Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

LA RESPONSABILIDAD INSTITUCIONAL DE LAS UNIVERSIDADES PÚBLICAS MEXICANAS EN EL TRATAMIENTO DE DATOS PERSONALES: MARCO NORMATIVO, DESAFÍOS Y ALCANCES EN LA ERA DIGITAL

INSTITUTIONAL RESPONSIBILITY OF MEXICAN PUBLIC UNIVERSITIES IN THE PROCESSING OF PERSONAL DATA: LEGAL FRAMEWORK, CHALLENGES, AND SCOPE IN THE DIGITAL ERA

Ana Cristina Marmolejo Alcántara
Universidad Autónoma de Querétaro, México

Cristina Alcántara Donaciano
Universidad Autónoma de Querétaro, México

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22814

La Responsabilidad Institucional de las Universidades Públicas Mexicanas en el Tratamiento de Datos Personales: Marco Normativo, Desafíos y Alcances en la Era Digital

Ana Cristina Marmolejo Alcántara[1]
cristinamar2241@gmail.com
https://orcid.org/0009-0004-2453-2834
Universidad Autónoma de Quéretaro
México

Cristina Alcántara Donaciano
cristina.alcantara@uaq.mx
https://orcid.org/0009-0004-4591-0013
Universidad Autónoma de Quéretaro
México

RESUMEN

El presente estudio analiza la responsabilidad institucional de las universidades públicas mexicanas en el tratamiento y protección de datos personales, considerando el marco jurídico nacional y los desafíos derivados de la creciente digitalización. A partir del reconocimiento de la privacidad como derecho humano fundamental y de las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017), se examinan las obligaciones específicas que recaen en estas instituciones como sujetos obligados. La investigación evalúa el cumplimiento de principios como licitud, consentimiento, finalidad, proporcionalidad y seguridad, así como el papel desempeñado por el INAI como autoridad garante hasta su desaparición. Asimismo, se identifican riesgos recurrentes, entre ellos vulneraciones, filtraciones, protocolos insuficientes y debilidades estructurales en materia de ciberseguridad. Desde una perspectiva interdisciplinaria, se plantea que la protección de datos personales no solo constituye una obligación normativa, sino una dimensión esencial de la gobernanza universitaria que impacta directamente en la confianza social. Finalmente, se proponen estrategias orientadas al fortalecimiento de políticas internas y a la consolidación de una cultura de responsabilidad digital en las universidades públicas.

***Palabras clave*:** datos personales, universidades públicas, responsabilidad institucional, marco jurídico, ciberseguridad

[1] Autor principal
Correspondencia: cristinamar2241@gmail.com

Institutional Responsibility of Mexican Public Universities in the Processing of Personal Data: Legal Framework, Challenges, and Scope in the Digital Era

ABSTRACT

This study analyzes the institutional responsibility of Mexican public universities in the processing and protection of personal data, considering the national legal framework and the challenges posed by increasing digitalization. Based on the recognition of privacy as a fundamental human right and the provisions of the General Law on the Protection of Personal Data Held by Obligated Subjects (2017), the specific obligations of universities as public entities are examined. The research evaluates compliance with key principles such as lawfulness, consent, purpose, proportionality, and security, and discusses the role previously exercised by the National Institute for Transparency, Access to Information and Personal Data Protection (INAI) until its disappearance. It identifies recurring risks, including data breaches, unauthorized disclosures, insufficient security protocols, and structural weaknesses in cybersecurity management. From an interdisciplinary perspective, the study understands personal data protection not only as a regulatory duty but also as a dimension of institutional governance that directly affects public trust. Finally, it proposes strategies aimed at strengthening data governance policies and reinforcing a culture of accountability within public universities in the digital era.

***Keywords*:** personal data, public universities, institutional responsibility, legal framework, cybersecurity

Artículo recibido 02 enero 2026
Aceptado para publicación: 30 enero 2026

INTRODUCCIÓN

La falta de infraestructura tecnológica, de supervisión y de comités especializados en la protección de datos personales incrementa los riesgos de filtración, uso indebido o pérdida de información académica, laboral o administrativa dentro de las universidades públicas mexicanas, afectando directamente el derecho fundamental a la privacidad de datos personales. Esta situación refleja un desafío persistente en la era digital y revela una brecha relevante entre el marco normativo existente particularmente la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y su implementación cotidiana en las instituciones, lo que implica vulneraciones y prácticas ineficaces en la gestión de la información personal de las comunidades universitarias. Aunque las universidades operan bajo obligaciones jurídicas claras y han incorporado mecanismos como Unidades de Transparencia y avisos de privacidad, estas herramientas suelen funcionar de manera mínima o reactiva, sin consolidar una cultura institucional sólida en materia de protección de datos.

