



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública, que someten la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, la **Auditoría Interna**, la **Dirección de la Revista de la Universidad de México**, la **Escuela Nacional de Estudios Superiores, Unidad Morelia**, la **Dirección General para la Prevención y Mejora de la Gestión Institucional** y la **Contraloría de la UNAM**, en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

### ANTECEDENTES

- I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.
- II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.
- IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los “Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”.
- V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado “V. Reglas de Generales de Evaluación” del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

Por otra parte, en el apartado “VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia”, Capítulo II. Criterios y formatos, **Vertiente 2: Deberes, Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.

- VI.** En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.
- VII.** Mediante oficio **DGRIQRP/204/2022**, recibido fecha 9 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, informó lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>1</sup>; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

*Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

*En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de*

<sup>1</sup> DOF: 26 de noviembre de 2021



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*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, **relacionados tanto con documentación física como electrónica**, cuya autorización de reserva total se solicita a ese Comité:*

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
a) 3.- Análisis de riesgos	<i>El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura física y tecnológica de esta área universitaria, cuyo conocimiento otorgaría herramientas a las personas para indebidamente tener acceso a los datos personales o implementar un ataque informático a los activos electrónicos.</i>	<b>89 a 124</b>
b) 4.- Análisis de brecha	<i>El análisis de brecha integra información relativa a la seguridad de la infraestructura física y tecnológica; enlistan 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 datos personales.</i>	<b>125 a 140</b>
c) 5. Plan de Trabajo	<i>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 que se implementen nuevos controles.</i>	<b>141 a 147</b>



**COMITÉ DE TRANSPARENCIA DE LA  
UNIVERSIDAD NACIONAL AUTÓNOMA DE  
MÉXICO**

**RESOLUCIÓN: CTUNAM/526/2022**

<b>d)</b> IX. Procedimiento de respaldo y recuperación de datos	Contiene información del momento de los respaldos de la información, así como la ubicación física de estos, que podrían ocasionar la pérdida, destrucción no autorizada, robo, copia no autorizada, uso, acceso o tratamiento no autorizado, el daño, la alteración o modificación no autorizada de datos personales.	<b>186 y 187</b>
---	---	------------------

Los fundamentos y motivos se exponen a continuación, de conformidad con lo establecido por el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, mismo que dispone literalmente:

...

En relación con el **primer supuesto**, se precisa lo siguiente:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgos, el análisis de brecha, procedimiento de respaldo y recuperación de datos 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 otorgaría directamente si se difundiera la información.*

Por cuanto hace al **segundo supuesto**, lo siguiente:

- *Divulgar el análisis de riesgo, el análisis de brecha, procedimiento de respaldo, recuperación de datos, las políticas de respaldo 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.*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*En ese contexto, dicho supuesto se actualiza, pues de publicarse la información propuesta a reserva, se vulneraría la seguridad e integridad de las personas cuyos datos personales están bajo el resguardo de esta área universitaria.*

*Y, finalmente por cuanto hace al **tercer supuesto**:*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha, en las procedimiento de respaldo y recuperación de datos y en 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, ante el riesgo de pérdida y destrucción de la información, en agravio de sus titulares.*

*Así se considera que la limitación de proporcionar la información se ajusta al Principio de Proporcionalidad y representa el medio restrictivo disponible para evitar el perjuicio, ya que de dar a conocer la información cuya reserva se solicita, colocaría en desventaja y vulnerabilidad a las personas cuyos datos personales están bajo el resguardo de esta área universitaria.*

*La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé 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 las autoridades 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 de esta área universitaria y el procedimiento de respaldo y recuperación de datos, no podrían prevenirse 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 vulnerar 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.*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha, al plan de trabajo y procedimiento de respaldo y recuperación de datos de esta área se adecua al principio de proporcionalidad porque 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; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino 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 documentos, que obran como anexos y procedimiento del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*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 ...” (sic).*

VIII. Mediante oficio **AINT/0837/2022**, recibido fecha 16 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Auditoría Interna** informó lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>2</sup>; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

*Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

*En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, las Reglas Generales de Evaluación Décima Tercera y*

<sup>2</sup> DOF: 26 de noviembre de 2021



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*Décima Cuarta del apartado V y las Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran 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:*

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
<b>a) Análisis de riesgos</b>	<i>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.</i>	<b>13-15</b>
<b>b) Análisis de brecha</b>	<i>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 herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.</i>	<b>16-17</b>
<b>c) Plan de Trabajo</b>	<i>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 que se implementen nuevos controles.</i>	<b>18 y 19</b>

