COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/476/2026

FOLIO: 410031900248326

Visto el expediente relativo a la clasificación de reserva parcial de la información para la elaboración de la versión pública determinada por el **Instituto de Biotecnología**, por la **Coordinación de Universidad Abierta y Educación Digital,** por la **Secretaría General de la UNAM**, por el **Instituto de Neurobiología**, por la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"** , por la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional**, por la **Dirección General de Asuntos del Personal Académico**, por la **Escuela Nacional de Estudios Superiores Unidad Morelia**, por el **Centro de Física Aplicada y Tecnología Avanzada**, así como por la **Dirección General de Artes Visuales**, en relación con la solicitud de acceso a la información con número de folio **410031900248326**, se procede a dictar la presente resolución con base en los siguientes:

A N T E C E D E N T E S

I. Con fecha 10 de septiembre de 2026, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia, se recibió la solicitud de acceso a la información con número de folio **410031900248326**, en la que la persona solicitante requirió lo siguiente:

> *"Solicito todos los documentos de seguridad de datos personales obligatorios por ley, previa reserva de la información. Lo solicito de todas las áreas universitarias, para que no acoten las áreas, aquí las desgloso: 1. Entidades Académicas Educación Superior: 16 Facultades (en Ciudad Universitaria y áreas metropolitanas). 10 Unidades Multidisciplinarias (5 FES: Acatlán, Aragón, Cuautitlán, Iztacala, Zaragoza; más sedes/unidades asociadas). 9 Escuelas Nacionales (incluyendo ENES Juriquilla, León, Mérida, Morelia, ENAC, ENCiT, ENCiF, ENALLT y ENTS). Bachillerato: 9 planteles de la Escuela Nacional Preparatoria (ENP). 5 planteles del Colegio de Ciencias y Humanidades (CCH). Subsistema de Investigación: 36 Institutos de investigación (25 en Ciencias y 11 en Humanidades). 13 Centros de investigación (6 en Ciencias y 7 en Humanidades). 14 Programas Universitarios multidisciplinarios. Unidades académicas y de extensión regional (Morelos, Querétaro, Yucatán, Michoacán, Chiapas, etc.). 2. Dependencias Administrativas y Centrales Rectoría, Oficinas Centrales y Abogacía General. Secretarías Generales y de Apoyo: Secretaría General. Secretaría Administrativa. Secretaría de Desarrollo Institucional. Secretaría de Prevención y Apoyo a la Movilidad y Seguridad Universitaria. Secretaría de Servicio y Atención a la Comunidad Universitaria. Direcciones Generales y Coordinaciones: Más de 50 direcciones generales y coordinaciones (DGAE, DGAPA, DGCS, DGTIC, DGPe, DGPO, Deporte Universitario, Difusión Cultural con sus distintas direcciones de Danza, Música, Teatro, Artes Visuales, TV UNAM, Radio UNAM, etc.). Sedes de la UNAM en el Extranjero: 12 sedes internacionales (Centros de Estudios Mexicanos / UNAM Boston, Canadá, China, España, Francia, Alemania, UK, etc.). Servicios e Instalaciones Nacionales: Servicio Sismológico Nacional (SSN), Observatorio Astronómico Nacional (OAN), Jardín Botánico, Biblioteca y Hemeroteca Nacionales, Red Mareográfica, entre otros. Resumen La cifra aproximada a la que haces referencia (~220 a 230 unidades operativas / centros de adscripción) corresponde a la suma consolidada de todas las unidades con clave presupuestal y estructura orgánica propia (entidades académicas, planteles*

foráneos y dependencias centrales) registradas en el catálogo institucional y presupuestal de la UNAM" (sic).

II. En la solicitud de acceso a la información se estableció como modalidad de entrega de la información por medio electrónico, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia.