En este trabajo se examina la forma en que las universidades públicas cumplen su responsabilidad institucional en el tratamiento de datos personales, atendiendo tanto al marco jurídico aplicable como a los desafíos derivados de la creciente digitalización de procesos académicos y administrativos. A lo largo del estudio se analizan elementos normativos, organizacionales y tecnológicos que permiten comprender el alcance real del cumplimiento universitario, problemáticas como vulneraciones, filtraciones y deficiencias en medidas de seguridad, así como los retos emergentes asociados al uso de plataformas digitales, gestión de sistemas automatizados y riesgos de ciberseguridad. Asimismo, se busca identificar hasta qué punto estas instituciones cuentan con políticas internas efectivas, mecanismos de supervisión y medidas de prevención que garanticen un tratamiento adecuado de la información personal.

La investigación parte de la premisa de que el tratamiento adecuado de los datos personales no depende únicamente de la existencia de normas, sino de la capacidad institucional para aplicarlas mediante políticas internas claras, capacitación del personal y mecanismos de seguridad robustos. Bajo esta línea, se explorará si el fortalecimiento de la infraestructura tecnológica y la gestión adecuada de procesos digitales permite disminuir vulneraciones, en concordancia con la idea de que una mejora estructural reduce los riesgos de filtración y uso indebido de información. Desde esta perspectiva, se indagan los principios rectores que estructuran la protección de datos personales, la evolución constitucional del derecho a la

privacidad y el papel que desempeñaba el INAI como autoridad garante. En este proceso se consideran tanto las obligaciones formales que recaen en las universidades como sujetos obligados, como los factores que explican la persistencia de incidencias: insuficiencia presupuestal, ausencia de personal especializado y el manejo heterogéneo de sistemas digitales.

El análisis se desarrolla mediante una revisión documental que permite sistematizar criterios jurídicos, informes institucionales y literatura académica reciente. A través de un enfoque cualitativo se examinan documentos normativos y casos reportados, utilizando un método de razonamiento deductivo que parte del marco jurídico general para descender a las prácticas y experiencias concretas de diversas universidades públicas. Esta aproximación indirecta, basada en el análisis de legislación, lineamientos, reportes y estudios especializados, ofrece una visión amplia y comparada que permite valorar si las estrategias implementadas por las instituciones resultan suficientes frente a los riesgos actuales.

Con base en este análisis se abordan las vulneraciones documentadas, los desafíos organizacionales y las limitaciones estructurales, mediante una revisión sistemática de informes institucionales, criterios normativos y estudios recientes en la materia. Este enfoque permite no solo identificar el estado actual de cumplimiento, sino también valorar si las políticas internas, la capacitación y la aplicación de principios legales contribuyen a reducir riesgos y fortalecer la responsabilidad digital en las universidades. El procesamiento de esta evidencia permite anticipar tendencias y resultados esperados respecto de la manera en que estas instituciones han enfrentado la era digital, así como delimitar los alcances reales de su cumplimiento jurídico.

Los resultados del estudio permiten observar que las vulneraciones no se explican únicamente por fallas técnicas, sino por errores humanos, deficiencias institucionales más profundas que requieren atención estratégica. La evidencia analizada confirma que la efectividad del marco jurídico depende en gran medida de la capacidad real de las universidades para implementar medidas preventivas, garantizar derechos y establecer mecanismos permanentes de supervisión. En ese sentido, el análisis ofrece una visión integral sobre los alcances y limitaciones del sistema actual y permite delinear conclusiones orientadas a proponer acciones institucionales que favorezcan una cultura de protección de datos más robusta, coherente y acorde con las exigencias de la era digital.

Antecedentes

Vulneraciones y problemáticas registradas en el manejo de datos personales en las universidades públicas mexicanas.