*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 los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*documentos consistentes en análisis de riesgo, el análisis de brecha, así como, los planes de respaldo y 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, así como, los planes de respaldo y 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 otorgados.*
- *En este sentido la revelación de la información que obra, el análisis de riesgo, el análisis de brecha, así como, los planes de respaldo y 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 y harían vulnerable a esta Área Universitaria respecto a la prevención de delitos.*

*La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé 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 las autoridades para evitar la comisión de delitos.*

*En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha así como, los planes de respaldo y de trabajo de esta área universitaria, no podrían prevenirse 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 vulnerar las*





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*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, así como, los planes de respaldo y de trabajo de esta área se adecua al principio de proporcionalidad porque 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; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.*

*Por tales motivos, respetuosamente, se propone la reserva de las partes o secciones indicadas en el documento de seguridad y anexos de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*Por lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda ...” (sic).*

- IX.** Mediante oficio **DRUM/146/2022**, recibido con fecha 17 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección de la Revista de la Universidad de México** informó lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>3</sup>; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

*Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

---

<sup>3</sup> DOF: 26 de noviembre de 2021



**COMITÉ DE TRANSPARENCIA DE LA  
UNIVERSIDAD NACIONAL AUTÓNOMA DE  
MÉXICO**

**RESOLUCIÓN: CTUNAM/526/2022**

*En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran 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:*

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
<b>a) Análisis de riesgos</b>	<i>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.</i>	<i>22, 23, 34, 45, 57, 69, 80, 92, 105, 118, 130, 143</i>
<b>b) Análisis de brecha</b>	<i>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 herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.</i>	<i>24, 35, 46, 58, 70, 81, 93, 106, 107, 119, 131, 144</i>
<b>c) Plan de Trabajo y Medidas de Seguridad.</b>	<i>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 que se implementen nuevos controles.</i>	<i>25, 26, 28-32, 36-43, 47-54, 59-66, 71-78, 82-89, 94, 95, 97-101, 108-115, 120-127, 132-139, 145-152,</i>



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

		163-181 y 205
--	--	------------------

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 los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo 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, las políticas de respaldo 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, las políticas de respaldo 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, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé 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 las autoridades para evitar la comisión de delitos.*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse 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 vulnerar 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 porque 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; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino 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 documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*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 ...” (sic).*

- X. Mediante oficio **ENESM/ST/TRANS/023/2022**, recibido fecha 17 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Escuela Nacional de Estudios Superiores, Unidad Morelia** informó lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>4</sup>; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

---

<sup>4</sup> DOF: 26 de noviembre de 2021



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran 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:

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
<b>a) Análisis de riesgos</b>	<i>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.</i>	12-13, 40-41, 67-68, 94-95, 123-125, 155-156, 182-183, 216-217, 247-248, 274-275, 300-301, 326-328
<b>b) Análisis de brecha</b>	<i>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 herramientas que se deben</i>	13-15, 41-42, 68, 95- 97, 125-126,



**COMITÉ DE TRANSPARENCIA DE LA  
UNIVERSIDAD NACIONAL AUTÓNOMA DE  
MÉXICO**

**RESOLUCIÓN: CTUNAM/526/2022**

	<i>adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.</i>	156-158, 183-185, 217-219, 248-250, 276-277, 302-303, 328-329.
<b>c) Plan de Trabajo</b>	<i>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 que se implementen nuevos controles.</i>	15-17, 43-45, 69, 97- 99, 126-128, 158-160, 185-187, 219-221, 250-252, 277-279, 303-305, 330-331.
<b>d) Características del lugar donde se resguardan los soportes</b>	<i>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.</i>	11, 39, 66, 93, 123, 154, 181, 215- 216, 246, 274, 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 los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo, las características del lugar donde se resguardan los soportes 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, las políticas de respaldo, las características del lugar donde se resguardan los soportes y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*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 planemos 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, las políticas de respaldo, las características del lugar donde se resguardan los soportes 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, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé 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 las autoridades 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, no podrían prevenirse 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 vulnerar 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 porque 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; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*solo la comunidad universitaria sino 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 documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*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 ...” (sic).*

- XI.** Mediante oficio **DGPMGI/035/2022**, recibido con fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General para la Prevención y Mejora de la Gestión Institucional** informó lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>5</sup>; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

*Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

*En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

<sup>5</sup> DOF: 26 de noviembre de 2021.





