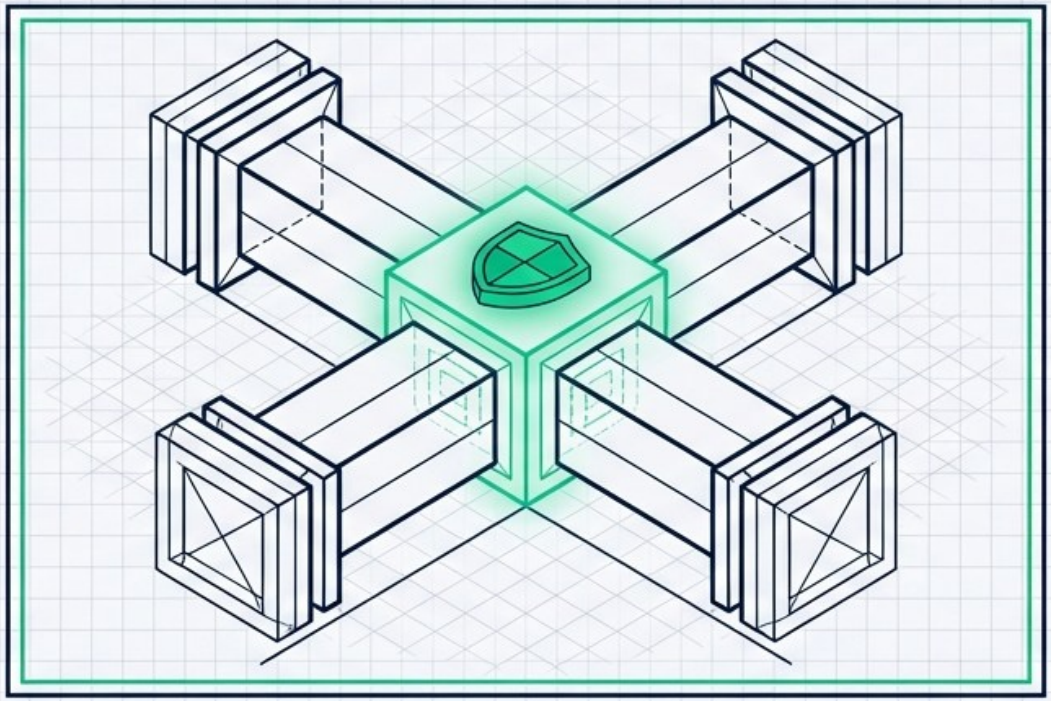

Supervisión (Calificación)
No delegar nunca la calificación final a la automatización sin revisión critica humana (evitar sesgos).
Transparencia (Día 1)
Definir en la guía docente los usos de IA permitidos y qué constituye fraude.
Escepticismo (Evaluación)
Cuestionar los detectores de IA (riesgo de falsos positivos) -> Priorizar presunción de inocencia y defensa oral.

La Matriz de Seguridad

Pilar	Objetivo Principal	Prevención (Qué hacer)	Línea Roja (Qué evitar)
Protección de Datos	Minimización	Usar solo entornos institucionales	Plataformas externas sin contrato
Propiedad Intelectual	Doble respeto	Marcas de agua y Creative Commons	Ignorar la venta de apuntes propios
Accesibilidad	Cero barreras	Diseño universal y planes B	Exigir apps de pago o hardware premium
Ética IA	Transparencia	Reglas claras en la guía docente	Delegar calificación al algoritmo

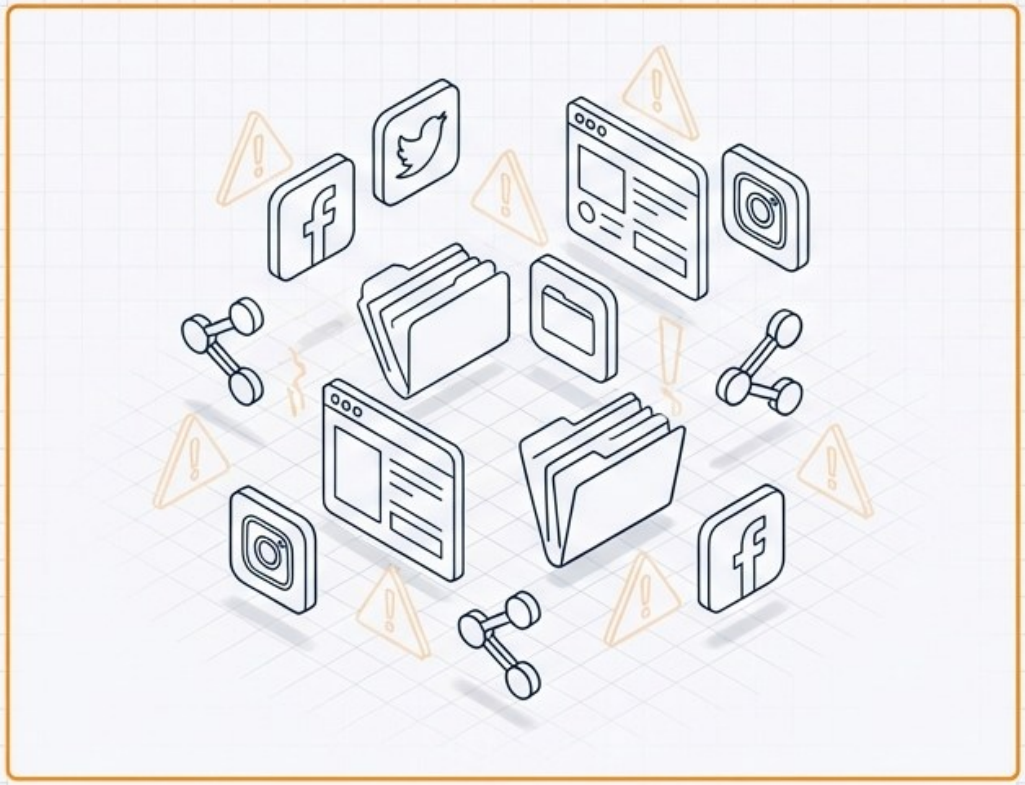
LOS PILARES DE LA RESPONSABILIDAD DIGITAL DEL DOCENTE

Guía de actuación segura para el entorno universitario

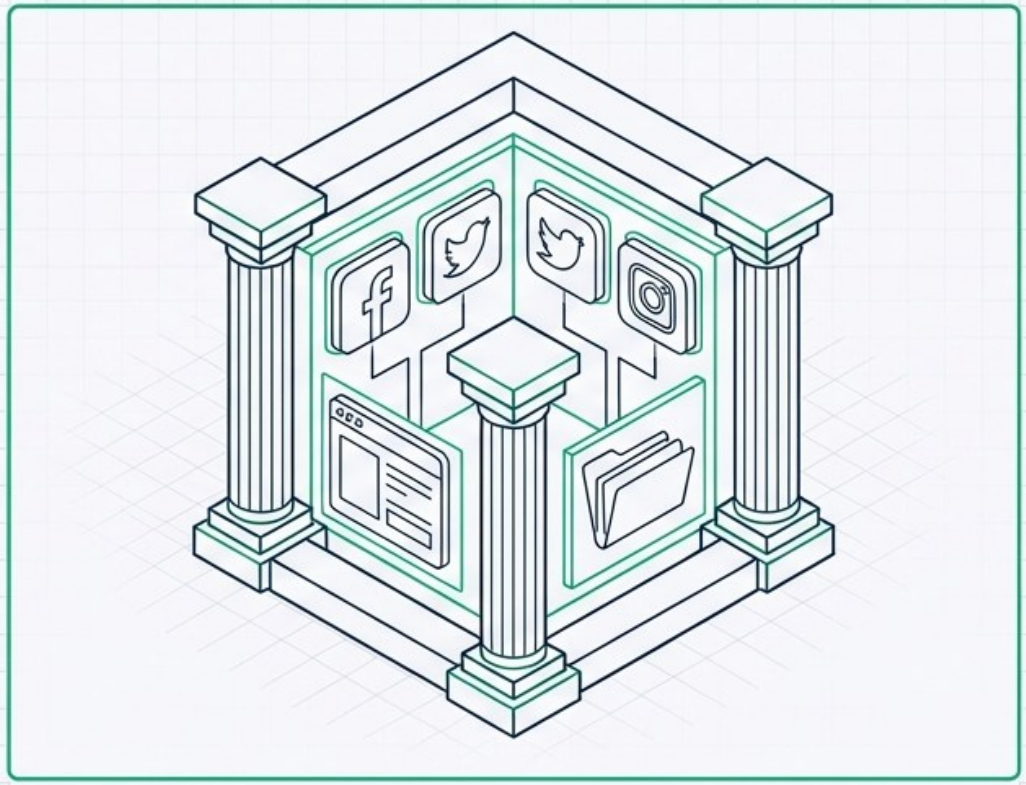


De la vulnerabilidad a la seguridad estructural

La tecnología trae innovación, pero también exposición. El objetivo no es rechazar las herramientas digitales, sino utilizar el derecho positivo como un escudo protector para garantizar una educación justa, segura y de calidad.



Innovación sin marco jurídico.



Innovación protegida.

El marco arquitectónico de la docencia digital

Cuatro fundamentos de obligado cumplimiento que estructuran la responsabilidad del profesorado en la Facultad de Comercio y Turismo.

1. Protección de Datos (RGPD)

2. Propiedad Intelectual

3. Accesibilidad y Equidad

4. Ética de la Inteligencia Artificial (IA)

Pilar 1: La anatomía del rastro digital del alumno

El concepto de ‘dato personal’ bajo el RGPD abarca cualquier información que permita identificar al estudiante, directa o indirectamente.

Nombre y Apellidos

Correo Electrónico Personal
(Asociable a un usuario)

Dirección IP
(Rastreada al contestar cuestionarios)

Calificaciones
(Evaluación continua)

Fotografía
(Perfil del campus virtual)

Bajo ninguna justificación “innovadora” se puede solicitar la cesión de estos datos a plataformas de terceros no auditadas.