1. Responsabilidad institucional y políticas internas de las universidades públicas mexicanas

Según el INAI (2019, p. 665), la responsabilidad institucional en el tratamiento de datos personales implica la obligación de garantizar la licitud, seguridad, confidencialidad y finalidad legítima de los datos tratados. El Diccionario de Protección de Datos Personales del INAI (2019) define este principio como la capacidad del responsable de demostrar que las operaciones realizadas sobre datos personales cumplen con la normativa aplicable

Arellano López (2020) señala que las instituciones mexicanas deben transitar de un modelo básico de gestión de datos personales (GDP) hacia un Sistema de Gestión de Protección de Datos Personales (SGPDP), que incorpore medidas administrativas, técnicas y organizacionales integrales.

No obstante, el Tercer Censo Nacional de Transparencia (INEGI, 2019) evidencia deficiencias significativas en el cumplimiento normativo: el 44 % de las instituciones desconoce las obligaciones previstas en la LGPDPPSO y la LFPDPPP; el 50 % no cuenta con capacidad técnica suficiente para atender los derechos ARCO; y únicamente el 48 % ha implementado procesos de capacitación interna. En la misma línea, Arellano López (2020, p. 171) advierte que solo el 6 % dispone de personal especializado en la materia.

Chornet (2021) sostiene que las universidades públicas, en su calidad de sujetos obligados, administran expedientes académicos, laborales, financieros e incluso médicos, lo que exige políticas internas claras, personal capacitado, sistemas de seguridad digital y procedimientos estandarizados. Sin embargo, muchas carecen de protocolos homogéneos que permitan determinar con precisión qué información puede divulgarse y cuáles datos deben reservarse.

Conforme a los Lineamientos Generales (INAI, 2024, arts. 26–28), los responsables deben emitir avisos de privacidad claros, garantizar el ejercicio de los derechos ARCO y evitar divulgaciones indebidas. El INAI, como autoridad garante, resolvía estos conflictos aplicando criterios de proporcionalidad, máxima publicidad y protección reforzada de datos sensibles.

2. Uso indebido y filtración de datos personales

El INAI (2023, pp. 118, 133–134) identifica el uso indebido de datos personales como una de las problemáticas más frecuentes en universidades, hospitales y dependencias públicas. El Informe Anual de Labores 2023 documenta un incremento en vulneraciones derivadas tanto de errores humanos como de fallas técnicas, así como la difusión no autorizada de bases de datos institucionales y la publicación de información académica o médica sin consentimiento.

En particular, el INAI (2023, p. 133) precisa que "las vulneraciones notificadas incluyeron filtraciones accidentales o deliberadas de bases de datos institucionales, muchas de las cuales terminaron publicadas en plataformas digitales o utilizadas con fines comerciales". Asimismo, el artículo 66 de los Lineamientos Generales (INAI, 2024) prohíbe expresamente la transferencia no autorizada de datos personales sin fundamento legal o consentimiento expreso.

El propio INAI (2023, p. 18) ha detectado incluso la venta de bases de datos de estudiantes, servidores públicos o pacientes, conductas que constituyen violaciones graves y pueden derivar en responsabilidades administrativas e incluso penales.

3. Ciberseguridad y gestión digital universitaria

Las universidades públicas utilizan plataformas digitales para la gestión académica, trámites administrativos, servicios escolares, control biométrico y sistemas de archivo digital. Sin embargo, el INAI (2023, p. 118) advierte que muchas presentan vulnerabilidades estructurales, tales como contraseñas débiles, sistemas de almacenamiento obsoletos, ausencia de cifrado en bases de datos, falta de controles de autenticación y accesos no autorizados por terceros.

Durante 2023, el 27 % de los incidentes de vulneración se debieron a fallas técnicas en sistemas informáticos. En el ámbito de la salud universitaria, el expediente clínico electrónico también enfrenta riesgos asociados a infraestructura insuficiente, problemas de interoperabilidad y accesos indebidos (Piña-Mondragón, 2021, pp. 23–25).

En un plano más amplio, Harari (2024) advierte que el poder contemporáneo radica en el control de la información y señala la necesidad de no "invocar un poder que no se puede controlar", en referencia al uso acrítico de tecnologías avanzadas, incluida la inteligencia artificial. Esta reflexión resulta pertinente para las universidades que digitalizan procesos sin implementar protocolos de seguridad adecuados.

