



PROGRAMA
DIAGNÓSTICO
DE CUMPLIMIENTO
en materia de protección
de datos personales
UNAM

PROTOCOLO
METODOLÓGICO



UNAM
Nuestra gran
Universidad

475+
UNIVERSIDAD
de MÉXICO
1551 2026



PROTOCOLO METODOLÓGICO

Contenido

I.	Presentación	2
II.	Glosario.....	3
III.	Objetivos.....	5
IV.	Marco normativo.....	6
V.	Disposiciones generales	8
	a) Competencia:.....	8
	b) Instancias universitarias involucradas:.....	8
VI.	Principios que rigen el tratamiento de los datos personales	11
VII.	Procedimiento	12
	a) Proceso de selección de áreas sujetas al Programa Diagnóstico.....	12
	b) Preparación.....	14
	c) Reunión preparatoria	15
	d) Emisión de minuta de la reunión preparatoria	15
	e) Desarrollo del Diagnóstico de Cumplimiento	16
	f) Notificaciones.....	16
	g) Etapa de revisión	16
	h) Conclusión del Diagnóstico de Cumplimiento	17
	i) Plan de acción.....	17
	j) Atención de recomendaciones	18
	k) Emisión del Acuerdo de seguimiento.....	18
VIII.	Referencias para las actuaciones del equipo revisor	18
	a) Autoridad Garante de la UNAM.....	18
	b) Dirección General de Cómputo y de Tecnologías de Información y Comunicación	20
	c) Área Coordinadora de Archivos de la UNAM	21
IX.	Anexos	24



I. Presentación

El 20 de diciembre de 2024 se aprobó la reforma constitucional al artículo 6º, con la que se transformó de manera sustancial el modelo de autoridades garantes de dos derechos fundamentales: el acceso a la información pública y la protección de datos personales. Posteriormente, el 20 de marzo de 2025 se publicaron en el Diario Oficial de la Federación la nueva "Ley General de Transparencia y Acceso a la Información Pública", la "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", así como la "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", las cuales modificaron de manera integral el marco jurídico aplicable en ambas materias.

El eje central de esta reforma fue la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, cuyas funciones fueron redistribuidas entre diversas autoridades garantes a nivel federal y local.

En este nuevo esquema, las instituciones públicas autónomas quedaron obligadas a crear su propia Autoridad Garante con autonomía técnica y presupuestal, como es el caso de la Universidad Nacional Autónoma de México (UNAM). En ese contexto, el 19 de mayo de 2025 se publicó en la Gaceta UNAM el "Acuerdo que crea y establece funciones de la Autoridad Garante de la Universidad Nacional Autónoma de México en materia de acceso a la información pública y protección de datos personales". La Autoridad Garante (AGA UNAM) cuenta con atribuciones para interpretar la normatividad aplicable en materia de acceso a la información pública, así como resolver recursos de revisión y vigilar el cumplimiento de disposiciones en materia de protección de datos personales, y de acceso a la información pública dentro de la Universidad.

Como parte de las labores de vigilancia y con un enfoque preventivo, la Autoridad Garante de la Universidad, implementará revisiones diagnósticas a las áreas universitarias con el fin de identificar riesgos, fortalecer medidas de seguridad y promover el cumplimiento de las obligaciones en materia de protección de datos personales en la materia, así como el desarrollo de una cultura institucional de protección de datos personales.



PROTOCOLO METODOLÓGICO

Para el desarrollo de estas revisiones diagnósticas, la Autoridad Garante de la UNAM contará con la participación técnica y especializada de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación y del Área Coordinadora de Archivos de la UNAM, en el ámbito de sus respectivas competencias.

La intervención de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación permitirá evaluar los aspectos tecnológicos y las medidas de seguridad de los sistemas de tratamiento de datos personales, mientras que la participación del Área Coordinadora de Archivos de la UNAM se orientará a la revisión de los procesos de gestión documental, el ciclo de vida de los documentos y las condiciones de resguardo archivístico de aquellos que contienen datos personales.

La coordinación entre estas instancias universitarias permitirá a la Autoridad Garante de la UNAM contar con una visión integral del tratamiento de los datos personales, considerando tanto los componentes normativos, técnicos y archivísticos, como las prácticas operativas de las áreas universitarias, privilegiando en todo momento un enfoque de acompañamiento, prevención y mejora continua.