III. En cumplimiento a lo dispuesto en el punto Segundo, fracción II del Acuerdo por el que se constituyen la Unidad de Transparencia y el Comité de Transparencia de la Universidad Nacional Autónoma de México, mediante correos electrónicos de fecha 14 de septiembre de 2026, la Unidad de Transparencia remitió la solicitud de acceso a la información con número de folio **410031900248326,** entre otras áreas universitarias, al **Instituto de Biotecnología,** a la **Coordinación de Universidad Abierta y Educación Digital**, a la **Secretaría General de la UNAM**, al **Instituto de Neurobiología,** a la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, a la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** a la **Dirección General de Asuntos del Personal Académico,** a la **Escuela Nacional de Estudios Superiores Unidad Morelia,** al **Centro de Física Aplicada y Tecnología Avanzada**, así como a la **Dirección General de Artes Visuales**.

IV. A través de correo electrónico**,** recibido con fecha 14 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Unidad de Transparencia** solicitó la ampliación de plazo para dar respuesta.

Derivado de lo anterior, con fecha 18 de septiembre de 2026 y con fundamento en los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 134, segundo párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 1, 11, 15, fracción X y 58, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, se amplió el plazo para emitir la respuesta a la solicitud por 10 días más, contados a partir del día hábil siguiente a su vencimiento.

V. Mediante oficio **IBIT/D/450/2026**, recibido con fecha 18 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Biotecnología** señaló lo siguiente:

"El documento de seguridad es el instrumento que describe y da cuenta de manera general de 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 un área universitaria, cuya versión se integra por siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); así como en los numerales 112, fracción VII en relación con el 103, fracción 1, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad

técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados, cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	***36-51***
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	***53-64***
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el*	***65-73***

	momento en que se implementen nuevos controles.	
d) *Acceso a las instalaciones*	*Describe los protocolos de seguridad física, los controles de ingreso, los mecanismos de identificación y las áreas restringidas donde se resguardan los soportes de datos personales. Su divulgación expone las vulnerabilidades de los accesos físicos, facilitando intrusiones no autorizadas o la sustracción de documentos e infraestructura crítica.*	***81***

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real, demostrable e identificable respecto del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, pues la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo y acceso a las instalaciones de esta dependencia contiene información sobre la forma en que de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, podría hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, información que esta serie de documentos les otorga directamente si se difundiera la información.

• Divulgar el análisis de riesgo, el análisis de brecha, el plan de trabajo y los controles de acceso a las instalaciones evidencia los nuevos controles que estamos pendientes de implementar, describen la forma en que almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y los presupuestos otorgado.

• En este sentido la revelación de la información que obra en el análisis de riesgos, el análisis de brecha, el plan de trabajo y los controles de acceso de esta área revela y hace identificables las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales

que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgos, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y de tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como acceso no autorizado a los sistemas, el robo de información, la suplantación de identidad, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión de delitos al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgos, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas implementadas caduquen o bien se implementen otras diversas. De igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquier persona que deposite su confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para realizar alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic)

VI. Por oficio **CUAED/UJ/ADLRG/311/2026**, recibido con fecha 23 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Universidad Abierta y Educación Digital** refirió lo siguiente:

> *"El documento de seguridad es el instrumento que describe y da cuenta de manera general de 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 un área universitaria, cuya versión se integra por siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); así como en los numerales 112, fracción VII en relación con el 103, fracción 1, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.*
>
> *A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados, cuya autorización de reserva total se solicita a ese Comité:*

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a. *Estructura y descripción de los sistemas de tratamientos de datos personales*	*Las características del lugar donde se resguardan los soportes identifican el espacio físico, virtual y los controles de acceso para las fuentes de información de cada sistema informático*	***239***
b. *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	
c. *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de*	

	la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
d. *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	
e. *Acceso a las instalaciones*	*El acceso a las instalaciones permite identificar los caminos, físicos, horarios, o áreas de la CUAED por las cuáles se podría vulnerar la seguridad en la dependencia.*	
f. *Mecanismos de Monitoreo y Revisión de las medidas de seguridad*	*Todos los mecanismos de monitoreo y revisión de las medidas de seguridad implementadas permiten identificar lo que se ha realizado y los resultados de estas acciones, lo que permite realizar ingeniería inversa para identificar brechas o riesgos y poder explotarlos.*	

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real, demostrable e identificable respecto del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, pues la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta dependencia contiene información sobre la forma en que de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, podría hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, información que esta serie de documentos les otorga directamente si se difundiera la información.