4. Comités de transparencia y unidades de datos personales

Los Comités de Transparencia y las Unidades de Transparencia constituyen órganos fundamentales en la gestión institucional de datos personales dentro de las universidades públicas. De conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales emitidos por el INAI (2024), estos órganos deben aprobar políticas internas de protección de datos (art. 47), supervisar el cumplimiento de las medidas de seguridad, atender solicitudes de ejercicio de derechos ARCO y notificar incidentes de seguridad en un plazo máximo de 72 horas (art. 66).

No obstante, diversos estudios señalan que, en la práctica, muchas universidades carecen de comités plenamente funcionales o los integran únicamente de manera formal, sin capacidad operativa real ni personal especializado (Dialnet, 2021, p. 7). Esta situación genera debilidades en la supervisión interna, retrasa la atención de incidentes y limita la implementación efectiva de políticas preventivas.

La ausencia de estructuras institucionales sólidas no solo afecta el cumplimiento normativo, sino que compromete la confianza de la comunidad universitaria en la gestión de su información personal. En consecuencia, el fortalecimiento de estos órganos resulta indispensable para consolidar una cultura institucional de protección de datos.

5. El aviso de privacidad

El aviso de privacidad constituye una de las obligaciones centrales del responsable del tratamiento de datos personales. Conforme al artículo 26 de los Lineamientos Generales (INAI, 2024), este debe ser claro, accesible, específico y actualizado, a fin de garantizar que los titulares conozcan las finalidades del tratamiento y los mecanismos para ejercer sus derechos.

En el ámbito universitario, se observan con frecuencia diversas deficiencias, tales como avisos incompletos o desactualizados, falta de visibilidad para estudiantes y docentes, omisión de finalidades específicas del tratamiento y ausencia de avisos en sistemas de videovigilancia, controles biométricos o plataformas digitales. Estas omisiones generan incertidumbre jurídica y vulneran el principio de información, afectando directamente el derecho a la autodeterminación informativa.

La falta de avisos adecuados no solo contribuye a la opacidad institucional, sino que incrementa el riesgo de vulneraciones y posibles sanciones administrativas.

Por ello, su correcta elaboración y difusión representa una medida preventiva esencial dentro del Sistema de Gestión de Protección de Datos Personales.

Análisis del marco jurídico mexicano sobre la protección de datos personales en las universidades públicas mexicanas

1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2017) regula de manera directa a las universidades públicas en su calidad de sujetos obligados. En consecuencia, les impone obligaciones específicas orientadas a garantizar un tratamiento adecuado de la información personal.

Entre sus principales deberes se encuentran la licitud del tratamiento, la determinación de finalidades específicas y legítimas, la obtención del consentimiento cuando resulte procedente, la implementación de medidas de seguridad administrativas, técnicas y físicas, el deber de confidencialidad, la garantía de los derechos de acceso, rectificación, cancelación y oposición (ARCO), así como la obligación de notificar vulneraciones de seguridad.

Asimismo, la ley considera como datos personales sensibles aquellos relacionados con la salud, la trayectoria educativa y la situación laboral, entre otros (arts. 24–25), lo que implica la adopción de medidas reforzadas de protección por parte de las instituciones universitarias.

2. Marco jurídico de la protección de datos personales en México.

El marco jurídico mexicano en materia de protección de datos personales se integra por disposiciones de rango constitucional, legal y reglamentario. En el ámbito constitucional, los artículos 6° y 16° de la Constitución Política reconocen el derecho a la protección de datos personales y establecen las bases para su tutela.

En el plano legal, la LGPDPPSO regula el tratamiento de datos en el sector público, mientras que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) rige al sector privado. A ello se suman los Lineamientos Generales emitidos por el INAI (2024), así como regulaciones técnicas, acuerdos y criterios interpretativos.

La Suprema Corte de Justicia de la Nación ha contribuido a delimitar el alcance de este derecho. En este sentido, Piña-Mondragón (2021, pp. 18–19) señala que la SCJN ha reiterado que los expedientes

clínicos y educativos pertenecen al titular de los datos, mientras que las instituciones únicamente actúan como responsables del tratamiento. Este entramado normativo configura un sistema integral que impone obligaciones claras a las universidades públicas y delimita los márgenes entre transparencia y privacidad.

3. Evolución constitucional del derecho a la privacidad

La protección de datos personales adquirió reconocimiento constitucional expreso con la reforma de 2009 al artículo 16, mediante la cual se estableció el derecho a la protección de datos personales, así como los derechos de acceso, rectificación y cancelación. Asimismo, se impuso al Estado la obligación de garantizar mecanismos efectivos de tutela y salvaguardas administrativas adecuadas.