AEPD. https://www.aepd.es/preguntas-frecuentes/0-conceptos-basicos/FAQ-0001-que-es-un-dato-personal

Un dato personal es cualquier información sobre una persona física que permita identificarla, directa o indirectamente, como por ejemplo un nombre, un número de identificación (nº del DNI, de tarjeta de crédito, o de cualquier otro documento personal), datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

¿Es la dirección de correo electrónico un dato personal?

En los casos en que la dirección de correo electrónico contenga información acerca de su titular que lo identifique ha de ser considerada como dato de carácter personal (nombre y apellido, Nº DNI…). Por ejemplo, una dirección del tipo nombre.apellido@compañía.com sería un dato personal.

Por el contrario, en los supuestos en los que la dirección de correo electrónico no contenga datos relacionados con el titular de la cuenta no nos encontramos ante un dato de carácter personal, a no ser que otros datos (dominio, domicilio, etc.), conjunta o separadamente, permitan la identificación del sujeto, en cuyo caso, la dirección de correo electrónico se consideraría dato personal. Por ejemplo, una dirección del tipo gestion@compañía.com no sería un dato personal.

Por tanto, cuando la dirección de correo electrónico contenga información que permita la identificación de su titular, o en la medida en que se pueda asociar al mismo, ha de ser considerada como dato de carácter personal y su tratamiento sometido al Reglamento General de Protección de Datos.

¿Qué es un tratamiento de datos personales?
Cualquier operación realizada sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Redes Sociales obligatorias en asignaturas de Marketing Turístico/Digital

- *El problema:*

  Una práctica común para evaluar es pedir a los alumnos que creen una cuenta de Instagram o TikTok y lancen una campaña para un destino turístico o producto comercial, evaluando sus likes o interacciones.

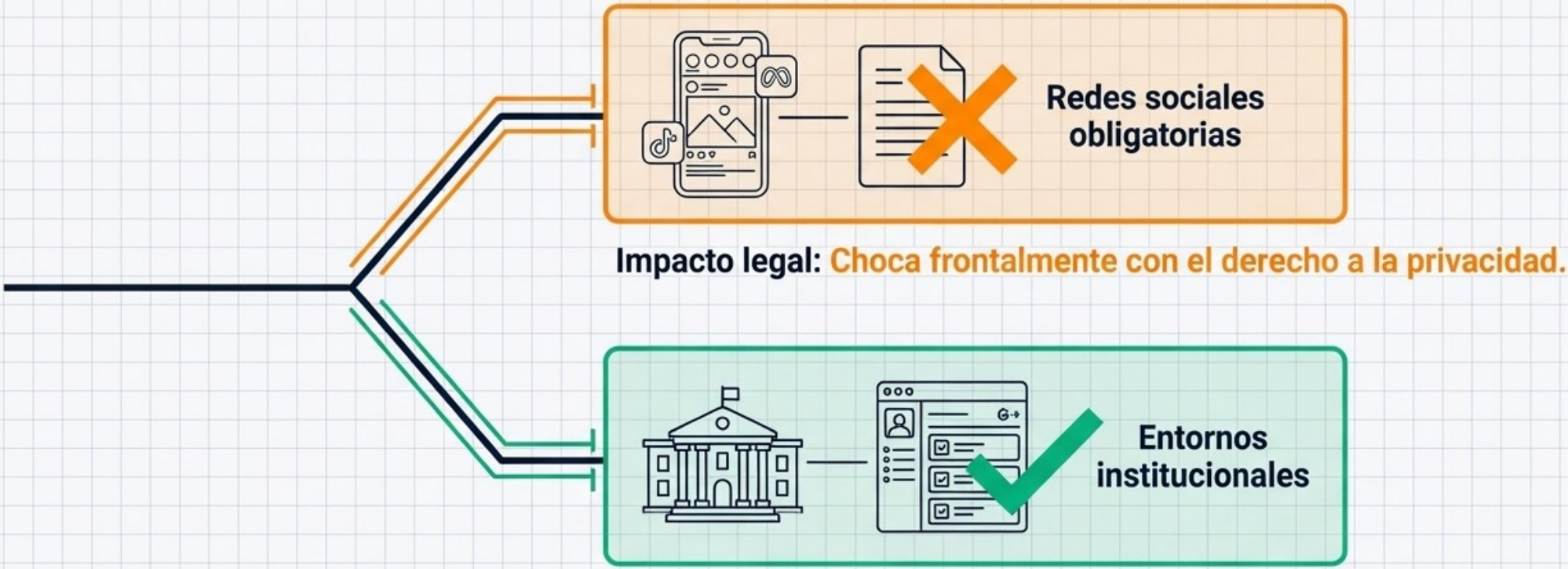
- *El impacto legal:*

  ¿Puede un profesor obligar a un alumno a ceder sus datos a Meta o ByteDance y exponer su huella digital públicamente para poder aprobar una asignatura?

  ***Pues no, esto choca frontalmente con el derecho a la privacidad**.*

La trampa de la “tecnología en la sombra” (Shadow IT)

Operar en la clandestinidad digital vulnera el derecho a la privacidad. La regla de oro es el uso exclusivo de entornos institucionales auditados o con contrato explícito de tratamiento de datos.



El conflicto de ‘pasar lista’: Privacidad frente a tradición

Evaluación de métodos de control de asistencia y sus riesgos legales.

Método	Nivel de Riesgo	Implicación Legal
Apps de terceros (ej. escanear QR)	 [Riesgo Alto]	Cede datos a empresas externas sin auditar. Responsabilidad por brecha de seguridad.
Hoja de firmas pública	 [Riesgo Alto]	Expone nombres y DNI ante compañeros sin base legal.
Geolocalización del móvil	 [Riesgo Alto]	Invasivo y desproporcionado. Vulnera el principio de minimización.
Sistemas oficiales (Moodle / UCM)	 [Seguro]	Uso de logs de conexión o exhibición visual de carnet vía webcam (Estatuto del Estudiante).

El principio de minimización y el teletrabajo

Solicitar o exponer solo la información estrictamente necesaria.

Publicación de Calificaciones

Incorrecto

~~Nombre Completo + DNI Completo (71234567Z)~~

Correcto (Regla CRUE/AEPD)

Nombre + Apellidos + Nota

(Solo en caso de homonimia:
Nombre + 4 cifras aleatorias del DNI)

Recomendación:
Usar el calificador oficial de Moodle, no PDFs adjuntos.

Privacidad en Tutorías Online

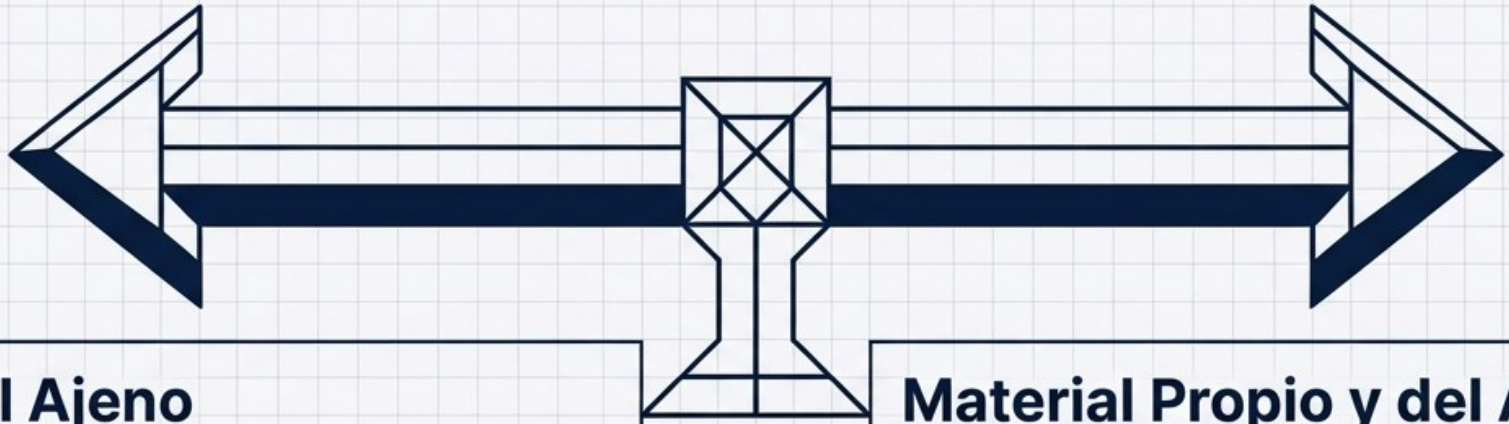
Bloqueo de pantalla automático

Uso de auriculares para evitar que familiares escuchen

Fondo desenfocado o virtual

Pilar 2: Propiedad Intelectual, una avenida de doble sentido

El entorno digital genera una falsa sensación de impunidad, pero exige una doble vigilancia legal.