II. Glosario

- a) **Áreas Universitarias:** Las Autoridades Universitarias, Cuerpos Colegiados, Dependencias Administrativas, Entidades Académicas, Tribunal Universitario y Defensoría de los Derechos Universitarios;
- b) **Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos;
- c) **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;
- d) **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando



PROTOCOLO METODOLÓGICO

su identidad pueda determinarse directa o indirectamente a través de cualquier información. La información académica que obre en los archivos universitarios constituye un dato personal;

- e) **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, así como opiniones políticas y preferencia sexual;
- f) **Derechos ARCO:** Derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales;
- g) **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;
- h) **Equipo revisor:** equipo de trabajo interinstitucional encargado de la coordinación y ejecución del Programa Diagnóstico, conformado por personal adscrito a la Autoridad Garante de la UNAM, la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM y el Área Coordinadora de Archivos de la UNAM, adscrita a la Dirección General de Servicios Generales y Movilidad;
- i) **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales; las pueden clasificarse en:
 - i. **Medidas de seguridad administrativas:** Políticas, procedimientos y prácticas orientadas a la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, que incluyen la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;
 - ii. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico en el que se resguardan los datos personales y los recursos involucrados en su tratamiento;
 - iii. **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que, mediante el uso de tecnologías de hardware y software, permiten proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento;

PROTOCOLO METODOLÓGICO

- j) **Normas complementarias:** Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad publicadas en la Gaceta el 30 de enero de 2020;
- k) **Personas acompañantes:** personas designadas por los titulares de las áreas universitarias para atender la revisión diagnóstica del Programa, o bien, aquellas designadas previamente responsables de archivos y/o como responsables de seguridad de datos personales del área universitaria;
- l) **Programa Diagnóstico de cumplimiento:** Es un instrumento jurídico preventivo, que constituye un mecanismo de revisión orientado a identificar riesgos, brechas y áreas de oportunidad en el tratamiento de datos personales, fortalecer el principio de responsabilidad y asegurar que las áreas universitarias cumplan de manera efectiva con sus obligaciones legales, sin constituir un procedimiento sancionador;
- m) **Sistemas de Gestión de Seguridad de Datos Personales:** Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales;
- n) **Sistema de Tratamiento de Datos:** Conjunto de elementos que conforman las operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales; sistemas que serán objeto de la revisión diagnóstica del presente protocolo.
- o) **Responsable:** Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

III. Objetivos

El presente Protocolo tiene como objetivo establecer las bases, criterios y el procedimiento para la implementación del Programa Diagnóstico de cumplimiento en materia de protección de datos personales en la Universidad Nacional Autónoma de México, así como proporcionar a la comunidad universitaria información relacionada con la labor de vigilancia que realiza la Autoridad Garante de la UNAM, en coordinación con la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM y el Área Coordinadora de Archivos de la UNAM, para



PROTOCOLO METODOLÓGICO

implementar el Programa Diagnóstico de cumplimiento en materia de protección de datos personales.

El Programa Diagnóstico de cumplimiento es una iniciativa de carácter permanente para revisar y fortalecer los sistemas de tratamiento de datos personales en toda la universidad. Las áreas a evaluar serán seleccionadas a través de indicadores de cumplimiento en materia archivística, tecnologías de la información y protección de datos personales.

Con ello, se busca fortalecer la cultura de la protección de datos personales al interior de la universidad, con un enfoque preventivo y no sancionador, diseñado para impulsar la mejora continua de las áreas universitarias. En ese sentido, las instancias universitarias que participarán en la implementación del Programa Diagnóstico, la Autoridad Garante de la UNAM, la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM y el Área Coordinadora de Archivos de la UNAM, no ejercerán funciones sancionatorias.

Por ello, el presente Protocolo busca:

- Informar a las áreas universitarias sobre los procedimientos de revisión diagnóstica que implementa la Autoridad Garante de la UNAM en materia de protección de datos personales.
- Dar a conocer a las áreas universitarias las instancias responsables de la implementación del Programa Diagnóstico de cumplimiento en materia de protección de datos personales, así como sus ámbitos de competencia.
- Promover acciones de prevención, fortalecimiento y mejora continua de los mecanismos utilizados por las áreas universitarias para el cumplimiento de sus obligaciones en materia de protección de datos personales.
- Contribuir al desarrollo y consolidación de una cultura institucional de protección y privacidad de los datos personales en la UNAM.

IV. Marco normativo

La realización del Diagnóstico de Cumplimiento en materia de Protección de Datos Personales en la Universidad Nacional Autónoma de México es una obligación jurídica



PROTOCOLO METODOLÓGICO

y una medida institucional necesaria, derivada del marco constitucional, legal y universitario vigente.

El artículo 6° de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho humano a la protección de datos personales y establece la existencia de autoridades garantes responsables de tutelar su ejercicio. En desarrollo de este mandato, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados impone a los responsables del tratamiento la obligación de acreditar el cumplimiento de los principios, deberes y obligaciones en la materia (artículos 23 y 24), así como de someterse a mecanismos de supervisión, vigilancia y auditoría.

Asimismo, el artículo 83, fracción X, de dicha Ley faculta expresamente a las autoridades garantes para vigilar el cumplimiento de la normativa, lo que habilita la implementación de instrumentos preventivos de evaluación, como las revisiones diagnósticas.