• Divulgar la estructura y descripción de los sistemas de tratamientos de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta dependencia evidencian los trayectos y áreas físicas vulnerables, los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, los controles y claves de acceso al centro de datos, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

• En este sentido la revelación de la información que obra estructura y descripción de los sistemas de tratamientos de datos personales, análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta dependencia revela y hace identificable las formas en que es posible atacar o vulnerar física o lógicamente nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta dependencia para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer la estructura y descripción de los sistemas de tratamientos de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es

posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos a la estructura y descripción de los sistemas de tratamientos de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, acceso a las instalaciones y mecanismos de monitoreo y revisión de las medidas de seguridad de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic)

VII. Mediante el oficio **SGEN/ET/015/2026**, recibido con fecha 24 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Secretaría General de la UNAM** informó lo siguiente:

"El documento de seguridad es el 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 un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII

en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Secretaría de mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*48 a 50*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*54 a 57*
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros*	*59 a 73*

	riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.	

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real. demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha y el plan de trabajo de esta Secretaría contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria.

• Divulgar el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta Secretaría evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

• En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta Secretaría revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta Secretaría, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no

autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Secretaría, con relación al cumplimiento de los principios de protección de datos personales previsto en la LGPDPPSO.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta Secretaría se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquier persona que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta Secretaría, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic).

VIII. Por oficio **INEU/D/598/2026**, recibido con fecha 28 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Neurobiología** informó lo siguiente:

"El documento de seguridad es el 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 un área universitaria; cuyo contenido comprende diversos elementos o apartados, de los cuales al menos tres se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados1 (LGPDPPSO) y 112, fracción Vll2 en relación con el 103, fracción 13, de la Ley General de Transparencia y Acceso a la Información Pública4 (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales del Instituto de Neurobiología (INB). El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a. Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica del INB, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos v no críticos.*	*36-41*
b. Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información. Es decir, detalla diferencias entre los controles existentes y los requeridos; identifica deficiencias administrativas, físicas y técnicas, así como necesidades de fortalecimiento, herramientas y controles pendientes de implementar.*	*42-46*
c. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha,*	*46-51*

	priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.	
d. Inventario de Sistemas de Tratamiento de Datos Personales	*En el inventario de sistemas de tratamiento de datos personales se identifican sistemas físicos y electrónicos, áreas responsables, tipos de datos, medios de almacenamiento, transferencias y niveles de riesgo. Su divulgación permitiría ubicar activos, sistemas prioritarios y puntos de exposición institucional.*	*32-36*

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General. La información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB describe cómo se protegen los datos personales que los titulares han confiado al Instituto y cuya seguridad es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.
• Divulgar el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB evidencia los nuevos controles pendientes de implementar, describen la forma en que almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y recursos presupuestales otorgados.
• En este sentido, la revelación de la información que obra en el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de

tratamiento de datos personales del INB revela y hace identificable la forma en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y limitaría la capacidad de esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica del INB; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, el análisis de brecha, el plan de trabajo y el inventario de sistemas de tratamiento de datos personales del INB se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de cinco años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se ha previsto para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito atentamente que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa." (sic).