Material Ajeno

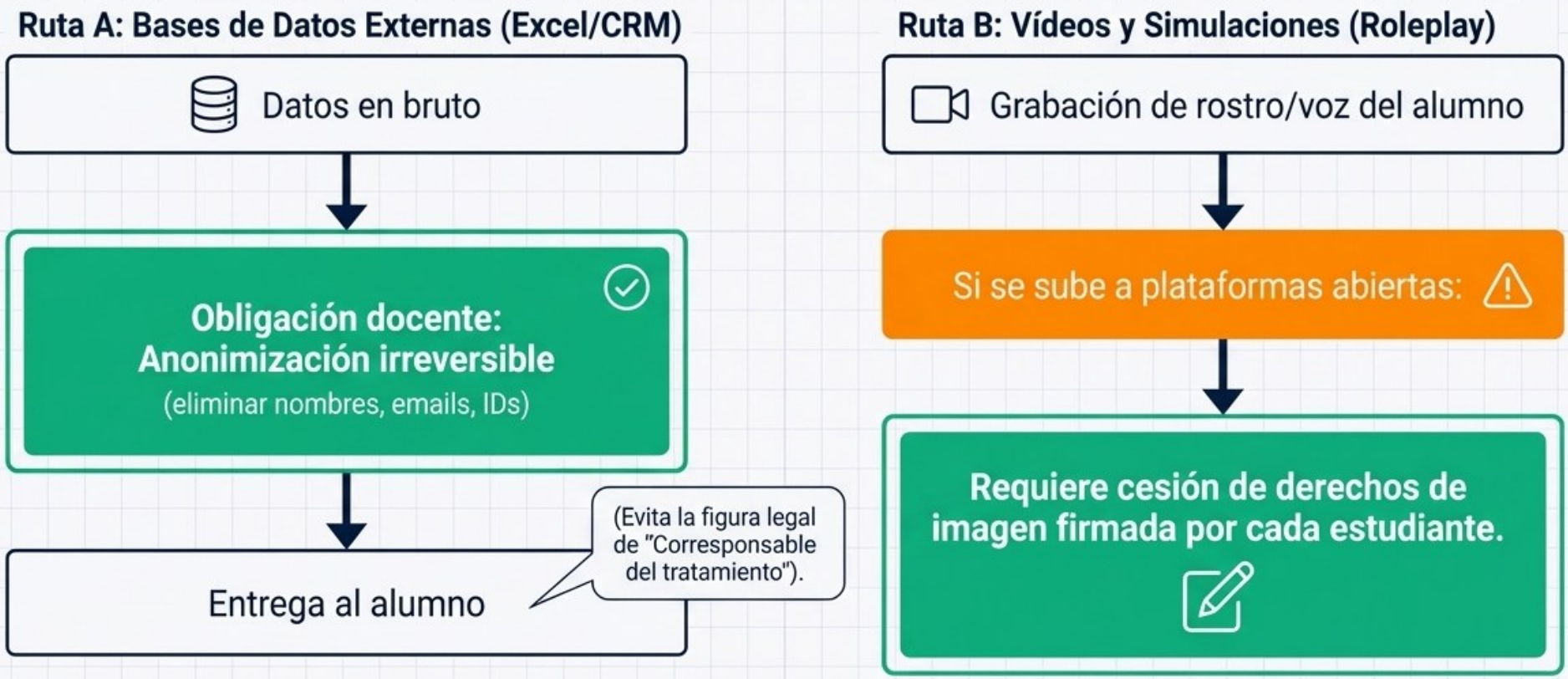
- Respeto a los derechos de autor.
- Límites legales del derecho de cita.
- Ilustración con fines educativos.
- Uso de licencias abiertas (Creative Commons).

Material Propio y del Alumno

- Protección de la creación intelectual.
- Presentaciones, casos prácticos y exámenes.
- Trabajos de alumnos son creaciones protegidas.
- Prevención frente al expolio en plataformas de intercambio.

Protocolos para datos de investigación y simulaciones

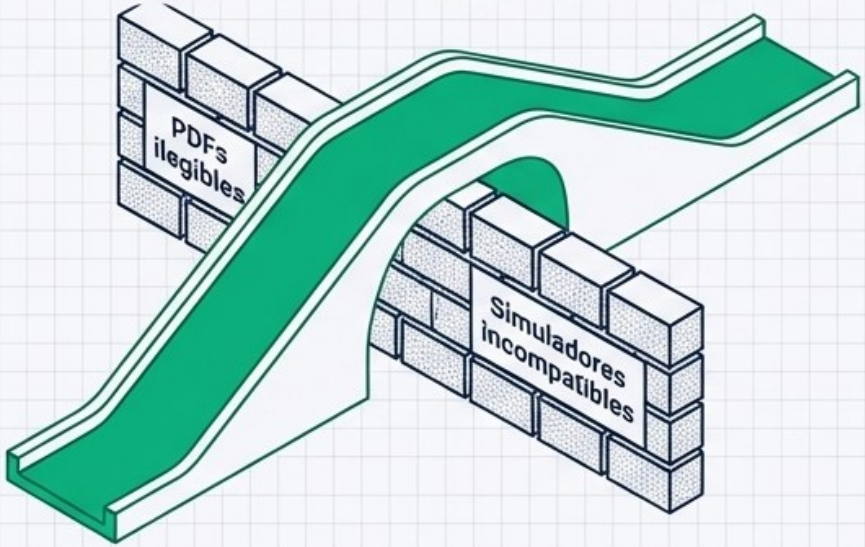
El uso de bases de datos reales y la grabación de roleplays requieren intervención activa del docente para evitar vulneraciones.



Pilar 3: La tecnología como puente, no como muro

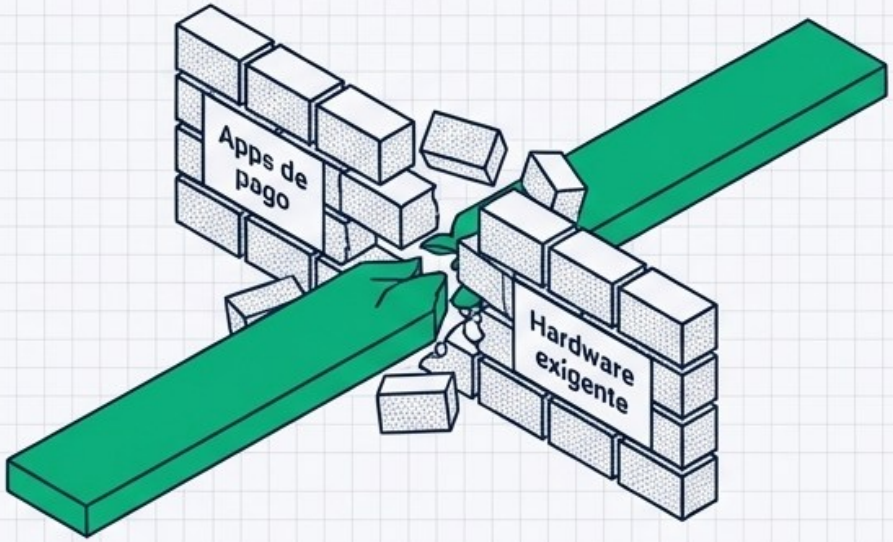
La obligación de no dejar a nadie atrás está consagrada en la ley. Las elecciones metodológicas no deben agravar las brechas existentes.

Barrera de Diversidad Funcional



- **Problema:** Herramientas incompatibles con lectores de pantalla.
- **Mandato legal:** Diseño universal y adaptación inmediata (ej. proveer alternativa oral sin penalización).

Brecha Socioeconómica



- **Problema:** Exigencia de plataformas costosas o de última generación.
- **Mandato legal:** La universidad debe garantizar alternativas accesibles y equitativas para todos.

Pilar 4: Ética de la IA y el principio de transparencia

Las herramientas generativas exigen abandonar las políticas prohibicionistas ineficaces en favor de reglas de juego claras desde el primer día.

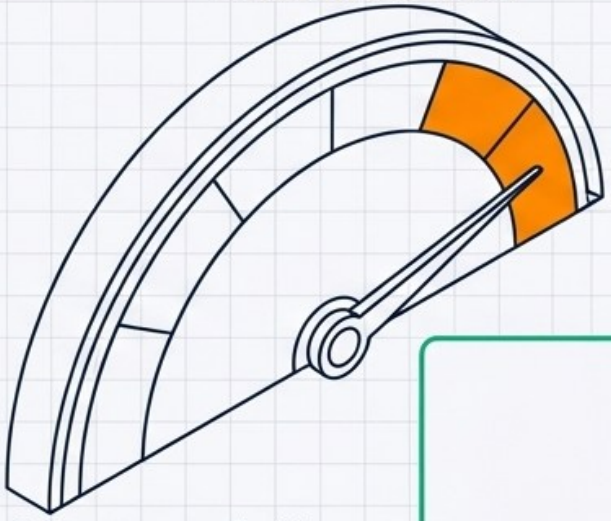
Requisito Fundamental LOSU: La Ley Orgánica del Sistema Universitario exige detallar claramente los usos permitidos en la Guía Docente de la asignatura para garantizar la equidad desde el primer día.

Supervisión humana frente al sesgo algorítmico

La delegación de la evaluación a sistemas automatizados conlleva altos riesgos de discriminación e indefensión del alumnado.

Caution Dashboard

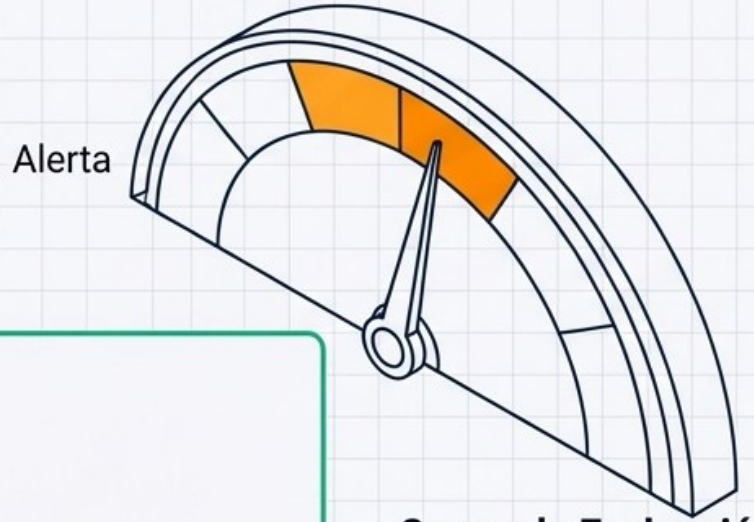
Detectores de IA



Detectores de IA

Los sistemas actuales no son infalibles. Una acusación basada solo en un software genera indefensión legal.