En el ámbito universitario, el Acuerdo por el que se crea la Autoridad Garante de la UNAM establece que esta instancia es responsable de vigilar el cumplimiento de la normatividad en materia de protección de datos personales, emitir recomendaciones y promover acciones de mejora institucional. De manera complementaria, el Programa Universitario de Protección de Datos Personales prevé la realización de revisiones como mecanismos de supervisión continua.

A continuación, se señala de manera enunciativa, más no limitativa la normatividad universitaria aplicable al presente protocolo:

- Acuerdo que crea y establece funciones de la Autoridad Garante de la Universidad Nacional Autónoma de México en materia de Acceso a la Información Pública y Protección de Datos Personales.
- Reglamento Interno de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación.
- Acuerdo por el que se establece el Área Coordinadora de Archivos de la Universidad Nacional Autónoma de México.
- Acuerdo que actualiza las funciones del Área Coordinadora de Archivos de la Universidad Nacional Autónoma de México y crea al Grupo Interdisciplinario de Archivos Universitarios.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.



PROTOCOLO METODOLÓGICO

- Ley General de Archivos.
- Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México.
- Lineamientos para la Protección de Datos Personales en Posesión de la UNAM.
- Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad.
- Programa Universitario de Protección de Datos Personales 2021.

V. Disposiciones generales

a) Competencia:

El presente Protocolo es de observancia obligatoria y aplicación general para todas las áreas universitarias que realicen el tratamiento de datos personales de cualquier persona, con independencia del tipo de soporte, medio o sistema mediante el cual se lleve a cabo dicho tratamiento, ya sea físico, electrónico o digital.

b) Instancias universitarias involucradas:

o **Autoridad Garante de la UNAM**

La intervención de la Autoridad Garante de la UNAM en el Diagnóstico de Cumplimiento en materia de Protección de Datos Personales se sustenta en el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, así como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, particularmente en sus artículos 23 y 24 en su fracción V, que obligan a los responsables a implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones en la materia, y a rendir cuentas ante las autoridades garantes mediante sistemas de supervisión, vigilancia y auditoría, y en el artículo 83, fracción X, que faculta a las autoridades garantes para vigilar el cumplimiento de dicha Ley.

Asimismo, la competencia de la Autoridad Garante de la UNAM se encuentra expresamente reconocida en el "Acuerdo por el que se crea y se establecen las funciones de la Autoridad Garante de la Universidad Nacional Autónoma de México en materia de acceso a la información pública y protección de datos personales",

PROTOCOLO METODOLÓGICO

el cual la instituye como el órgano universitario con autonomía técnica y presupuestal responsable de garantizar el ejercicio del derecho a la protección de datos personales y de vigilar el cumplimiento de la normatividad aplicable por parte de las áreas universitarias.

De acuerdo con la normatividad citada la Autoridad Garante de la UNAM es competente para impulsar, coordinar y ejecutar revisiones diagnósticas como mecanismos de supervisión preventiva, emitir recomendaciones no vinculantes, promover la capacitación y elaborar estudios que fortalezcan la gestión institucional de los datos personales. Su intervención en el Diagnóstico de Cumplimiento tiene carácter preventivo y orientador, y no constituye un procedimiento sancionador.

- o **Dirección General de Cómputo y de Tecnologías de Información y Comunicación**

La participación de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación en el Diagnóstico de Cumplimiento en materia de protección de datos personales se sustenta en el Reglamento Interno de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, que la define como la dependencia universitaria responsable de supervisar los servicios centrales de cómputo y telecomunicaciones (artículo 1), establecer, operar y vigilar la infraestructura central de cómputo y telecomunicaciones (artículo 6, fracción I), planear, implementar, monitorear y evaluar los servicios de sistemas y telecomunicaciones (artículo 10, fracción III), así como proporcionar servicios estratégicos de tecnologías de la información, incluyendo cómputo en la nube, sistemas de identidad digital y seguridad de la información (artículo 18, fracción I).

De manera específica, las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad reconocen su competencia técnica al definir la auditoría técnica interna como el proceso realizado por esta dependencia para evaluar la adecuación, eficacia y conformidad de los controles y medidas de seguridad (artículo 2, fracción III), así como al establecer la obligación de someter dichas medidas a auditorías periódicas (artículo 13) y presentar evidencias de cumplimiento en los procesos de auditoría (artículo 17). A ello se suma el numeral 5 del Programa Universitario de Protección de Datos Personales 2021, que la faculta expresamente para realizar auditorías y revisiones.



PROTOCOLO METODOLÓGICO

En este contexto, la Dirección General de Cómputo y de Tecnologías de Información y Comunicación es competente para intervenir en el Diagnóstico de Cumplimiento exclusivamente en el ámbito técnico y tecnológico, con un carácter evaluativo y preventivo, orientado a identificar riesgos, vulnerabilidades y brechas de seguridad.

o **Área Coordinadora de Archivos de la UNAM**

La intervención del Área Coordinadora de Archivos de la UNAM en el Diagnóstico de Cumplimiento en materia de Protección de Datos Personales se sustenta en el *Acuerdo por el que se Establece el Área Coordinadora de Archivos de la Universidad Nacional Autónoma de México* (29 de julio de 2013), actualizado mediante el *Acuerdo que Actualiza las Funciones del Área Coordinadora de Archivos de la Universidad Nacional Autónoma de México y Crea al Grupo Interdisciplinario de Archivos Universitarios* (31 de julio de 2017).

