



PRODAAPP

Estrategias para el cumplimiento de la normativa de
protección de datos personales en el Sector público

Documento de trabajo sobre privacidad y seguridad digital en las universidades públicas



1526 V Centenario 2026 Escuela de SALAMANCA

Premisa de partida...

La protección de datos y la seguridad digital deben incorporarse a la toma de decisiones de gobierno de las universidades públicas. El proyecto de I+D+i “Estrategias para el cumplimiento de la normativa de protección de datos personales en el Sector público” (PRODAAPP) desarrollado sitúa la prevención, la delimitación de responsabilidades, la dotación de recursos especializados y la cooperación entre instituciones como condiciones para una transformación digital compatible con los derechos y libertades fundamentales de la ciudadanía. A tal fin, el presente documento además de ordenar las principales ideas-fuerza de los debates impulsados en los últimos meses en el Estudio salmantino, pretende facilitar el debate académico y servir de base para formular criterios comunes de actuación en docencia, investigación y gestión universitaria.

[A] Del cumplimiento formal a la gobernanza responsable: desafíos de privacidad y seguridad en la universidad digital

La universidad necesita integrar la privacidad y la seguridad en la planificación de sus actividades desde el diseño y por defecto. En este contexto, el conocimiento de los tratamientos, la evaluación previa de riesgos y la coordinación institucional deben convertirse en el centro gravitacional de un modelo de gobernanza responsable, sustentado sobre los siguientes presupuestos:

1. La protección de las personas debe orientar necesariamente la transformación digital

La utilidad de una herramienta para la docencia, la investigación o la gestión debe examinarse junto con sus efectos sobre la confidencialidad, los accesos y el uso posterior de la información. La adopción tecnológica requiere una decisión institucional informada.

2. La prevención debe comenzar antes de implantar los sistemas

Es necesario acometer la revisión de proyectos, contratos públicos y procedimientos de adquisición de soluciones tecnológicas desde su fase de diseño. Las evaluaciones de impacto se presentan como instrumentos relevantes cuando el tratamiento puede entrañar un alto riesgo para los derechos y libertades fundamentales, evitando que las garantías se incorporen cuando el sistema ya está funcionando.

3. El uso de inteligencia artificial exige examinar el tratamiento de datos

La preocupación principal se refiere a la introducción de información universitaria en plataformas externas y a su eventual utilización para entrenar modelos. Por ello, es necesario insistir en la necesidad de analizar estos riesgos antes de autorizar la implementación de estas herramientas.

4. Los compromisos contractuales necesitan capacidad real de comprobación

En la actualidad, las universidades públicas experimentan importantes dificultades para verificar las prácticas desarrolladas por grandes proveedores y para negociar sus condiciones estándar. Una cláusula de confidencialidad o de exclusión del entrenamiento no resuelve por sí sola las dudas sobre el uso efectivo de los datos de la comunidad universitaria.

5. El cumplimiento requiere responsabilidades y recursos

La asesoría especializada debe conectarse con quienes deciden sobre las finalidades, los sistemas y la contratación. Los órganos universitarios de toma de decisiones necesitan disponer de información suficiente para asumir las decisiones y financiar las garantías necesarias.

Líneas futuras de trabajo

Elaborar un procedimiento común dentro del Sistema Universitario Español de evaluación previa de tecnologías y proyectos que reúna las consideraciones de privacidad, seguridad y contratación públicas.

[B] Gobernar los datos en la Universidad pública: organización, responsabilidad y criterios comunes

La dispersión de actividades y tratamientos de datos personales exige una organización estable que permita conocer los datos gestionados, delimitar los accesos y coordinar a los servicios. En este sentido, es indispensable tener en cuenta las siguientes cuestiones:

1. Conocer adecuadamente los tratamientos de datos personales es una condición para gobernarlos

La información universitaria comprende expedientes académicos, personal, proyectos de investigación, clínicas, encuestas y registros históricos. En este sentido, es necesario advertir que el volumen real de datos que obran en poder de las universidades públicas y centros de conocimiento puede ser desconocido y que su alto grado de dispersión dificulta extraordinariamente las labores de supervisión y garantía de cumplimiento normativo.

2. El delegado de protección de datos necesita apoyo especializado y reconocimiento institucional adecuado

La figura del delegado de protección de datos es una pieza esencial para lograr una adecuada transformación digital de la Universidad pública. Sin embargo, generalmente el DPD se enfrenta a una importante sobrecarga de trabajo y dispone de recursos insuficientes. Ante esta tesitura, es necesario avanzar hacia la instauración de unidades administrativas que dispongan de apoyo jurídico y técnico, así como revisar el tiempo y el reconocimiento institucional que realizan las universidades para los profesionales que desarrollan estas funciones, generalmente reservadas al personal docente e investigador.