IX. A través del oficio **ENP-1/D/289/2026**, recibido con fecha 29 de septiembre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"** notificó lo siguiente:

"Por medio del presente y derivado de la Solicitud de Información con folio 410031900248326 enviada a esta Escuela Nacional Preparatoria Plantel 1 'Gabino Barreda', me permito enviar el documento de seguridad el cual es el 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 un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los dalos personales que resguarda esta institución.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	***62-65***
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlista los controles de seguridad*	***65-67***

	con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
***c)** Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	***67-68***

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

• Divulgar el análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

• En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic).

X. Mediante oficios **CPESGI/0453/2026, DGAP/DG/DSDIA/1710/2026**, **CFAT/D/285/2026** y **DGAV/D/3074/2026**, recibidos con fechas 29 y 30 de septiembre, así como 6 de octubre de 2026, dirigidos a la Presidencia del Comité de Transparencia, la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional**, la **Dirección General de Asuntos del Personal Académico**, el **Centro de Física Aplicada y Tecnología Avanzada**, así como la **Dirección General de Artes Visuales** informaron lo siguiente:

"El documento de seguridad es el 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 un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública4 (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
… *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*…*
… *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura*	*…*

	tecnológica; enlista los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
***…** Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	*…*

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

• Divulgar el análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

• En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa" (sic).

XI. Por oficio **ENESM/ST/TRANS/023/2026**, recibido con fecha 2 de octubre de 2026, dirigido a la Presidencia del Comité de Transparencia, la **Escuela Nacional de Estudios Superiores Unidad Morelia** notificó lo siguiente:

"El documento de seguridad es el 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 un área universitaria; cuya versión se integra de siete elementos o apartados, de los cuales, por lo menos tres, se ajustan al supuesto de reserva contemplado en los artículos 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y 112, fracción VII en relación con el 103, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnicas, administrativas y físicas de los datos personales que resguarda esta institución.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*12, 38, 68, 95, 117, 140, 164, 189, 214, 237, 271, 300, 326*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las*	*13, 39, 69, 95, 118, 142, 165, 190, 215,*

	herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.	
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	*14, 40, 70, 96, 118, 142, 166, 191, 216, 240, 274, 303, 330.*
d) *Características del lugar donde se resguardan los soportes.*	*El apartado de Características del lugar donde se resguardan los soportes de cada sistema contiene información relativa a la seguridad de la infraestructura tecnológica y los controles de seguridad con los que cuenta esta área.*	*11, 37, 67, 94, 117, 140, 164, 188, 214, 236, 270, 300, 326.*

Los fundamentos y motivos se exponen a continuación:

• Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en el artículo 112, fracción VII, de la Ley General, la información contenida en los apartados relativos al análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.

• Divulgar el análisis de riesgo, el análisis de brecha, y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

• En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.

La prueba de daño precitada, colma los extremos establecidos en las tres fracciones del artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública; dado que podrá considerarse como información reservada aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de estas para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, afectaría la prevención de actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al no revelar las vulnerabilidades de las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad y se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen, o bien, se implementen otras diversas; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de la comunidad universitaria, así como de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

> *Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos apartados del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con el segundo párrafo del artículo 104 de la Ley General, plazo considerado como necesario para la adecuada salvaguarda de la información aludida, atendiendo a que es el lapso promedio que se tiene contemplado para alguna modificación sustancial o actualización del Documento de Seguridad en cita.*
>
> *En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda, para lo cual se adjunta la documentación completa."* (sic).

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

C O N S I D E R A C I O N E S

PRIMERA. De acuerdo con lo dispuesto por los artículos 1, 11 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la **clasificación de reserva parcial de la información para la elaboración de la versión pública** determinada por el **Instituto de Biotecnología,** la **Coordinación de Universidad Abierta y Educación Digital,** la **Secretaría General de la UNAM**, el **Instituto de Neurobiología,** la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda**, la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** la **Dirección General de Asuntos del Personal Académico,** la **Escuela Nacional de Estudios Superiores Unidad Morelia,** el **Centro de Física Aplicada y Tecnología Avanzada,** así como la **Dirección General de Artes Visuales** para atender la solicitud de acceso a la información con número de folio **410031900248326** y determinar, en consecuencia, si la confirma, modifica o revoca.