Posteriormente, la reforma constitucional en materia de transparencia de 2014 fortaleció la competencia del INAI como órgano garante autónomo encargado de tutelar tanto el derecho de acceso a la información como la protección de datos personales. Este diseño institucional permitió articular un equilibrio entre el principio de máxima publicidad y la protección reforzada de datos sensibles.

Menciona Guerrero et al. (2026) que la virtualización acelerada de la educación superior ha incrementado la captura, almacenamiento, análisis y circulación de datos personales a través de aulas virtuales, videoconferencias, repositorios institucionales, herramientas de evaluación y sistemas de analítica del aprendizaje. En este ecosistema, la identidad digital estudiantil se vuelve un activo crítico: credenciales, trazas de acceso, interacciones, rendimiento académico y contenidos generados por el usuario pueden ser tratados por múltiples actores, lo que amplía la superficie de riesgo y exige gobernanza institucional.

Señala Borbor, I. (2025) que, en la educación superior digitalizada, donde la gestión de plataformas virtuales, sistemas de gestión de aprendizaje y herramientas de inteligencia artificial es cada vez más frecuente, la recopilación, almacenamiento y tratamiento de datos sensibles exige protocolos claros, políticas institucionales y cumplimiento normativo. La adecuada protección de estos datos no solo previene vulneraciones legales y ciberataques, sino que también fortalece la confianza de la comunidad educativa en los entornos digitales.

4. El papel del INAI como autoridad garante hasta su desaparición

De acuerdo con el INAI (2023, p. 125), dicho organismo fungió como autoridad responsable de resolver conflictos entre transparencia y privacidad, emitir lineamientos y criterios técnicos, imponer sanciones por vulneración de datos personales, realizar procedimientos de verificación, supervisar comités y unidades de transparencia y ordenar la notificación de incidentes de seguridad.

Entre 2023 y 2024 resolvió múltiples casos relacionados con universidades, hospitales y dependencias públicas que difundieron información académica o médica sin consentimiento. Su desaparición genera un vacío institucional que impacta directamente en la supervisión y garantía efectiva del derecho a la protección de datos personales en el ámbito universitario.

La desaparición del INAI como menciona Castillo, H., (2025) elimina un garante independiente e imparcial del derecho de acceso a la información pública. Al transferir esta función a la Secretaría de Anticorrupción y Buen Gobierno, que forma parte del poder Ejecutivo, se pone en riesgo la independencia de las decisiones relacionadas con el acceso a la información pública, ya que no se puede garantizar que actúe sin intereses políticos o partidistas.

De esta manera, Castillo, H., (2025) asegura que, si bien el derecho constitucional al acceso a la información pública se conserva, lo cierto es que hemos perdido la institución encargada de garantizarlo. Conforme a este nuevo paradigma, la propia administración pública actuará como juez y parte en cualquier conflicto relacionado con el acceso a la información pública gubernamental. No es difícil poder avizorar que ello puede derivar en una mayor opacidad gubernamental.

Gutiérrez, A., & Calderón, J. M. (2025) afirman que la reciente decisión de extinguir el INAI y, en consecuencia, a los órganos garantes de las entidades federativas para regresar sus funciones al poder ejecutivo, bajo el argumento de la simplificación orgánica, representa un riesgo para que funcionarios y funcionarias actúen inadecuadamente frente a las múltiples funciones que llevan a cabo. El hecho de coincidir la simplificación orgánica con el cierre del INAI y el traslado de funciones al poder ejecutivo hace que quien genera, clasifica y reserva la información pasa a ser, a la vez, juez de sus propias decisiones.

Retos tecnológicos, organizacionales y normativos que enfrentan las universidades públicas mexicanas

El cumplimiento del marco jurídico descrito no depende únicamente de la existencia de normas claras, sino de la capacidad institucional para implementarlas de manera efectiva. En este contexto, las universidades públicas enfrentan desafíos estructurales que dificultan la consolidación de sistemas sólidos de protección de datos personales.

1. Principios rectores del tratamiento de datos personales

Según el INAI (2019, pp. 652–663), los principios rectores del tratamiento de datos personales son: licitud, finalidad, consentimiento, información, calidad, seguridad, confidencialidad, proporcionalidad y responsabilidad. Estos principios constituyen el parámetro fundamental para evaluar el cumplimiento normativo por parte de las universidades públicas.