La competencia del Área Coordinadora de Archivos de la UNAM se encuentra alineada con la Ley General de Archivos, particularmente con el artículo 4, fracción X, el artículo 21 y el artículo 27, que la reconocen como la instancia responsable de promover y vigilar la gestión documental, coordinar el Sistema Institucional de Archivos, elaborar instrumentos de control archivístico, coordinar la valoración y disposición documental y supervisar el ciclo de vida de los documentos. Asimismo, los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México, en su artículo 4, fracción V, y artículo 54, refuerzan dichas atribuciones.

Adicionalmente, el numeral 5 del Programa Universitario de Protección de Datos Personales 2021 reconoce expresamente la participación del Área Coordinadora de Archivos de la UNAM en auditorías y revisiones vinculadas con la protección de datos personales contenidos en documentos de archivo.

En este marco, el Área Coordinadora de Archivos de la UNAM es competente para intervenir en el Diagnóstico de Cumplimiento en el ámbito archivístico y de gestión documental, con un carácter técnico, preventivo y orientador, enfocado en la identificación de riesgos archivísticos, brechas en el ciclo de vida documental y áreas de oportunidad en el tratamiento de datos personales.



PROTOCOLO METODOLÓGICO

Canaliza y orienta sobre las obligaciones en materia de protección de datos personales y el ejercicio de derechos correspondientes.

VI. Principios que rigen el tratamiento de los datos personales

Los principios que rigen el tratamiento de los datos personales y que deberán observar todas las áreas universitarias involucradas en su protección son los siguientes:

- Licitud. El responsable deberá tratar los datos personales que posea sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los presentes Lineamientos generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.
- Finalidad. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas, en relación con las atribuciones expresas que la normatividad aplicable le confiera.
- Lealtad. No deberá obtenerse y tratarse datos personales, a través de medios engañosos o fraudulentos, el responsable privilegia los intereses del titular cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste, Por expectativa razonable de privacidad, la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en las disposiciones normativas aplicables.
- Consentimiento. Previo al tratamiento de los datos personales, el responsable deberá obtener el consentimiento del titular, de manera libre, específica e informada.
- Calidad. Los datos personales serán exactos, correctos, completos, y actualizados.
- Proporcionalidad. Los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo

PROTOCOLO METODOLÓGICO

con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable.

- Información. El responsable deberá informar a los titulares, a través del aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.
- Responsabilidad. El responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en las disposiciones normativas; así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares.
- Seguridad. Se deberán implementar medidas administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado.
- Confidencialidad. Las personas involucradas en el tratamiento de datos personales están obligadas a guardar confidencialidad respecto de estos, la cual subsistirá después de concluida la relación con la UNAM.

La observancia de estos principios constituye un deber permanente para las áreas universitarias y será considerada como criterio fundamental en el desarrollo del Programa Diagnóstico de cumplimiento en materia de protección de datos personales.

VII. Procedimiento

a) Proceso de selección de áreas sujetas al Programa Diagnóstico.

Las áreas universitarias que están sujetas al cumplimiento de las obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normativa aplicable en la materia, presentan diversas características en su composición organizacional, estructura orgánica, sistemas de tratamiento, volumen de datos y complejidad institucional.



PROTOCOLO METODOLÓGICO

La Universidad cuenta aproximadamente con 200 áreas universitarias¹ con características heterogéneas. Dichas áreas pueden agruparse en categorías según la propia legislación universitaria, a saber:

- Autoridades Universitarias;
- Cuerpos Colegiados;
- Dependencias Administrativas;
- Entidades Académicas;
- Tribunal Universitario; y
- Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género.

En ese sentido, es indispensable tomar en consideración las capacidades operativas del equipo revisor que llevará a cabo la ejecución del Programa Diagnóstico. Por ello, se deberá hacer un muestreo de áreas universitarias, respecto del cual se realizará la selección de áreas universitarias que serán revisadas conforme al presente Protocolo.

Aunado a lo anterior y considerando la variedad de áreas universitarias que pueden ser sujetas al Programa Diagnóstico, se establece una estrategia de implementación en etapas:

- **Primera etapa**

En la que se priorizará la revisión diagnóstica de entidades ubicadas en Ciudad Universitaria o zona metropolitana, lo cual permitiría optimizar tiempos y recursos.

- **Etapas subsecuentes**

En virtud de que el Programa Diagnóstico tiene por objeto realizar una revisión permanente del grado de cumplimiento en materia de protección de datos personales de todas las áreas universitarias, se deberá incorporar progresivamente otras entidades, incluidas entidades foráneas, según las capacidades operativas, de gestión y de ejecución del equipo revisor.