SEGUNDA. En términos de lo previsto en los artículos 102, tercer párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 33, 34, fracción I y 56, fracción II, inciso b) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, dicha determinación.

TERCERA. Las áreas universitarias clasificaron como reservada, por un periodo de **cinco años**, parte de la información contenida en su Documento de Seguridad correspondiente a los apartados relativos **al análisis de riesgo, al análisis de brecha, al plan de trabajo**, así como **diversa información relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales que obran en sus archivos**, conforme a lo expuesto en los antecedentes V, VI, VII, VIII, IX, X y XI de la presente resolución, por actualizarse el supuesto establecido en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Ahora bien, en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, se prevé lo siguiente:

> *"Como información reservada podrá clasificarse aquella cuya publicación:*
> *…*
>
> ***VII.** Pueda causar daño u obstruya la prevención … de los delitos;*
>
> *…".*

Conforme a lo anterior, la clasificación de reserva se debe asignar a aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Inicialmente, cabe tener en consideración lo establecido en el documento de trabajo del 12º. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: "*La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad…*".

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

Desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

También, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981**,** publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter

personal registrados en ficheros automatizados, contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 24, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

Además, de conformidad con el artículo 27, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual es recomendable observar, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan resguardarlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrán pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

En ese sentido, el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece que los sujetos obligados deben elaborar un Documento de Seguridad, entendiéndose como tal, el 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; mismo que deberá contener, cuando menos:

1. El inventario de datos personales y de los sistemas de tratamiento.

2. Las funciones y obligaciones de las personas que traten datos personales.
3. El análisis de riesgo.
4. El análisis de brecha.
5. El plan de trabajo.
6. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
7. El programa general de capacitación.

Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad, en términos del artículo 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal orden de ideas, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales de las Áreas Universitarias, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Además de lo anterior, de conformidad con el artículo 19, fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

Por ende, de difundirse la información contenida en los apartados relativos al **análisis de riesgo**, al **análisis de brecha** y al **plan de trabajo**; así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y, derivado de ello, ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **análisis de riesgo**, el **análisis de brecha**, el **plan de trabajo**; así como de **toda aquella información que se encuentre directamente relacionada con alguno de dichos**

apartados o que **revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias**, tiene como propósito evitar o prevenir la comisión de conductas delictivas, tales como el acceso ilícito a equipos y sistemas de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

> *"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa".*
>
> *"Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *…".*

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, **sean o no propiedad del Estado**, o bien, conozca o copie dicha información; conductas que de igual manera se pueden materializar en los archivos físicos, ya que es factible **sustraer, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, los datos personales contenidos en los documentos bajo custodia de las áreas universitarias**, por lo que la misma protección deberá otorgarse tanto a los sistemas electrónicos, como a los archivos físicos con los que se cuenta.

Por lo que de darse a conocer la información objeto de reserva se expondrían las acciones implementadas o por implementar, anticipando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las áreas universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar la información personal que obra en sus archivos, revelando elementos que, de manera concatenada con otra

información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica de las áreas universitarias, ya que la información relativa a las medidas físicas, administrativas y técnicas puede ser utilizada para propiciar, entre otros, actos vandálicos, o bien, ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a los documentos físicos y/o electrónicos que obran en los archivos, así como a la infraestructura informática, programas y desarrollos tecnológicos de las áreas universitarias, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, tales como las relacionadas en párrafos anteriores.

En este orden de ideas, la información analizada actualiza la causal de reserva prevista en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

Consecuentemente, en términos del artículo 107 de la Ley General citada, se analiza la siguiente prueba de daño:

> *"Artículo 107. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio"*

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

Difundir la información relativa al **análisis de riesgo**, el **análisis de brecha**, el **plan de trabajo,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias**, representa un riesgo potencial, pues dichos apartados contienen elementos informativos a partir de los cuales se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole en contra de los sistemas de tratamiento de datos personales y la información contenida en ellos, disminuyendo la capacidad de las áreas universitarias para prevenir y/o contrarrestar posibles amenazas.