El principio de responsabilidad, en particular, exige que las instituciones no solo cumplan la normativa, sino que puedan demostrar dicho cumplimiento mediante políticas internas documentadas y mecanismos verificables.

2. Problemas y casos frecuentes

El Informe Anual de Labores 2023 del INAI (2023, pp. 118–134) documenta incidentes recurrentes en universidades públicas, entre los que destacan la publicación de listas de estudiantes con datos sensibles, la filtración de expedientes académicos y laborales, accesos indebidos a plataformas institucionales, extravío de expedientes físicos o digitales, divulgación de información médica en hospitales universitarios y manejo inadecuado de bases de datos por proveedores externos.

Estos casos evidencian deficiencias estructurales en los sistemas de control interno y en la cultura institucional de protección de datos personales.

3. Limitaciones técnicas y presupuestales

Las universidades públicas frecuentemente carecen de infraestructura tecnológica adecuada, personal especializado en protección de datos, sistemas robustos de ciberseguridad y presupuestos específicos destinados a esta materia.

Si bien los Lineamientos Generales (INAI, 2024, art. 62) establecen que los responsables deben destinar recursos humanos, financieros y tecnológicos suficientes para garantizar la seguridad de la información,

en la práctica muchas instituciones enfrentan restricciones estructurales que dificultan el cumplimiento integral de dichas obligaciones.

4. Desafíos en la era digital

La incorporación de inteligencia artificial, reconocimiento biométrico, videovigilancia y sistemas automatizados en el entorno universitario exige nuevas capacidades institucionales. INFO CDMX (2024) advierte que la región enfrenta dificultades para adaptar su marco jurídico a estándares internacionales como el Reglamento General de Protección de Datos (GDPR), particularmente ante el avance acelerado de tecnologías emergentes.

En esta misma línea, Harari (2024) señala que gobiernos e instituciones compiten por desarrollar tecnologías cada vez más poderosas, lo que incrementa los riesgos cuando no se ejerce un control ético y jurídico adecuado.

5. Propuestas de fortalecimiento institucional

Diversos estudios y organismos especializados (INFO CDMX, 2024; INFOEM, 2025) identifican propuestas orientadas al fortalecimiento institucional, entre las que destacan:

- Establecer Comités Universitarios de Protección de Datos Personales.
- Incluir materias de privacidad y ética digital en los planes de estudio.
- Implementar evaluaciones de impacto antes de digitalizar sistemas.
- Crear unidades especializadas para el resguardo y auditoría de datos sensibles.
- Impulsar convenios entre universidades y organismos garantes locales.
- Homologar protocolos internos con estándares internacionales.
- Promover una cultura institucional de seguridad digital y privacidad.

Estas medidas apuntan hacia la consolidación de una gestión preventiva y responsable del tratamiento de datos personales en el ámbito universitario.

CONCLUSIÓN

Atilio, H., et. al. (2025) afirma que la protección de datos personales no debe concebirse únicamente como una obligación jurídica, sino como un componente esencial de la confianza pública, la autonomía universitaria y la dignidad de las personas.

Su garantía efectiva constituye, en última instancia, un indicador del compromiso democrático de las instituciones educativas frente a los desafíos de la era digital.

Atilio, H., et. al. (2025) menciona que para aprovechar las oportunidades y superar los desafíos identificados, es crucial generar líneas de acción estratégicas en los usos de la tecnología educativa en el contexto universitario para explorar las aplicaciones prácticas de la tecnología en tres pilares fundamentales del proceso educativo, entre ellos se tienen el aprendizaje, la enseñanza y evaluación, y la administración y gestión, son los tres aspectos claves que se entrelazan para crear una sinergia o interacción armoniosa en el contexto de la tecnología educativa, cada uno de estos componentes juega un papel crucial en la transformación de la experiencia educativa, permitiendo una integración fluida de la tecnología en el día a día de las instituciones universitarias.

En México, la protección de datos personales se consolidó a partir de las reformas constitucionales de 2009 y 2014, las cuales dieron origen a un marco normativo específico para el sector público y fortalecieron los mecanismos institucionales de tutela. No obstante, los informes del INAI (2023) evidencian vulneraciones recurrentes en universidades públicas mexicanas, principalmente asociadas a deficiencias en seguridad digital, capacitación y supervisión interna. La literatura contemporánea coincide en que el cumplimiento normativo no puede reducirse a la existencia formal de leyes, sino que debe acompañarse de una cultura institucional basada en la responsabilidad proactiva y la ética digital.