Esta estrategia permitiría reducir costos operativos, fortalecer la experiencia del equipo revisor y consolidar el Programa de manera gradual.

¹ Término definido por el Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, vigente.



PROTOCOLO METODOLÓGICO

Para obtener el muestreo de áreas universitarias, se podrá tomar en cuenta parámetros objetivos relacionados con el nivel de cumplimiento en materia archivística y de protección de datos personales relacionadas con supervisiones previas, entre ellos, los siguientes:

- Capacidad operativa institucional para la realización de los diagnósticos, considerando los recursos humanos disponibles, el tiempo requerido para la revisión de procesos y documentación, así como las actividades de análisis y elaboración de resultados.
- Ubicación geográfica de las áreas universitarias, particularmente en relación con aquellas que se encuentran fuera de Ciudad Universitaria, incluso fuera de la zona metropolitana, lo cual puede implicar mayores tiempos de traslado, coordinación logística y disponibilidad de recursos para la realización de las revisiones.
- Existencia de acciones archivísticas o procesos de regularización ya iniciados ya que algunas áreas universitarias podrían encontrarse en procesos de fortalecimiento de sus prácticas archivísticas, lo cual podría ser considerado al momento de establecer prioridades para la aplicación del Programa Diagnóstico.

De acuerdo con los parámetros antes descritos, una vez acotado el universo de áreas universitarias del cual se obtendrá la selección de las áreas a revisar, se deberá documentar el proceso utilizado para la selección de las mismas, debiendo utilizar criterios objetivos. En dicho proceso podrá utilizarse el apoyo de herramientas digitales confiables. Se determinará el número y nombre de áreas que serán sujetas a la revisión diagnóstico en la etapa que corresponda, y se asentará en un acta constancia para registro.

b) Preparación

La Autoridad Garante de la UNAM emitirá un oficio de invitación mediante el cual se informará al titular del área universitaria que será objeto del Diagnóstico de Cumplimiento.

- Fundamento normativo de la revisión.
- Presentación de las personas integrantes del equipo revisor.
- Descripción de las acciones que se realizarán durante la revisión.

PROTOCOLO METODOLÓGICO

- Solicitud de participación de las personas acompañantes responsables en materia de protección de datos personales, archivos, tecnologías de la información, o bien, de cualquier otra persona funcionaria que el titular del área universitaria considere pertinente.
- Convocatoria a una reunión preparatoria entre el equipo revisor y las personas acompañantes designadas.
- Solicitud al área universitaria que indique la fecha y horario en la que puede llevarse a cabo la reunión, conforme a las propuestas señaladas en el oficio de invitación. El área debe dar respuesta al oficio de invitación en un plazo de cinco días hábiles, señalando la fecha y hora en que desea celebrar la reunión preparatoria.
- Indicación de que la reunión se realizará de manera virtual en el medio que se determine.
- Definición de los medios de notificación que se utilizarán durante el procedimiento, privilegiando el uso del correo electrónico institucional.

c) Reunión preparatoria

Se llevará a cabo una reunión entre el equipo revisor y las personas acompañantes del área universitaria, o bien aquellas que el titular del área determine, con los siguientes objetivos:

- Exponer los antecedentes y generalidades del sistema de tratamiento de datos personales que será sometido a revisión.
- Establecer los alcances y objetivos del Diagnóstico de Cumplimiento.
- Precisar las obligaciones del área universitaria durante el desarrollo del procedimiento.
- Explicar las acciones que realizará el equipo revisor, así como la forma y criterios mediante los cuales se dará por concluida la revisión.

d) Emisión de minuta de la reunión preparatoria

Derivado de la reunión preparatoria, la Autoridad Garante de la UNAM elaborará una minuta, la cual deberá:

- Ser validada y firmada por las personas participantes.
- Notificarse al titular del área universitaria, para su conocimiento y efectos conducentes.

PROTOCOLO METODOLÓGICO

e) Desarrollo del Diagnóstico de Cumplimiento

Una vez celebrada la reunión preparatoria, la Autoridad Garante de la UNAM emitirá el *Acuerdo de inicio* del Diagnóstico de Cumplimiento, el cual deberá contener, al menos:

- La descripción del sistema de tratamiento de datos personales objeto de revisión, incluyendo:
 - ✓ Nombre del sistema de tratamiento.
 - ✓ Tipo de datos personales que se tratan.
 - ✓ Personas (administrativos de base, confianza, prestadores de servicios profesionales, becarios, prestadores de servicio social, funcionarios, entre otros) responsables del tratamiento de los datos personales.
 - ✓ Finalidad específica del tratamiento.
 - ✓ Flujo de los datos personales, desde su obtención, tratamiento, resguardo, archivo, conservación, eliminación o supresión.
 - ✓ Cualquier otra información que permita definir y comprender particularidades del sistema de tratamiento.
- La formalización de los alcances y objetivos establecidos en la reunión preparatoria.
- El inicio del cómputo del plazo del Diagnóstico de Cumplimiento.
 - La posibilidad de emitir requerimientos de información, realizar visitas a las instalaciones o llevar a cabo entrevistas con el personal involucrado.