3. La responsabilidad de decidir acerca de los tratamientos de datos debe permanecer en los órganos competentes

Conviene distinguir entre las funciones de asesoramiento y supervisión desempeñadas por el DPD y la responsabilidad institucional universitaria sobre las decisiones estratégicas que atañen a los tratamientos de datos personales. Por esta razón, la coordinación entre responsables académicos, servicios jurídicos, servicios de contratación, equipos tecnológicos y DPD resulta indispensable para evitar actuaciones fragmentadas.

4. El principio de minimización debe aplicarse a situaciones cotidianas

En la actuación cotidiana de la universidad pública es habitual encontrar muestras de laboratorio con identificadores innecesarios, acceso del profesorado a teléfonos o domicilios y entrega de documentación clínica extensa para justificar ausencias del estudiantado o instaurar medidas de adecuación de la actividad docente a aquellas personas que tienen alguna necesidad especial. Por ello, la información solicitada por los servicios universitarios debe racionalizarse y ajustarse en virtud de la naturaleza y la finalidad de la tarea a realizar.

5. Las prácticas externas y la investigación requieren circuitos claros

Existen riesgos vinculados con la extracción de datos de pacientes y menores durante la realización de prácticas curriculares o el tratamiento de datos masivo para el desarrollo de TFG y TFM. Por ello, es necesario establecer protocolos precisos y garantizar la participación del DPD en el Comité de Ética de la Investigación para garantizar el cumplimiento normativo desde el diseño y por defecto.

6. La cooperación universitaria puede reducir diferencias de capacidad

Es necesario proceder al diseño de guías compartidas, protocolos comunes y apoyo entre instituciones para la realización de evaluaciones y auditorías. Estos instrumentos permitirían aprovechar experiencia especializada sin diluir la responsabilidad de cada universidad.

Líneas futuras de trabajo

Priorizar el inventario de actividades de tratamientos, el refuerzo de la unidad de privacidad y los protocolos de protección para prácticas, investigación y adaptaciones académicas.

[C] Una Universidad cibersegura: prevención, resiliencia y respuesta coordinada frente a incidentes

La seguridad universitaria requiere estructuras de dirección, controles técnicos y participación de la comunidad universitaria. La apertura de los entornos académicos, la descentralización de los centros y la renovación constante de usuarios dificultan la gestión de los accesos y la correcta protección de la información. Con la finalidad de fortalecer la ciberseguridad de la universidad público es necesario tener en cuenta las siguientes premisas:

1. La seguridad digital debe sostener el funcionamiento del servicio universitario.

La prevención está estrechamente relacionada con la detección, la respuesta y la recuperación. La planificación institucional debe atender tanto a la protección de la información como a la capacidad para mantener y recuperar los servicios afectados.

2. La política de seguridad necesita una estructura operativa precisa

La adaptación al Esquema Nacional de Seguridad exige articular políticas, comités y oficinas especializadas que permitan dar cumplimiento a las exigencias contempladas en la Guía CCN-STIC 881. En este sentido, es necesario distinguir entre funciones relativas a la información y los servicios, la supervisión de la seguridad y la ejecución técnica de los sistemas.

3. Los accesos deben asignarse y revisarse según las necesidades reales de la comunidad universitaria

Es necesario limitar los permisos y registrar las operaciones para detectar usos indebidos de los sistemas de información de la universidad pública. La gestión de cuentas inactivas y del almacenamiento en la nube está estrecha y directamente vinculada con el control de la exposición y de los recursos disponibles.

4. Las medidas técnicas deben responder a riesgos identificados

Entre las actuaciones prioritarias a implementar destacan la autenticación multifactor, los cortafuegos de aplicaciones web, la protección de redes y seguimiento de credenciales comprometidas, etc.

5. La formación contribuye a la seguridad colectiva

Los hábitos del estudiantado, el personal docente e investigador y el personal técnico, de gestión y administración y servicios constituyen un factor decisivo que condiciona la protección de la infraestructura y los sistemas de información universitaria. Los planes de concienciación deben ayudar a reconocer riesgos y utilizar adecuadamente las herramientas institucionales y, necesariamente, deberían alcanzar al 100% de la comunidad universitaria.

6. Los órganos de gobierno deben implicarse en la gestión de riesgos

Las políticas de seguridad digital están estrechamente imbricadas con la aprobación, la supervisión y la financiación institucionales. Un ciberincidente no solamente puede paralizar el normal funcionamiento de una institución académica, sino también afectar a los derechos de las personas afectadas, además del correspondiente coste reputacional.

Líneas futuro de trabajo

Articular un programa de seguridad con responsables identificados, revisión de accesos, formación y procedimientos coordinados de respuesta y recuperación.



VNiVERSiDAD
D SALAMANCA

NEGUEDA.USAL.ES