El análisis desarrollado en este trabajo permite confirmar la hipótesis planteada: las vulneraciones de datos personales en las universidades públicas mexicanas derivan principalmente de deficiencias institucionales estructurales y no exclusivamente de fallas tecnológicas. La evidencia revisada demuestra que la ausencia de políticas internas claras, la falta de capacitación especializada y el incumplimiento de los principios establecidos en la LGPDPPSO constituyen factores determinantes en los incidentes reportados. Aunque el marco jurídico mexicano puede considerarse robusto en términos normativos, su implementación práctica presenta inconsistencias significativas que debilitan su eficacia.

Finalmente, resulta indispensable que las universidades adopten modelos formales de gobernanza de datos, consoliden comités especializados con capacidad operativa real, fortalezcan sus sistemas de ciberseguridad y establezcan programas permanentes de profesionalización en materia de protección de

datos personales. Solo mediante un fortalecimiento institucional integral será posible reducir las vulneraciones y avanzar hacia una auténtica cultura de responsabilidad digital en el ámbito universitario.

REFERENCIAS BIBLIOGRAFICAS

Arellano López, C. A. (2020). El derecho de protección de datos personales. Revista Biolex, 23, 163–174. https://doi.org/10.36796/Biolex.v0i23.194

Díaz Lima, D. (2023). Transparencia y protección de datos personales en el ámbito universitario: ¿Avance o retroceso? Revista Española de la Transparencia, 17, 201–224. https://doi.org/10.51915/ret.311

Harari, Y. N. (2024, August 24). Never summon a power you can't control. The Guardian. https://www.theguardian.com/world/2024/aug/24/never-summon-a-power-you-cant-control

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX). (2024). Desafíos del derecho a la protección de datos personales en la era digital: Una mirada desde América Latina. Tirant Lo Blanch.

Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM). (2025). Programa de cultura de protección de datos personales del Estado de México 2025–2027.

Instituto Nacional de Estadística y Geografía (INEGI). (2019). Tercer censo nacional de transparencia, acceso a la información pública y protección de datos personales.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2019). Diccionario de protección de datos personales.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2023). Informe anual de labores 2023. Ciudad de México: INAI.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2024). Lineamientos generales de protección de datos personales para el sector público (versión integrada con reformas al 14 de junio de 2024). Diario Oficial de la Federación.

Piña-Mondragón, J. J. (2021). Tratamiento y protección de datos personales en el sector público de la salud: El tránsito hacia el expediente clínico electrónico. Universidad De La Salle Bajío.

Guerrero, H. A., Plaza, V. P., Alcívar, I. M., & Murillo, A. R. (2026). Protección de datos personales: estudiantes universitarios en entornos virtuales, desafíos y propuestas en el contexto ecuatoriano. Pulso Científico, volumen 4. Páginas 50-65. https://doi.org/10.70577/rps.v4i1.144

Borbor, I., (2025). Protección de Datos y Propiedad Intelectual en la Educación Superior Digitalizada: Retos Legales Frente al uso de Inteligencia Artificial y Recursos Tecnológicos en los Procesos Pedagógicos. Reincisol, 4(8), pp. 4011-4036. https://doi.org/10.59282/reincisol.V4(8)4011-4036

Castillo, H., (2025). La desaparición del INAI ¿Reforma constitucional regresiva?. Hechos y derechos. Volumen 16. Número 86. https://revistas.juridicas.unam.mx/index.php/hechosyderechos/article/view/20040/20019

Atilio, H., Silvia, D. N., & Labrador, O. M., (2025). Nuevas fronteras de la educación universitaria: Desafíos y oportunidades de las tecnologías digitales. Revista Formación Estratégica. Vol. 12 Núm. 2. https://formacionestrategica.com/index.php/foes

Gutiérrez Luna, A., & Calderón Pérez, J. M. (2025). La desaparición del INAI y sus implicaciones en la percepción de la corrupción en México. ¿Retroceso institucional?. Estudios En Derecho a La Información, 11(21), e20560. https://doi.org/10.22201/iij.25940082e.2026.21.20560