Sesgo de Evaluación



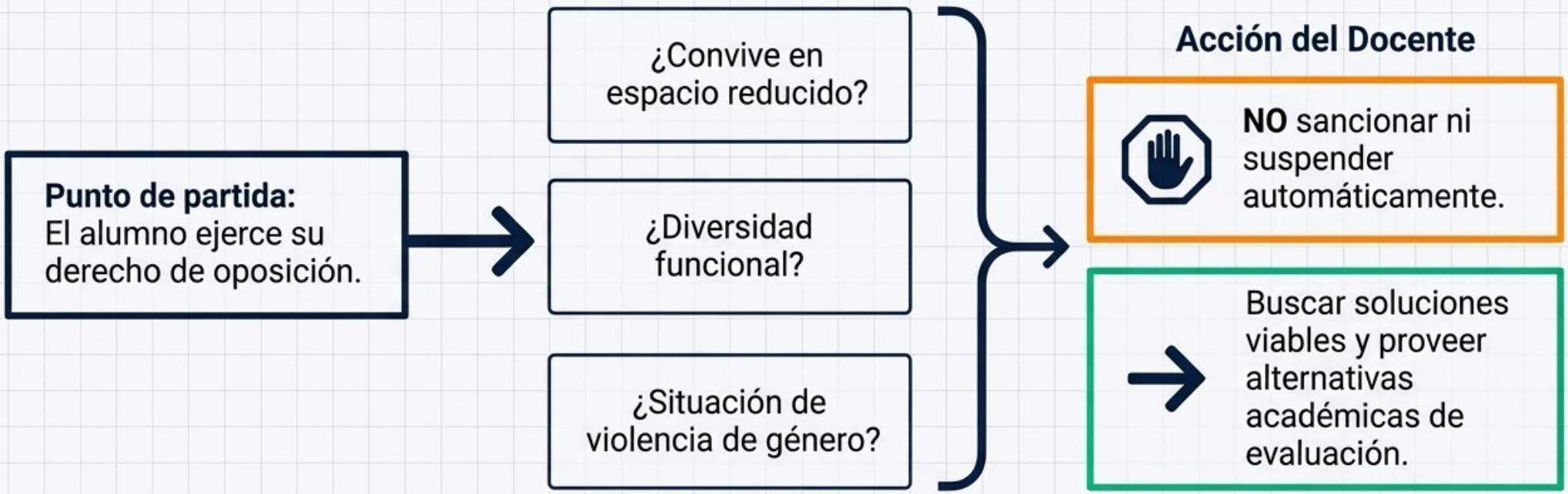
Sesgo de Evaluación

Los algoritmos pueden penalizar enfoques no convencionales o discriminar perfiles demográficos.

Presunción de inocencia: Ante la duda de uso indebido de IA, la solución legal y pedagógica es la **auditoría humana**. Citar al estudiante a una **defensa oral** del proceso de investigación.

Protocolos Especiales: El derecho de oposición a ser grabado

Cómo actuar cuando un alumno se niega a encender la cámara en clases online o exámenes.



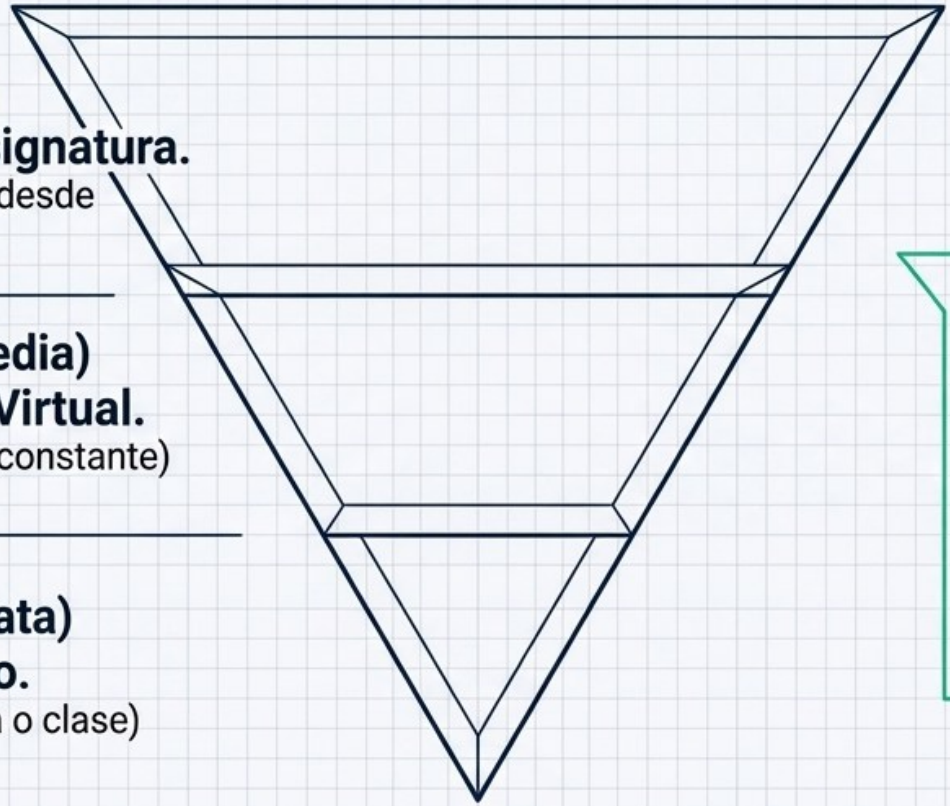
El embudo de la “Información en Capas”

El botón de grabar requiere un protocolo previo de transparencia en tres niveles distintos.

Nivel 1 (Capa Amplia)
Guía Docente de la asignatura.
(Documentación base legal desde el primer día)

Nivel 2 (Capa Intermedia)
Aviso en el Campus Virtual.
(Recordatorio institucional constante)

Nivel 3 (Capa Inmediata)
Aviso verbal o escrito.
(Justo al inicio de la prueba o clase)



Responsabilidad sobre el entorno:

Advertir al alumno que prepare su espacio doméstico para proteger la intimidad de terceros durante la grabación.

El Escudo Protector del Docente

Mantener presentes estos pilares permite innovar con absoluta tranquilidad y seguridad jurídica.

1. Datos (RGPD)

Utiliza exclusivamente herramientas institucionales. Minimiza los datos que solicitas.

2. Propiedad Intelectual

Protege tu material original (PDFs, cláusulas) y respeta las licencias en la creación ajena.

3. Accesibilidad

Verifica la compatibilidad de plataformas y ofrece siempre **alternativas** formativas inmediatas.

4. IA y Ética

Establece reglas transparentes en la guía docente y no delegues decisiones sin supervisión humana.

TERCERA PARTE

Seminario: Marco Jurídico Integral para el Docente

PLAYBOOK DE CRISIS DIGITAL DOCENTE

Protocolos tácticos y legales para el aula (Taller de Simulacro)

La Tranquilidad de la Teoría

El marco jurídico es sólido sobre el papel, pero la verdadera prueba de fuego no ocurre en el análisis normativo...

La Urgencia de la Realidad

...ocurre en la urgencia del día a día.

Reglas del Simulacro

Enfrentamos **3 escenarios realistas**. Objetivo: Diseñar protocolos viables, éticos y legales en 15 minutos. Cero respuestas vagas. Solo acción táctica.

ALERTA	RIESGO DETECTADO	PILAR VULNERADO
 Escenario 01	Software acusa al alumno de uso de IA / Plagio	Ética y Transparencia
 Escenario 02	Venta ilícita de materiales del profesor	Propiedad Intelectual
 Escenario 03	Barrera arquitectónica digital en plataforma	Accesibilidad y Equidad

REPORTE DE INCIDENTE 01

LA ALERTA

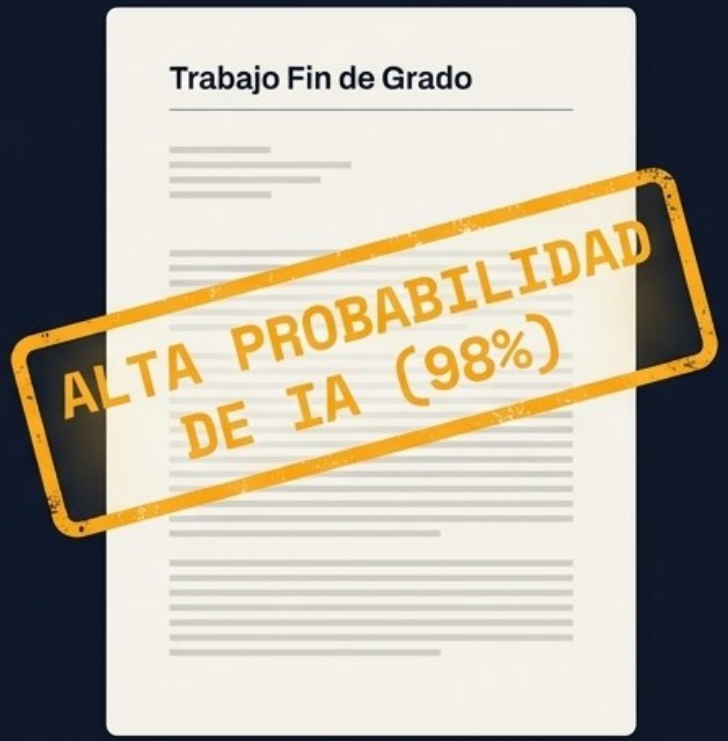
Un software de detección marca el TFG de un alumno como altamente probable de haber sido generado por IA.

LA REACCIÓN

El estudiante lo niega rotundamente.

EL RIESGO LEGAL & IMPACTO

Sancionar o acusar formalmente basándose únicamente en el porcentaje de una máquina genera **indefensión del alumno** y expone al docente a problemas legales graves, especialmente si no se prohibió explícitamente a principio de curso.