La Autoridad Garante de la UNAM deberá emitir El *Acuerdo de inicio* en un plazo de máximo cinco días hábiles contados a partir de la celebración de la reunión preparatoria.

f) Notificaciones

La Autoridad Garante notificará los acuerdos del Diagnóstico de Cumplimiento al área universitaria en el medio señalado en el oficio de preparación, privilegiando el uso del correo electrónico institucional.

g) Etapa de revisión

Durante esta etapa, el equipo revisor llevará a cabo, de manera enunciativa más no limitativa, las siguientes acciones:

PROTOCOLO METODOLÓGICO

- Emisión de requerimientos de información mediante oficio, los cuales deberán ser atendidos por el área universitaria dentro de los plazos que se señalen, adjuntando la documentación correspondiente o poniéndola a disposición para su consulta.
- Aplicación de instrumentos de diagnóstico por parte del equipo revisor, en materia de archivos, de tecnologías de la información y aspectos administrativos.
- Realización de entrevistas con personas del funcionariado universitario estratégicas vinculadas con el sistema de tratamiento objeto de revisión, de manera presencial o virtual.
- Revisión física y/o lógica del sistema de tratamiento de datos personales en revisión.

h) Conclusión del Diagnóstico de Cumplimiento

Concluidas las actividades de revisión, la Autoridad Garante de la UNAM emitirá el *Acuerdo de conclusión* del Diagnóstico de Cumplimiento, el cual deberá contener, al menos, los siguientes elementos:

- Exposición de las acciones realizadas durante el procedimiento.
- Presentación de los resultados obtenidos.
- Análisis técnico de los riesgos identificados y de las brechas de seguridad en materia de protección de datos personales.
- Emisión de recomendaciones, orientadas a la prevención y mejora de los mecanismos de protección de datos personales.

El *Acuerdo de conclusión* tendrá carácter preventivo y orientador, y no constituirá, por sí mismo, un procedimiento de verificación ni dará lugar a la imposición de sanciones.

i) Plan de acción

Recibida la notificación del Acuerdo de Conclusión, el área universitaria contará con un plazo de quince días hábiles para informar a la Autoridad Garante de la UNAM, un plan de acción ante las recomendaciones realizadas; el cual deberá contener al menos lo siguiente:

- Acciones, actividades o medidas por implementar.
- El plazo en el que realizará dichas acciones que deberá ser validado por la Autoridad Garante de la UNAM.

PROTOCOLO METODOLÓGICO

j) Atención de recomendaciones

Dentro del plazo fijado por el área universitaria, deberá informar a la Autoridad Garante de la UNAM sobre las acciones implementadas en cumplimiento del *Acuerdo de conclusión* del Diagnóstico de Cumplimiento, adjuntando, en su caso, la documentación que acredite su atención.

La Autoridad Garante de la UNAM podrá dar seguimiento a la ejecución del plan de acción establecido por el área universitaria.

k) Emisión del Acuerdo de seguimiento

- Una vez atendidas las recomendaciones y el plan de acción, el equipo revisor emitirá el Acuerdo de seguimiento, mediante el cual se manifestará conformidad respecto de las acciones implementadas por el área universitaria, o bien se señalarán observaciones adicionales de carácter preventivo.
- Con la notificación del Acuerdo de seguimiento al área universitaria, se tendrá por concluida en su totalidad la revisión diagnóstica, sin perjuicio de que el área universitaria continúe fortaleciendo de manera permanente sus mecanismos de protección de datos personales.

VIII. Referencias para las actuaciones del equipo revisor

Las siguientes referencias orientan las actuaciones del equipo revisor durante el desarrollo del Diagnóstico de Cumplimiento, de acuerdo con el ámbito de competencia de cada instancia universitaria involucrada.

a) Autoridad Garante de la UNAM

En el ámbito normativo, administrativo y de cumplimiento, se revisarán los siguientes aspectos:

1. Titulares de los datos personales

- Identificación de los titulares: alumnado, personal universitario, personas externas.
- Identificación de datos de menores de edad o grupos en situación de vulnerabilidad.

PROTOCOLO METODOLÓGICO

2. Personal que da tratamiento a los datos personales

- Identificación de roles y perfiles.
- Número de personas con acceso a los datos personales.
- Revisión del perfil técnico y profesional.
- Evaluación del grado de conocimiento sobre el tratamiento adecuado de datos personales, medidas de seguridad y atención a incidentes de seguridad.