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran 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:

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
<b>a) Análisis de riesgos</b>	<i>El análisis de riesgos contiene información sobre las vulnerabilidades de los sistemas físicos y de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar acciones que redunden en la comisión de actos ilícitos a los sistemas físicos y ataques informáticos a los activos críticos y no críticos.</i>	<b>12 a 15</b>
<b>b) Análisis de brecha</b>	<i>El análisis de brecha integra información relativa a la seguridad de los sistemas físicos y de la infraestructura tecnológica; enlistan 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.</i>	<b>16 y 17</b>
<b>c) Plan de Trabajo</b>	<i>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.</i>	<b>18 a 20</b>

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 los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los apartados del documento de seguridad consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*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 apartados del documento de seguridad les otorgaría directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha, las políticas de respaldo 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 físicos y 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, las políticas de respaldo y el plan de trabajo de esta área pondría de manifiesto y haría 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, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé 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 las autoridades 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, no podrían prevenirse 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 vulnerar 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.*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*En tal sentido, proteger la información de los apartados del documento de seguridad, relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque 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; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino 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 dichos apartados del documento de seguridad ... por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*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 ..." (sic).*

- XII.** Mediante oficio **CONT/066/2022**, recibido con fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Contraloría de la UNAM** informó lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>6</sup>; exigen elaborar una versión pública del documento de seguridad de esta área universitaria.*

*Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

*En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento*

<sup>6</sup> DOF: 26 de noviembre de 2021



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran 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:*

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
<b>a) Análisis de riesgos</b>	<i>El análisis de riesgos contiene información sobre las vulnerabilidades de los sistemas físicos y de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar acciones que redunden en la comisión de actos ilícitos a los sistemas físicos y ataques informáticos a los activos críticos y no críticos.</i>	<b>6 y 7</b>
<b>b) Análisis de brecha</b>	<i>El análisis de brecha integra información relativa a la seguridad de los sistemas físicos y de la infraestructura tecnológica; enlistan 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.</i>	<b>7,8 y 9</b>
<b>c) Plan de Trabajo</b>	<i>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 que se implementen nuevos controles.</i>	<b>9,10,11 y 12</b>

*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 los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

*Transparencia y Acceso a la Información Pública, respectivamente, pues los apartados del documento de seguridad consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo 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 apartados del documento de seguridad les otorgaría directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha, las políticas de respaldo 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 físicos y 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, las políticas de respaldo y el plan de trabajo de esta área pondría de manifiesto y haría 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, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé 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 las autoridades 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, no podrían prevenirse 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*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

*decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar 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 apartados del documento de seguridad, relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque 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; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino 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 dichos apartados del documento de seguridad ... por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*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 ...” (sic).*

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

### CONSIDERACIONES

**PRIMERA.** Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, por la **Auditoría Interna**, por la **Dirección General para la Prevención y Mejora de la Gestión Institucional** y por la **Contraloría de la UNAM**, en este acto, la Directora General para la Prevención y Mejora de la Gestión Institucional y suplente del Contralor en este Cuerpo Colegiado, Lic. María Elena García Meléndez, formalmente se excusa de conocer del caso, para no afectar la imparcialidad del mismo.

**SEGUNDA.** De conformidad con lo dispuesto en los artículos 1, 10 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



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, la **Auditoría Interna**, la **Dirección de la Revista de la Universidad de México**, la **Escuela Nacional de Estudios Superiores, Unidad Morelia**, la **Dirección General para la Prevención y Mejora de la Gestión Institucional** y la **Contraloría de la UNAM**, y determinar, en consecuencia, si la confirma, modifica o revoca.

**TERCERA.** De conformidad con lo dispuesto en los artículos 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 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, esa clasificación.

En tal virtud, la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, la **Auditoría Interna**, la **Dirección de la Revista de la Universidad de México**, la **Escuela Nacional de Estudios Superiores, Unidad Morelia**, la **Dirección General para la Prevención y Mejora de la Gestión Institucional** y la **Contraloría de la UNAM**, clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha**, al **Plan de Trabajo**, al **Procedimiento de Respaldo y Recuperación de Datos** y/o a las **Políticas o Planes de Respaldo**, a las **Medidas de Seguridad** y a las **Características del lugar donde se Resguardan los Soportes**, conforme a lo expuesto, en cada caso, en los antecedentes VII, VIII, IX, X, XI y XII, respectivamente, de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública.

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

*“... Como información reservada podrá clasificarse aquella cuya publicación:*

*[...]*

**VII. Obstruya la prevención o persecución de los delitos;**

*[...]”.*

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

***“Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, 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 las autoridades para evitar la comisión de delitos.***

...”

**Énfasis añadido.**

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada 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.

Al respecto, 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.

Asimismo, 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





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

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 30, 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.

De igual forma, de conformidad con el artículo 33, 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 en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, 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 protegerlos 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 35 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.

Ahora bien, de conformidad con los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los numerales 55 al 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y 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 ese sentido, 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 administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria, 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.