El Embudo de la Presunción de Inocencia

ALERTA DE SOFTWARE

Positivo de IA. Pausa táctica.
Los sistemas actuales no son infalibles. Generan falsos positivos (común en estructuras rígidas o estudiantes no nativos).

AUDITORÍA HUMANA

Citar al estudiante a tutoría o defensa oral obligatoria.

FILTRO DE EVALUACIÓN

Preguntas clave:
¿Defiende el marco teórico?
¿Explica el proceso?
¿Domina la bibliografía?

RESOLUCIÓN

Si el alumno demuestra el conocimiento en la defensa oral, el reporte automático del software debe ser desestimado.

PROTOCOLO 01 (PREVENCIÓN) - Mutación de la Guía Docente

El Producto Final

Evaluar únicamente el documento final entregado facilita el fraude indetectable y el uso indebido de IA.

Evaluación del Proceso

Modificar la guía docente para requerir entregas parciales, borradores iterativos y defensas orales continuas. Reglas claras desde el día 1.

Nota sobre Publicación de TFGs

A diferencia de las tesis doctorales, no hay obligación estatal de publicar TFGs. Para usar un TFG anterior como ejemplo en clase o publicarlo, se requiere consentimiento expreso del alumno.

REPORTE DE INCIDENTE 02

LA ALERTA

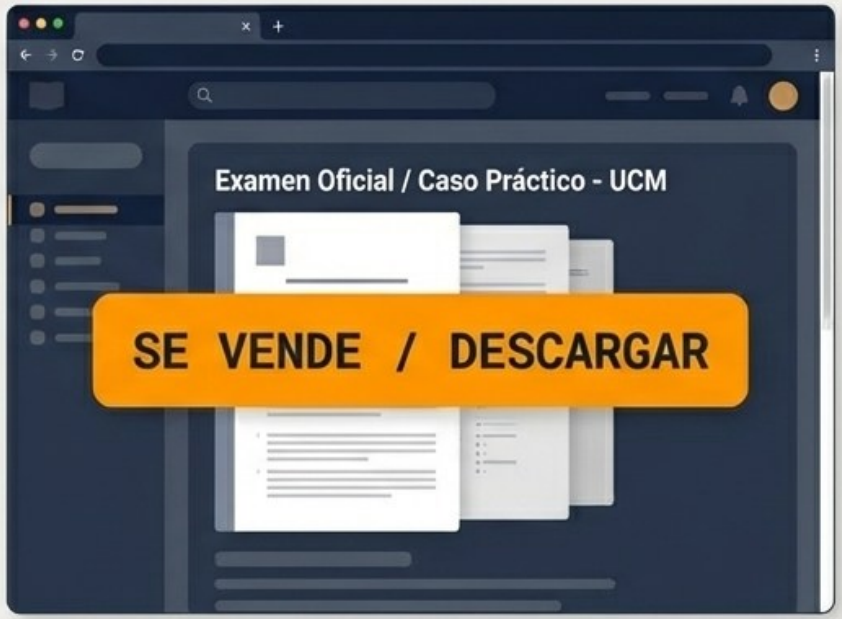
Descubre que sus casos prácticos originales y exámenes oficiales están siendo vendidos en una popular plataforma web de intercambio de apuntes.

EL CONFLICTO

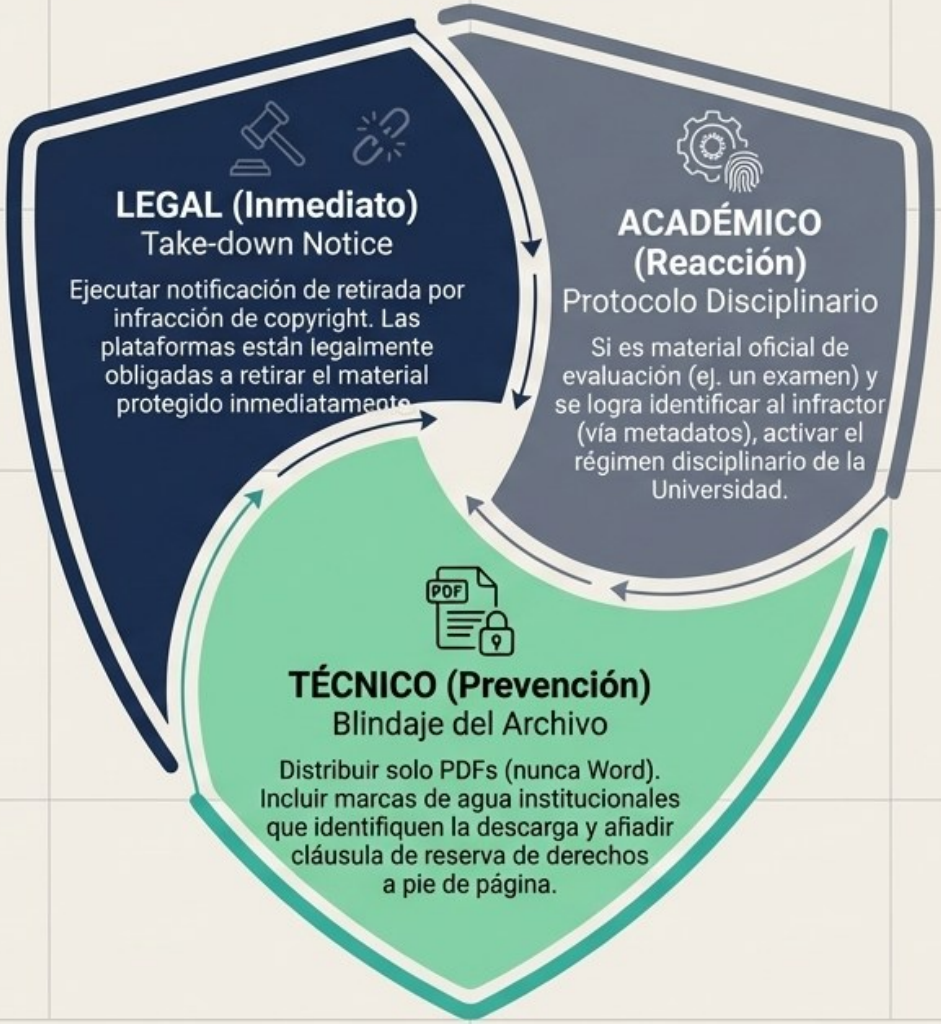
Pérdida total de control sobre los instrumentos de evaluación y frustración profunda del claustro ante el expolio de su propiedad intelectual.

EL RIESGO

Sensación de impunidad que desmotiva la innovación en la creación de nuevos materiales docentes.



PROTOCOLO 02 - La Tríada de Defensa IP



REPORTE DE INCIDENTE 03

LA ALERTA

Un estudiante con discapacidad visual informa que no puede realizar una actividad obligatoria.

LA CAUSA

El simulador externo elegido por el docente no es compatible con su software lector de pantalla.

LA REALIDAD LEGAL

El docente ha introducido, sin querer, una barrera arquitectónica digital en el aula, vulnerando el derecho a la educación inclusiva (Diseño Universal). No se puede penalizar al alumno.

PROTOCOLO 03 - La Vía Alternativa y Delegación

ACCIÓN INMEDIATA (La Rampa)

Equidad Táctica

Suspender la obligatoriedad de esa actividad para el estudiante sin merma de calificación.
Diseñar y aplicar de inmediato una alternativa académica viable (formato texto accesible o evaluación oral).

ACCIÓN A LARGO PLAZO (El Puente)

Auditoría y Delegación

El docente no tiene que ser experto informático.
Derivar la incidencia a la Unidad de Apoyo a la Diversidad.
Ellos auditarán la herramienta y, si procede, la vetarán para su uso en la Facultad.

REPORTE ESPECIAL: Datos Reales en Trabajos de Campo

LA PRÁCTICA COMÚN

En Comercio y Turismo es habitual pedir a los alumnos encuestas a turistas, recolección de emails para campañas ficticias, o análisis de bases de datos de clientes reales.

EL RIESGO RGPD

Inducir a los alumnos a recopilar datos de terceros sin base legitimadora, convirtiendo al docente en corresponsable de una infracción.

LA SOLUCIÓN TÁCTICA

Proporcionar siempre un documento de consentimiento informado oficial para las encuestas. Exigir a las empresas colaboradoras que las bases de datos entregadas estén anonimizadas irreversiblemente antes de que los alumnos las procesen.

RESPUESTAS RÁPIDAS:
Shadow IT y Grabaciones

El Grupo de WhatsApp	¿Puedo crear un grupo de WhatsApp para el viaje de prácticas de Turismo?	**NO.** Expone datos personales (teléfonos) sin necesidad. La CRUE obliga a usar vías institucionales (Shadow IT vulnera la privacidad).
Uso de Kahoot/Mentimeter	¿Debo dejar de usar herramientas interactivas gratuitas en clase?	**NO, PERO ANONIMIZA.** Riesgo minimizado si los alumnos usan apodos ficticios y no ceden sus correos reales.
Grabación de Roleplays	¿Puedo grabar a alumnos simulando una recepción de hotel?	**SÍ, PARA EVALUAR.** La voz y la imagen son datos biométricos. Solo se permite sin firma si es puramente para evaluación, se guarda en repositorio oficial y se borra al acabar el curso. No subir a nubes personales.

SÍNTESIS: El Cuadrante del Blindaje Docente (1/2)

Protección de Datos (RGPD)

- Priorizar siempre herramientas y campus virtual institucionales.
- Minimizar datos (no pedir correos o teléfonos personales si no es vital).
- Cero apps externas sin contrato de encargo de tratamiento.

Propiedad Intelectual

- Usar bancos de imágenes libres (**Creative Commons**) e invocar ilustración con fines educativos.
- Proteger material propio (marcas de agua, formato PDF, reservas de derechos).
- Ejecutar **Take-down notices** implacables ante ventas ilícitas.