3. Documento de seguridad

- Verificación de su existencia.
- Identificación del sistema de tratamiento en revisión.
- Revisión de las secciones 3 "Análisis de riesgos", 4 "Análisis de brecha" y 5 "Plan de trabajo", del Anexo I "Documento de seguridad de datos personales", del documento normativo denominado: "Anexos de las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad".
- Revisión de su actualización.

4. Documentación de funciones y responsabilidades

- Verificación de la documentación que describe las funciones del personal.
- Revisión de la congruencia entre las funciones documentadas y la práctica real.

5. Avisos de privacidad

- Fecha de elaboración y actualización.
- Ubicación física y electrónica.
- Momento en que se pone a disposición de las personas.
- Verificación del cumplimiento de los elementos normativos.
- Identificación de si se cuenta con avisos específicos o generales por sistema, finalidad o tipo de titular.

6. Datos personales sensibles

- Identificación de su tratamiento.
- Verificación de la implementación de medidas de seguridad adicionales.

7. Confidencialidad

- Verificación de la firma de cartas de confidencialidad por parte del personal que trata datos personales.

PROTOCOLO METODOLÓGICO

8. Incidentes de seguridad y vulneraciones

- Revisión del procedimiento para la atención de incidentes y vulneraciones de seguridad.

9. Política y programas

- Verificación de la existencia de políticas o programas institucionales en materia de protección de datos personales.

10. Capacitación

- Identificación de la capacitación impartida:
 - externa o interna.
 - constancias o lista de asistencia.
 - fechas.
- Revisión de la difusión interna sobre el correcto tratamiento de datos personales.
- Identificación de capacitación pendiente.

11. Transparencia y acceso a la información

- Determinar si la información forma parte de obligaciones de transparencia o ha sido objeto de solicitudes de acceso a información o de datos personales
- Verificación de:
 - información pública
 - versiones públicas o íntegras
 - fundamento de su clasificación.

12. Ejercicio de derechos ARCO

- Descripción de los procesos de acceso, rectificación, cancelación y borrado de los datos.

13. Presupuesto

- Revisión del presupuesto destinado a la seguridad del sistema de tratamiento de datos personales.

b) Dirección General de Cómputo y de Tecnologías de Información y Comunicación

1. Descripción del Inventario de Sistemas de Tratamiento de Datos Personales.

Considerar el numeral 1, del Anexo I: Documento de Seguridad de Datos Personales, del documento normativo denominado: "Anexos de las normas complementarias

PROTOCOLO METODOLÓGICO

sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad".

2. Medidas de seguridad

Considerar la sección del Anexo V del Formato de cumplimiento de las Medidas de Seguridad Técnicas" del documento normativo denominado: "Anexos de las normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad".

3. Incidentes de seguridad

¿Los componentes informáticos que soportan los sistemas de tratamiento de Datos Personales, han sufrido algún evento que afecten su confidencialidad, integridad y disponibilidad?

4. Entrevista

- Entrevista con la persona responsable de seguridad de los datos personales, a efecto de verificar que conozca y cumpla con las responsabilidades a su cargo.

c) Área Coordinadora de Archivos de la UNAM

El equipo revisor evaluará las condiciones físicas, archivísticas y de conservación del sistema de tratamiento de datos personales, considerando el ciclo de vida documental, la normativa aplicable en materia de archivos y los principios de protección de datos personales.

1. Espacios físicos

- Identificación y descripción de las oficinas donde se realiza el tratamiento de datos personales.
- Verificación de la existencia y condiciones de los espacios destinados al resguardo documental.
- Revisión de archiveros, cajas, estantería y mobiliario, valorando su idoneidad para la conservación de documentos.
- Evaluación de puertas, cerraduras, controles de acceso y uso de llaves, a fin de verificar que existan mecanismos que limiten el acceso no autorizado.

2. Soporte y estado de los datos personales

- Identificación del soporte documental en el que se encuentran los datos personales: papel, digital, electrónico, sistemas automatizados u otros.
- Verificación de que los documentos que contienen datos personales se encuentren completos, legibles y en condiciones adecuadas de conservación física y lógica.

PROTOCOLO METODOLÓGICO

- Identificación de riesgos de deterioro, pérdida de información o daño documental derivado de humedad, plagas, exposición a luz, manipulación inadecuada o fallas tecnológicas.

3. Resguardo físico y control archivístico

- Identificación de las personas autorizadas para acceder a los documentos que contienen datos personales.
- Revisión del control y resguardo de llaves, así como de otros mecanismos de seguridad física.
- Verificación de la aplicación de la política de mesas limpias y de prácticas que eviten la exposición innecesaria de documentos.
- Evaluación del mobiliario y de la suficiencia de los espacios para el adecuado resguardo documental, conforme a los volúmenes y características del acervo.