En ese sentido la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

Al verse limitada la capacidad de las áreas universitarias para prevenir y/o contrarrestar conductas que amenacen los sistemas de tratamiento de datos personales y/o su contenido, se expone a los integrantes de la comunidad universitaria, integrada por personal administrativo, académico y el estudiantado, así como a las diversas personas que proporcionan sus datos personales a las distintas entidades académicas y/o dependencias administrativas con motivo del desarrollo de las actividades que tienen encomendadas, a la comisión de diversos actos ilícitos tales como la sustracción, el ocultamiento, la alteración, mutilación, destrucción o inutilización de sus datos personales, la suplantación de identidad, extorsiones u otras conductas delictivas relacionadas con la explotación de dichos elementos informativos.

De ahí, resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información objeto de reserva, supera el interés público general de que se difunda.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

La limitación se ajusta al principio de proporcionalidad, toda vez que se justifica no difundir la información en cuestión, a cambio de garantizar la capacidad de las áreas universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan con motivo del desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, la limitación representa el medio menos restrictivo disponible para evitar el perjuicio, ya que únicamente se restringirá el acceso a la información, por un periodo de **cinco años,** que se computará a partir del **9 de octubre de 2026** y fenecerá el **9 de octubre de 2031**, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero.

Periodo que se estima pertinente, toda vez que durante el mismo podría tener lugar alguna modificación sustancial o una actualización del Documento de Seguridad de las áreas universitarias.

Ahora bien, por cuanto hace a la información que se encuentre directamente relacionada con los apartados de análisis de riesgo, análisis de brecha, y plan de trabajo o que revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias, resulta procedente únicamente el resguardo de aquellos elementos informativos cuya divulgación ponga en riesgo los sistemas de tratamiento de datos personales o su contenido, pues de la revisión a las versiones públicas remitidas por las áreas universitaria se observa que en diversos apartados

como lo son: la estructura y la descripción de los sistemas de tratamientos de datos personales; acceso a las instalaciones; el inventario de sistemas de tratamiento de datos personales; las características del lugar donde se resguardan los soportes; las finalidades del tratamiento; el nombre de usuarios; los mecanismos de monitoreo y revisión de las medidas de seguridad, se protege información de carácter genérico que no representa una amenaza a tales sistemas ni a la información almacenada en ellos, por lo que se deberá verificar dicha circunstancia previo a realizar el testado correspondiente.

Consecuentemente, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública, siendo procedente **CONFIRMAR** la clasificación de reserva parcial de la información para la elaboración de la versión pública determinada por el **Instituto de Biotecnología,** por la **Coordinación de Universidad Abierta y Educación Digital,** por la **Secretaría General de la UNAM**, por el **Instituto de Neurobiología,** por la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, por la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** por la **Dirección General de Asuntos del Personal Académico**, por la **Escuela Nacional de Estudios Superiores Unidad Morelia,** por el **Centro de Física Aplicada y Tecnología Avanzada**, así como por la **Dirección General de Artes Visuales**, por un periodo de **cinco años**, mismo que fenecerá el **9 de octubre del 2031**, de conformidad con lo establecido en el artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

CUARTA. En relación con el contenido del Documento de Seguridad y la versión pública correspondiente, **las áreas universitarias deberán**:

1. Verificar que su Documento de Seguridad cuenta con los apartados previstos en el artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, además de que cumpla con la información y características establecidas en el "Anexo I. Documento de Seguridad de Datos Personales" de los "Anexos de las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad", aprobados por este Cuerpo Colegiado mediante Acuerdo de fecha 10 de enero de 2020.