SÍNTESIS: El Cuadrante del Blindaje Docente (2/2)

Accesibilidad y Equidad

- Verificar compatibilidad con lectores de pantalla (diseño universal preventivo).
- Mitigar la brecha digital (evitar exigir hardware/software de pago muy costoso).
- Tener planes 'B' inmediatos (evaluaciones alternativas y ágiles).

Ética e Inteligencia Artificial

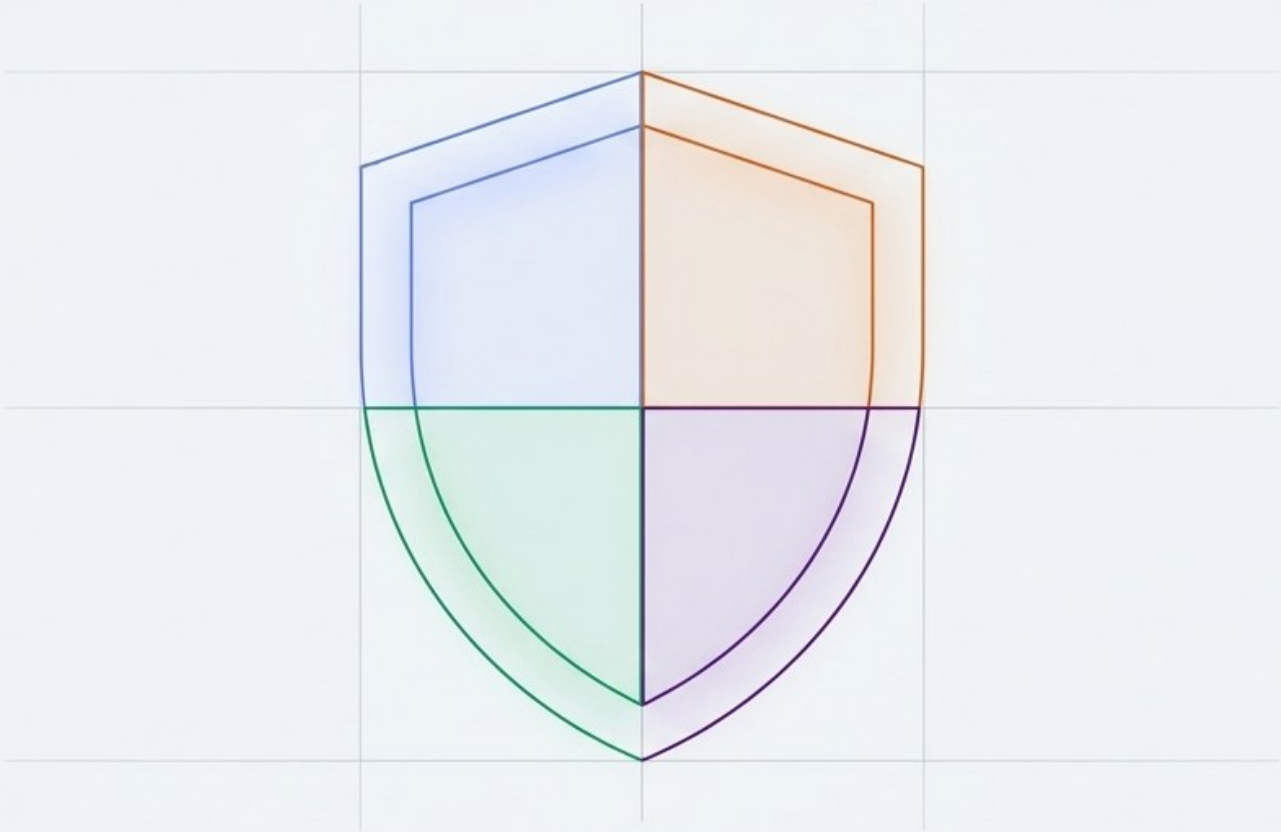
- Reglas claras y transparentes sobre IA desde la guía docente (día 1).
- Ante un detector de IA positivo, priorizar siempre la defensa oral.
- Supervisión humana crítica obligatoria sobre los algoritmos de evaluación.

“La tecnología avanzará y la IA evolucionará. Pero si mantenemos presentes nuestros cuatro pilares —protección de datos, autoría, accesibilidad y transparencia— podremos seguir innovando con la absoluta tranqiilidad de estar haciendo lo correcto.”

Fin del Simulacro. Facultad de Comercio y Turismo.

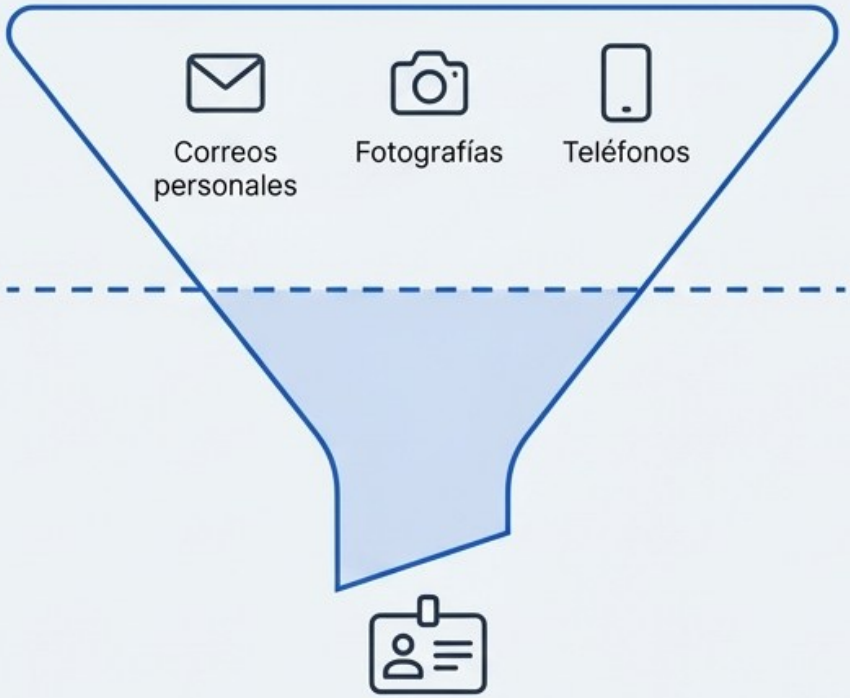
Checklist de Seguridad Digital Docente

La herramienta necesaria para el ecosistema universitario



La seguridad digital no es una traba burocrática; es una arquitectura de cuatro columnas diseñada para proteger al docente y garantizar los derechos del alumnado.

Filtro de Minimización



Solicitar solo lo estrictamente necesario para la docencia

Regla de Oro: Priorizar siempre el campus virtual y las aplicaciones institucionales.

Hacia Afuera - Blindaje Propio

1. Incluir autoría institucional
2. Usar marcas de agua
3. Añadir cláusula de reserva en PDFs

Protocol

Activar mecanismos de take-down notice (retirada) ante la venta de apuntes y exámenes oficiales.

Hacia Adentro - Respeto a Terceros

1. Utilizar bancos libres (Creative Commons)
2. Limitarse a la ilustración con fines educativos

Espectro de Inclusión

Compatibilidad Visual (Software)

Asegurar que documentos y plataformas sean legibles para softwares de lectura de pantalla.

Mitigación de Brecha (Hardware)

Evitar herramientas de pago o exigencias de hardware de alto rendimiento para no excluir por motivos socioeconómicos.

Plan B Inmediato (Contingencia)

Preparar formato alternativo inmediato (evaluación oral o texto plano) si la tecnología crea barreras inesperadas.

Archivo de Diagnóstico - Basado en directrices AEPD y CRUE

Guía Práctica de Resolución: 7 Dilemas Legales en el Aula Digital

Casos de uso cotidiano, riesgos ocultos y protocolos de actuación segura para el docente universitario.

El Mapa de Riesgos

Práctica Habitual	Nivel de Riesgo	Foco Legal	Veredicto Seguro
Grupos WhatsApp para viajes	Alto	RGPD / Directriz CRUE	Usar canales oficiales institucionales
Cuestionarios en vivo (Kahoot)	Medio	Art. 28 RGPD	Seguro si es 100% anónimo
Trabajos hechos con ChatGPT	Alto	Presunción de inocencia	Defensa oral + Guía Docente
Alumnos grabando clases	Infracción	Propiedad Intelectual	Exigir borrado inmediato
Grabar simulaciones (Roleplay)	Medio	Datos biométricos	Campus Virtual + Borrado final
Accesibilidad de PDFs/Web	Medio	Diseño Universal	Accesible por defecto (Preventivo)
Sanciones AEPD	Alto	Responsabilidad Patrimonial	Evitar negligencia grave o dolo

0. El 'Shadow IT' de la comunicación

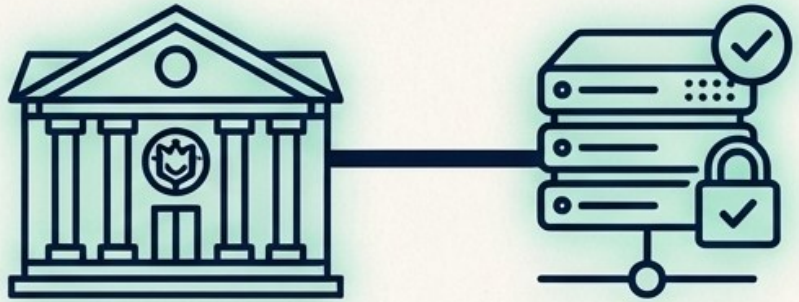
- **Pregunta**: 'Para organizar un viaje de prácticas de Turismo es utilísimo crear un grupo de WhatsApp con los alumnos. ¿Hay algún problema con esto?'
- **Respuesta**: 'Sí, el impacto legal es importante. Al meter a los alumnos en un grupo de WhatsApp, se vulnera su derecho a la privacidad. La alternativa legal es utilizar los sistemas oficiales de la Universidad.
- La CRUE dictamina la recomendación de utilizar exclusivamente las herramientas oficiales provistas por la universidad. Si se usa un proveedor externo, es obligatorio firmar un contrato de encargado de tratamiento que cumpla con el art. 28 del RGPD.
- La CRUE estipula que los empleados deben usar las vías y medios de comunicación institucionales. Crear grupos de WhatsApp expone datos personales (teléfonos) innecesariamente y requeriría cumplir exigencias estrictas del RGPD.