4. Expedientes y control documental

- Verificación de que los datos personales se encuentren debidamente integrados en expedientes, conforme a la estructura documental establecida.
- Revisión del contenido de los expedientes para comprobar:
 - integridad documental,
 - orden lógico,
 - correspondencia con las funciones y atribuciones del área universitaria.
- Identificación y revisión de los procedimientos de préstamo y consulta, verificando que existan registros, controles y plazos definidos.
- Análisis de casos de documentos o expedientes extraviados, dañados o destruidos, así como de las acciones emprendidas para su localización, recuperación o reposición.
- Identificación de supuestos de archivo siniestrado, entendidos como aquellos documentos afectados por incendios, inundaciones, sismos, fallas estructurales u otros eventos que comprometan su integridad, así como la existencia de medidas de contingencia, recuperación o documentación del siniestro.

5. Instrumentos de control y consulta archivísticos

- Verificación de que el tratamiento de datos personales se realice conforme a los instrumentos de control y consulta archivísticos institucionales, vigentes y autorizados.
- Revisión del cumplimiento del ciclo de vida documental en:



PROTOCOLO METODOLÓGICO

- ✓ Oficina Central de Correspondencia.
- ✓ Archivo de Trámite.
- ✓ Archivo de Concentración.
- ✓ Archivo Histórico.
- Evaluación de la congruencia entre los instrumentos archivísticos y la práctica real de organización, conservación y acceso a los documentos.

6. Destino final de los documentos

- Revisión de los procesos de transferencia documental, conservación permanente o baja documental de los documentos que contienen datos personales.
- Verificación de que el destino final se realice conforme a los dictámenes, plazos de conservación y procedimientos autorizados.
- Identificación de riesgos asociados a la eliminación indebida, conservación excesiva o falta de documentación de las decisiones sobre el destino final.

7. Entrevistas y personal responsable en materia de archivos

- Entrevista con la persona responsable de archivos y los responsables de archivo de trámite, concentración e histórico del área universitaria para verificar que conozca el marco normativo aplicable; identifique sus responsabilidades y participe activamente en el tratamiento de datos personales.
- Revisión de la labor de las personas que realiza tareas archivísticas, a fin de verificar conocimiento en sus funciones, cumplimiento de procedimientos establecidos y participación en acciones de capacitación en materia de archivos y protección de datos personales.



IX. Anexos

- Instrumentos de valoración.
- Listas de comprobación del equipo revisor.
- Formato Excell análisis de riesgo.
- Formato Excell análisis de brecha.
- Anexos I, IV y V de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad:
 - Anexo I. Documento de Seguridad de Datos Personales (Inventario).
 - Anexo IV. Ruta Crítica para Cumplimiento de las Medidas de Seguridad Técnicas (MST).
 - Anexo V. Formatos Para Cumplimiento de las Medidas de Seguridad Técnicas (MST).

Archivo

ProgramaDiagnóstico_ProtocoloMetodológico.pdf

Identificador único (hash)

ae1624e75adf5d659644d116e363e686ca73d0862919017fb0426ed19197b1ae

Fecha y hora de cierre

27/04/2026 21:07:51

Fecha y hora de emisión

27/04/2026 21:12:13

Número de páginas

25

Firmantes

6



Firmantes

Nombre	Mtra. Elizabeth Rangel Gutiérrez	Fecha y hora de firma	24/04/2026 12:00:48
Representante DGTIC			
Hash Firma	5ed33537465ccaa7e5e0e1070ac9a911cac1466a1615779a1d3eb9b397620347c8ef691afb786c08b26bbc5c3410c9ba		

Nombre	Dr. Héctor Benítez Pérez	Fecha y hora de firma	27/04/2026 21:07:51
Titular DGTIC			
Hash Firma	18467d7892da50ebb6c51e400985bdf675dfd653b564cd11ed8dab527271e666d9327a0a06c2d9faf871674240c09245		

Nombre	Lic. Celia Escobar Juárez	Fecha y hora de firma	27/04/2026 17:35:59
Representante ACA			
Hash Firma	8354ef91cb3b0b8abc46f01af377b7277a27a650d1ed7eac32bec022603c3e1b63bf91a23eb0c7e20536c4e2f6f80962		

Nombre	Mtro. Porfirio Antonio Díaz Rodríguez	Fecha y hora de firma	27/04/2026 17:44:49
Titular ACA			
Hash Firma	c8cf2af56613bd812eedc0955f3d094181c35e2f15c9eaaecf21515c4da6f8219b9c7fc1c9cc1c989aa6b7bc0e4460f5		

Nombre	Mtra. Mariana Vázquez Bracho García	Fecha y hora de firma	24/04/2026 12:05:41
Representante AGA			
Hash Firma	76bdf3974cb7b76b193658d719f3f63d704a94ffdf57d771b647f76031046aa42788df8abd5cc8d41f069c678bfb32b		

Nombre	Dra. María Marván Laborde	Fecha y hora de firma	24/04/2026 12:01:26
Titular AGA			
Hash Firma	e44f232d5f63b7828d5e92c570cc614d81180e68ea39b1382748f565546b665ed6ced1a60f71adc533e4e6a7c26a6ea4		