2. Revisar que la información correspondiente a los apartados de "Análisis de Riesgos", de "Análisis de Brecha", de "Plan de Trabajo" del Documento de Seguridad, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las áreas universitarias sea debidamente testada, a efecto de evitar posibles vulneraciones; para tal efecto, deberán emplear un medio de testado que no permita la visualización y/o recuperación de la información objeto de reserva, pero que no impida la lectura del resto del contenido.

3. Corroborar que la información diversa a los apartados de análisis de riesgo, análisis de brecha, así como al plan de trabajo, cuyo resguardo plantean en la versión pública de su Documento de Seguridad, corresponda a **elementos informativos que efectivamente constituyan un riesgo** para los sistemas de tratamiento de datos personales y/o para su

contenido, **sin que sea dable proteger información como**: **descripciones genéricas** de los accesos a las instalaciones, de los métodos empleados para autorizar los accesos (bitácoras, identificaciones, control biométrico), de los lugares o soportes en que se almacenan los datos personales, o bien, de los mecanismos de monitoreo implementados; el **inventario y la descripción** de los sistemas referidos en el mismo; las **finalidades** del tratamiento de los datos personales; las **categorías** de los datos personales recabados; el nombre de las personas responsables, encargadas y/o usuarias de dichos sistemas, entre otra diversa, que **no actualiza el supuesto de reserva invocado**, al no corresponder a datos que comprometan las medidas de seguridad físicas, administrativas y/o técnicas implementadas para proteger los sistemas en cuestión.

4. Insertar un cuadro de texto en las hojas de la versión pública en las cuales protejan información, a fin de indicar:

a) Las partes o secciones reservadas.
b) El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

Por lo expuesto, y de acuerdo con los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 24, 40, fracción II, 112, fracción VII, así como 139, fracción I de la Ley General de Transparencia y Acceso a la Información Pública; 1, 15, fracción X y 37 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto por los artículos 1 y 15 fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México; así como 139, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** parcial de la información para la elaboración de la versión pública determinada por el **Instituto de Biotecnología**, por la **Coordinación de Universidad Abierta y Educación Digital**, por la **Secretaría General de la UNAM**, por el **Instituto de Neurobiología,** por la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, por la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** por la **Dirección General de Asuntos del Personal Académico,** por la **Escuela Nacional de Estudios Superiores Unidad Morelia,** por el **Centro de Física Aplicada y Tecnología Avanzada,** así como por la **Dirección General de Artes Visuales** por un periodo de **cinco años,** mismo que se computará a partir del **9 de octubre de 2026** y fenecerá el **9 de octubre de 2031,** para atender la solicitud de acceso a la información con número de folio **410031900248326.**

Lo anterior, en términos de la consideración **TERCERA** de la presente resolución.

SEGUNDO. Se **instruye** a las áreas universitarias a fin de que atiendan las indicaciones enumeradas en la consideración **CUARTA** de esta resolución.

TERCERO. Se instruye a las áreas universitarias para que, **dentro de los tres días hábiles siguientes a la notificación de la presente resolución**, remitan a la Unidad de Transparencia la versión pública para su entrega a la persona solicitante, conforme a la modalidad elegida para ello.

Lo anterior, de acuerdo con los artículos 120 y 136, segundo párrafo de la Ley General de Transparencia y Acceso a la Información Pública.

CUARTO. La persona solicitante podrá interponer el recurso de revisión previsto en los artículos 144 y 145 de la Ley General de Transparencia y Acceso a la Información Pública, así como 67 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, a través de la Plataforma Nacional de Transparencia o ante la Unidad de Transparencia de la Universidad Nacional Autónoma de México, dentro de los quince días siguientes a la fecha de la notificación de la respuesta o del vencimiento del plazo para su notificación.