La Tentación: El "Shadow IT"

Crear un grupo de WhatsApp es utilísimo y rápido para coordinar a los alumnos en un viaje...

⚠ Al incluir a los alumnos, se exponos, se exponen datos personales (teléfonos) innecesariamente entre terceros sin base legal.

La Realidad Legal: El Mandato Institucional



La CRUE estipula que los empleados deben usar exclusivamente las vías y medios de comunicación institucionales.

Proveedores externos requieren un contrato de encargado de tratamiento (Art. 28 del RGPD).

El Dilema de las Herramientas Cotidianas (Kahoot, Mentimeter)

La regla de oro: El problema legal no es la herramienta en sí, **sino cómo obliga a sus alumnos** a ceder sus datos.

1. **La trampa de la IA no regulada**

- **Pregunta:** Si descubro que un alumno ha usado ChatGPT para redactar íntegramente su trabajo, pero en mi guía docente de principio de curso no prohibí explícitamente el uso de Inteligencia Artificial, ¿puedo suspenderle por plagio?"
- **Respuesta:** Este es un vacío legal muy común hoy en día. Si no ha establecido previamente una política de uso transparente con los estudiantes en su guía docente, sancionar a posteriori es jurídicamente muy débil y el alumno podría recurrir el suspenso con éxito, porque la presunción de inocencia y las reglas claras son fundamentales. Por ello, la solución no es suspenderle retroactivamente por una norma que no existía, sino citarle a una defensa oral para evaluar su conocimiento real del tema, y actualizar urgentemente su guía docente para el próximo curso.

La Trampa de la IA no Regulada

El Escenario

Un alumno redacta íntegramente su trabajo con ChatGPT. La Guía Docente no prohibía explícitamente el uso de Inteligencia Artificial al inicio del curso.

Suspenso Retroactivo

Suspender por plagio basándose en software detector.

Juridicamente muy débil. Los detectores tienen falsos positivos. El alumno podría recurrir con éxito por indefensión.

El Protocolo Seguro

Paso 1: Presunción de Inocencia. No sancionar sin pruebas irrefutables.

Paso 2: Defensa Oral. Citar al estudiante para evaluar su conocimiento real del marco teórico y bibliografia.

Paso 3: Actualización. Modificar urgentemente la Guía Docente para el próximo curso estableciendo una politica de IA transparente.

2. El dilema de las herramientas cotidianas (Kahoot, Mentimeter, etc.)

- Pregunta: Yo uso Kahoot y otras aplicaciones gratuitas para hacer cuestionarios anónimos en clase y dinamizar. ¿Me está diciendo que estoy violando el RGPD y que debo dejar de usarlas porque la universidad no tiene contrato con ellas?
- Respuesta: No necesariamente tiene que dejar de usarlas, pero debe cambiar cómo las usa. Como el RGPD protege la privacidad de los datos personales, si los alumnos participan de forma verdaderamente anónima (usando apodos ficticios y sin tener que registrarse con su correo personal ni ceder su IP a una cuenta permanente), el riesgo legal se minimiza drásticamente. El problema legal surge cuando les exige crear un perfil con sus datos reales en una plataforma no auditada por la institución.
- La CRUE dictamina que las herramientas de docencia virtual realizan tratamiento de datos y deben utilizarse exclusivamente las herramientas oficiales provistas por la universidad. Si se usa un proveedor externo, es obligatorio firmar un contrato de encargado de tratamiento que cumpla con el art. 28 del RGPD.

3. Grabaciones no autorizadas en el aula

- Pregunta: ¿Qué ocurre si un estudiante graba mis clases magistrales con su móvil sin mi permiso y luego las comparte por WhatsApp o redes sociales? ¿No vulnera eso mi propiedad intelectual?"
- Respuesta: Absolutamente. Esto atenta directamente contra su propiedad intelectual y sus derechos de autor, además de su derecho a la propia imagen. Como las clases magistrales son creaciones intelectuales del docente, como profesor, tiene toda la potestad legal para prohibir las grabaciones no autorizadas en su aula. Es más, si descubre que se están distribuyendo, puede exigir su eliminación inmediata y aplicar la normativa disciplinaria de la universidad por vulneración de derechos de autor.
- La AEPD y la CRUE establecen que la difusión de clases grabadas en redes sociales atenta contra el derecho a la protección de datos, la propia imagen y la propiedad intelectual, pudiendo generar responsabilidad disciplinaria, administrativa e incluso civil. Si un alumno graba, debe contar con el consentimiento expreso de todos los asistentes (profesor y compañeros).

Enlace: https://www.ucm.es/campusvirtual/protocolo-de-derechos-de-autor

Grabaciones No Autorizadas en el Aula Magistral

Derecho a la Propia Imagen y Protección de Datos Personales (AEPD).

La captación de la imagen del docente sin consentimiento para fines no académicos constituye una violación de derechos fundamentales.

Propiedad Intelectual. Las clases magistrales son creaciones intelectuales del docente.

El contenido académico y su presentación están protegidos por derechos de autor, prohibiendo su reproducción no autorizada.

Difusión Ilegal. Compartir en redes agrava la responsabilidad civil y administrativa.

La distribución a terceros a través de plataformas dlgitales puede generar sanciones disciplinarias y demandas.

Su Autoridad Legal: Como profesor, tiene toda la potestad legal para prohibir grabaciones, exigir su eliminación inmediata y aplicar la normativa disciplinaria de la universidad.

4. Grabación de simulaciones y roleplay

- **Pregunta**: En nuestras disciplinas, como las habilidades blandas son vitales, es frecuente que grabe a los alumnos simulando la atención al cliente en el mostrador de un hotel o en una negociación comercial para luego analizar el vídeo en clase. ¿Puedo guardar esos vídeos?
- **Respuesta**: Hay que tener mucho cuidado con esto, porque la imagen y la voz son datos biométricos y personales, por lo que almacenar esos vídeos en el ordenador personal del docente o en plataformas en la nube no institucionales (como un Google Drive o Dropbox personal) sin un consentimiento explícito, informado y por escrito del alumno: es un riesgo altísimo. Debe recabar su consentimiento previo y almacenar esas grabaciones exclusivamente en los repositorios seguros que provea la universidad, destruyéndolos una vez finalizado el curso académico.
- De hecho, la AEPD y la CRUE establecen que la difusión de clases grabadas en redes sociales atenta contra el derecho a la protección de datos, la propia imagen y la propiedad intelectual, pudiendo generar responsabilidad disciplinaria, administrativa e incluso civil. Si un alumno graba, debe contar con el consentimiento expreso de todos los asistentes (profesor y compañeros).
- La AEPD señala, sin embargo, que grabar sesiones de docencia o exámenes (como un roleplay evaluable) no requiere el consentimiento del alumno si la finalidad es puramente educativa, la verificación de conocimientos o servir de prueba de evaluación, ya que se ampara en el cumplimiento de una misión de interés público (art. 6.1.e RGPD) y en la Ley Orgánica de Universidades.

El consentimiento expreso y por escrito del alumno solo es estrictamente necesario si el profesor pretende difundir ese vídeo públicamente, reutilizarlo en cursos futuros o almacenarlo en plataformas no institucionales. Por lo que si la grabación se guarda en el campus virtual oficial y se borra al acabar el curso (o el periodo de reclamaciones), es una práctica lícita sin necesidad de recabar firmas.

Grabación de Simulaciones y Roleplays (Datos Biométricos)

¿Necesita grabar a los alumnos simulando una negociación o atención al cliente?

¿Va a guardar el vídeo en su ordenador, Dropbox personal, o reutilizarlo en cursos futuros?

⚠ **Riesgo Altísimo.** Requiere consentimiento previo, explícito, informado y por escrito de todos los asistentes.

¿La grabación es puramente educativa, se almacena solo en el Campus Virtual oficial y se destruye al finalizar el curso?

Práctica Lícita. Amparado en la misión de interés público (Art. 6.1.e RGPD). NO requiere recabar firmas.

5. **Accesibilidad preventiva vs. reactiva**

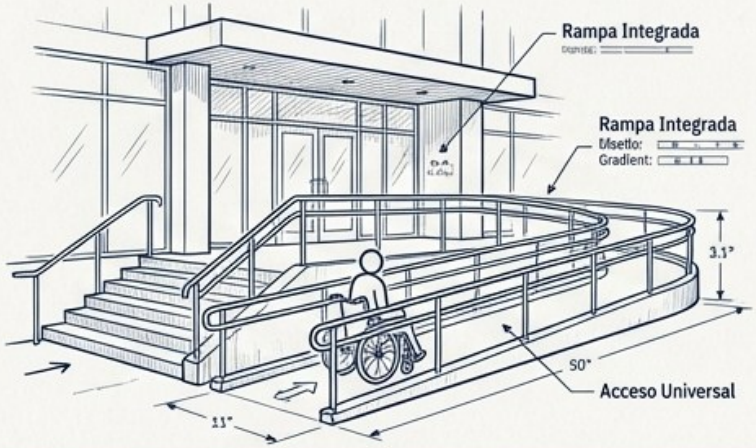
- Pregunta: Adaptar todos mis materiales visuales y plataformas para que sean compatibles con lectores de pantalla me lleva horas. Si este cuatrimestre no tengo matriculado a ningún alumno con discapacidad visual, ¿es legalmente obligatorio que lo haga?"
- Respuesta: La responsabilidad legal y ética implica asegurar que la tecnología no cree barreras. Aunque el conflicto estalle cuando el estudiante reporta el problema, el marco normativo actual de accesibilidad web exige un diseño universal, lo que significa que los materiales deben nacer accesibles: a corto plazo, podría no tener una queja formal, pero a largo plazo, su responsabilidad legal exige que el ecosistema digital de su asignatura sea inclusivo por defecto.

Accesibilidad Preventiva vs. Reactiva

El Error Reactivo

"Adaptaré mis PDFs y plataformas web solo si se matricula un estudiante con discapacidad visual."

⚠ **Legal Reality:** Esperar a la queja para eliminar la barrera arquitectónica digital vulnera la equidad.



El Deber Legal

Concepto: Diseño Universal.

✓ **Legal Reality:** El marco normativo exige que el ecosistema digital (documentos, plataformas) sea inclusivo por defecto. Los materiales deben nacer accesibles para lectores de pantalla.

6. El escudo institucional en caso de multa

- Pregunta: Volviendo al caso del principio, el de 'la app de calificaciones'. Si la Agencia de Protección de Datos impone una multa por la filtración, ¿la paga la universidad o me embargan la nómina a mí?"
- Respuesta: El objetivo de este seminario es dar un marco de actuación seguro precisamente para evitar llegar a este punto. Por regla general, la universidad, como responsable del tratamiento de datos, es quien asume la responsabilidad patrimonial e institucional frente a la Agencia. Sin embargo, si la universidad demuestra que actuó con 'negligencia grave' o 'dolo' (por ejemplo, si usó una app prohibida expresamente por el departamento de informática tras ser advertido), la institución podría iniciar una acción de repetición contra usted para reclamarle el importe de la sanción.

El Escudo Institucional (¿Quién paga la multa?)

El Paraguas:
Por regla general, la universidad asume la responsabilidad patrimonial frente a las multas de la AEPD.

La Perforación:
Si el docente ignora advertencias informáticas o usa apps prohibidas (Shadow IT), la universidad reclamará el importe íntegro de la sanción al patrimonio personal del profesor.

Las 4 Reglas de Oro del Aula Digital

1

El anonimato salva la innovación.

Las apps externas son seguras solo si los alumnos participan mediante apodos sin registro de datos reales.

2

La defensa oral supera al algoritmo.

Ante sospechas de IA generativa, la presunción de inocencia manda; evalúe el conocimiento real en persona, no con detectores.

3

El Campus Virtual es su refugio.

Almacenar grabaciones, calificaciones y datos en el entorno institucional le otorga inmunidad legal automática.

4

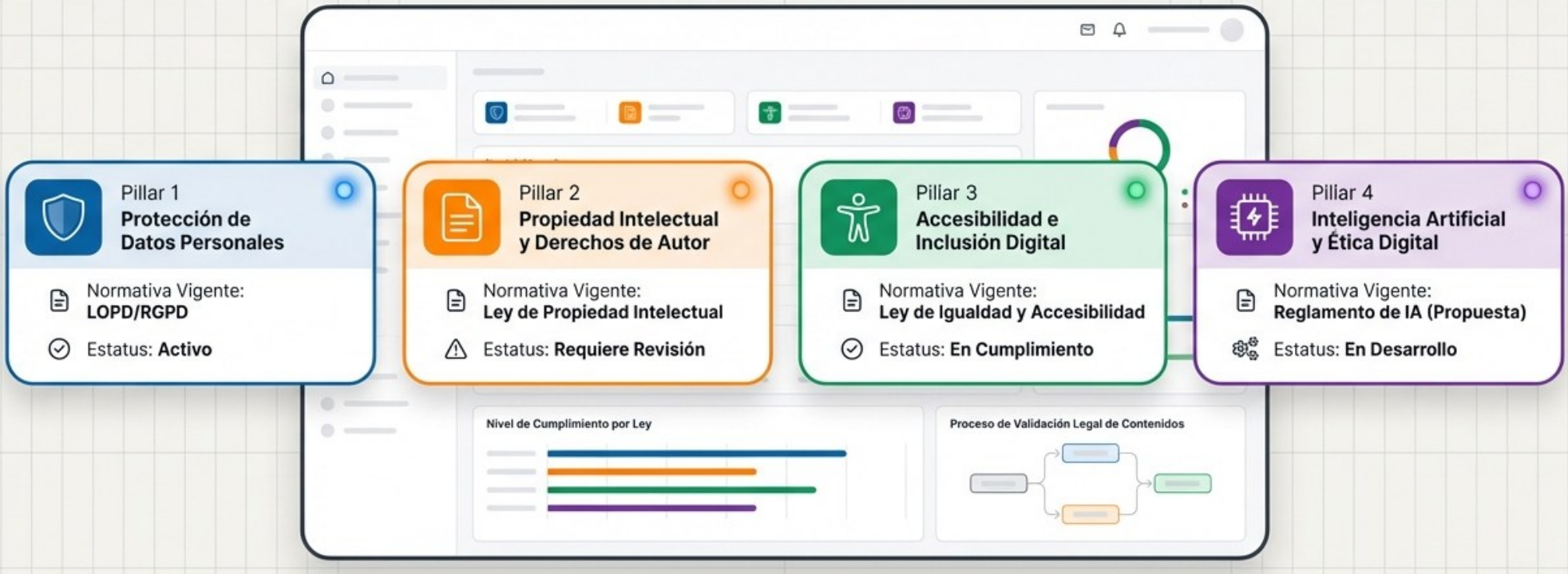
La accesibilidad se diseña, no se improvisa.

El diseño universal no es un favor reactivo, es una obligación legal preventiva.

DEL RIESGO NORMATIVO AL CUMPLIMIENTO PRÁCTICO EN LA EDUCACIÓN SUPERIOR.

El Dashboard Legal del Docente

Las 4 leyes que regulan nuestra docencia digital

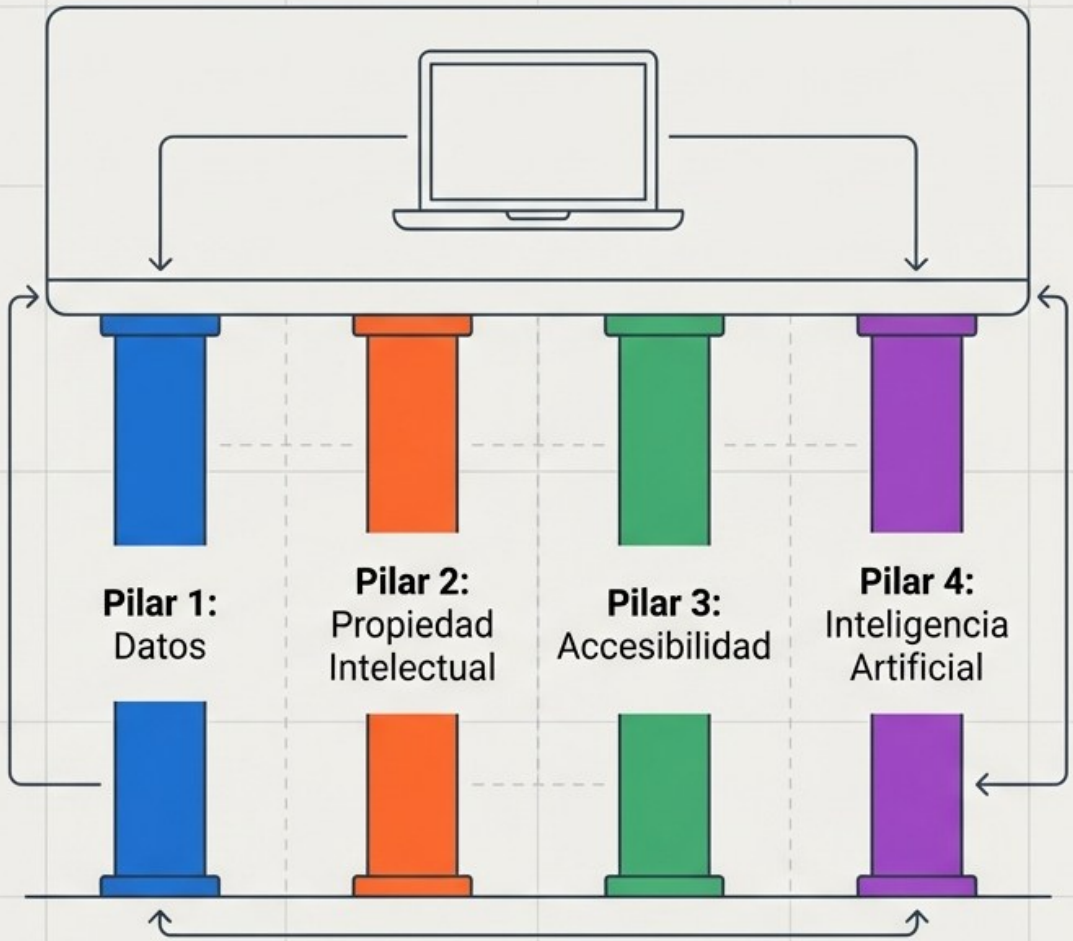


Un escudo profesional, no una simple recomendación

La privacidad, la autoría y la equidad exigen ajustes rigurosos en nuestro país.

Estos cuatro pilares legales conforman el terreno de juego obligatorio para proteger tanto al alumnado como a la Universidad.

Conocer su alcance es la mejor defensa del docente.



La tecnología avanza, pero los pilares permanecen.

El aula digital es segura cuando el diseño es intencional.

Tu próximo paso:

Revisa y actualiza tus guías docentes de este cuatrimestre utilizando esta matriz de seguridad.

UNIVERSIDAD COMPLUTENSE MADRID

Muchas gracias