QUINTO. Con fundamento en los artículos 41, fracción V y 139, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública; 21, fracción V y 58, fracción II, tercer párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo electrónico institucional al **Instituto de Biotecnología,** a la **Coordinación de Universidad Abierta y Educación Digital,** a la **Secretaría General de la UNAM**, al **Instituto de Neurobiología**, a la **Escuela Nacional Preparatoria Plantel 1 "Gabino Barreda"**, a la **Coordinación de Planeación, Evaluación y Simplificación de la Gestión Institucional,** a la **Dirección General de Asuntos del Personal Académico**, a la **Escuela Nacional de Estudios Superiores Unidad Morelia,** al **Centro de Física Aplicada y Tecnología Avanzada,** a la **Dirección General de Artes Visuales,** así como a la Unidad de Transparencia de esta Universidad, para que por conducto de esta última sea notificada a la persona solicitante, para los efectos procedentes.

Así lo resolvió en su Trigésima Sexta Sesión, por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 19 y 58, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

"POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., a 9 de octubre de 2026

Sistema de Firma de Documentos de Cuerpos Colegiados

Representación gráfica del acto de firma.

1 INFORMACIÓN DEL DOCUMENTO FIRMADO

Datos generales e identificadores del documento firmado.

Nombre del archivo
08-ctunam-476-2026-248326.pdf

Fecha y hora de solicitud de firma
09/10/2026 17:06:31

Fecha y hora de cierre
09/10/2026 18:27:02

Número de páginas
34

Identificador único del documento HASH

```
154eff0bffa3cba1e30de8a791f7a5cd02c60171d6c9c69cbf725695e446d63f
```

2 VALIDACIÓN DEL DOCUMENTO

Verificación mediante código QR.

La presente constancia acredita la integridad, autenticidad y fecha de firma del documento mediante evidencia criptográfica verificable.

SFD
09/10/2026 18:49

Validar documento

Escanee el código QR para validar la información de este documento.

Total de firmantes: **5**

3 FIRMANTES

Personas que realizaron la firma electrónica del documento.

01

Nombre
Dra. Ángela Quiroga Quiroga

Fecha y hora de firma
09/10/2026 18:27:02

Cargo
Directora General de Estudios de Legislación Universitaria y Suplente del Presidente del Comité de Transparencia

Orden de firma
1

Hash Firma

```
8c41f5112a87b16c249da6c8f9445bccb142f0755fbfcd41b9861a9d3bded78c62153f0f27adca8e1ad8e4a4f01b6455
```

02

Nombre
Mtro. Jairo Orlando Perilla Camelo

Fecha y hora de firma
09/10/2026 18:12:31

Cargo
Director General para la Prevención y Mejora de la Gestión Institucional y suplente del Contralor

Orden de firma
2

Hash Firma

```
d27afa12dddc2b2011f658e81ddb574540d4fdd012704f8034520691de94eacdbd5c17280fb614e670cfa0c412d8f942
```

03

Nombre
Lic. Lorena Orozco Novelo

Fecha y hora de firma
09/10/2026 18:06:49

Cargo
Defensora Adjunta de Derechos Universitarios y suplente de la Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género

Orden de firma
3

Hash Firma

```
d6ee1e56fec92594d32527aa76ff1feab99d0ca439570751322e5afc8fe8cdac6b6e5dc0932ef54c6182d466946d219c
```

04

Nombre
Mtro. Porfirio Antonio Díaz Rodríguez

Fecha y hora de firma
09/10/2026 17:32:26

Cargo
Titular de la Dirección General de Servicios Generales y Movilidad

Orden de firma
4

Hash Firma
e6140e783faa83001a740c68d480c396f6bb01c1a622218086d451d40b85360e1b1eead5072b957c4a3c4034cf1b723a

05

Nombre
Lic. Julio César Muñoz Bustos

Fecha y hora de firma
09/10/2026 17:28:47

Cargo
Titular de la Unidad de Transparencia

Orden de firma
5

Hash Firma
14961780c008f6dfe2f7912241008a331538a84ecea19f0226e65319b400444cb6e19426752d6a0a47cbd0f45fb2d278