En este sentido, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, al **Procedimiento de Respaldo y Recuperación de Datos** y/o a las **Políticas o Planes de Respaldo**, a las **Medidas de Seguridad**, a las **Características del lugar donde se Resguardan los Soportes**, así como a **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 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**, al **Procedimiento de Respaldo y Recuperación de Datos** y/o a las **Políticas o Planes de Respaldo**, las **Medidas de Seguridad** y en las **Características del lugar donde se Resguardan los Soportes**, 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**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

como el acceso ilícito a equipos y sistema 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 a los sistemas electrónicos, así como a los archivos físicos con los que se cuenta.

Por lo que de darse a conocer la información relativa al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, al **Procedimiento de Respaldo y Recuperación de Datos** y/o a las **Políticas o Planes de Respaldo**, a las **Medidas de Seguridad**, a las **Características del lugar donde se Resguardan los Soportes**, así como a **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**, la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal del responsable, 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 los datos en su poder, en tanto la publicación de esa información revelaría 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.

Por lo anterior, se concluye que la información solicitada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

*“Artículo 104. 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.**



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

De difundirse el plan de trabajo, el análisis de riesgos, el análisis de brecha, el procedimiento de respaldo y recuperación de datos, las medidas de seguridad y las características del lugar donde se resguardan los soportes del documento de seguridad, se afectarían las medidas y acciones implementadas por las Áreas Universitarias para reducir el riesgo de que se cometa una conducta o un comportamiento que pueda dañar o convertir a esta Universidad y su comunidad en sujetos o víctimas de conductas ilícitas.

Lo anterior, toda vez que la publicidad de la información contenida en el **Análisis de Riesgo**, el **Análisis de Brecha**, el **Plan de Trabajo**, el **Procedimiento de Respaldo y Recuperación de Datos** y/o en las **Políticas o Planes de Respaldo**, las **Medidas de Seguridad** y en las **Características del lugar donde se Resguardan los Soportes**, 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 para las Áreas Universitarias, pues a través de dicha información 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, disminuyendo la capacidad de las Áreas Universitarias para responder ante 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.**

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **Análisis de Riesgo**, el **Análisis de Brecha**, el **Plan de Trabajo**, el **Procedimiento de Respaldo y Recuperación de Datos** y/o en las **Políticas o Planes de Respaldo**, las **Medidas de Seguridad** y en las **Características del lugar donde se Resguardan los Soportes**, 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**, se limitaría la capacidad de las Áreas Universitarias para prevenir la comisión de conductas ilícitas.

De ahí resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, 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.**



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/526/2022

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, 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 las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, se considera que 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**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la versión pública propuesta por la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, por la **Auditoría Interna**, por la **Dirección de la Revista de la Universidad de México**, por la **Escuela Nacional de Estudios Superiores, Unidad Morelia**, por la **Dirección General para la Prevención y Mejora de la Gestión Institucional** y por la **Contraloría de la UNAM**, por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

**CUARTA.** Este Comité considera pertinente orientar a las Áreas Universitarias, a efecto de que en la elaboración de la versión pública de sus respectivos documentos de seguridad, tengan en cuenta lo siguiente:

- Deberán testar las secciones o información correspondientes al **Análisis de Riesgo**, al **Análisis de Brecha**, al **Plan de Trabajo**, al **Procedimiento de Respaldo y Recuperación de Datos** y/o a las **Políticas o Planes de Respaldo**, a las **Medidas de Seguridad**, a las **Características del lugar donde se Resguardan los Soportes**, 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 su poder**; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.
- Deberán insertar un cuadro de texto en el cual se indiquen:



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/526/2022

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

Lo anterior, de conformidad con lo dispuesto en los numerales Quincuagésimo Noveno, Sexagésimo y Sexagésimo Primero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

### RESUELVE

**PRIMERO.** Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN de RESERVA** total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, por la **Auditoría Interna**, por la **Dirección de la Revista de la Universidad de México**, por la **Escuela Nacional de Estudios Superiores, Unidad Morelia**, por la **Dirección General para la Prevención y Mejora de la Gestión Institucional** y por la **Contraloría de la UNAM**, en relación con el **Análisis de Riesgos**, el **Análisis de Brecha**, el **Plan de Trabajo**, el **Procedimiento de Respaldo y Recuperación de Datos** y/o las **Políticas o Planes de Respaldo**, las **Medidas de Seguridad**, las **Características del lugar donde se Resguardan los Soportes**, 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**, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

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

**SEGUNDO.** Se instruye a las **Áreas Universitarias** a efecto de que elaboren la versión pública en términos de lo dispuesto en la consideración **CUARTA**.



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

**RESOLUCIÓN: CTUNAM/526/2022**

**TERCERO.** Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública; así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional a la **Dirección General de Responsabilidades, Inconformidades, Quejas y Registro Patrimonial**, a la **Auditoría Interna**, a la **Dirección de la Revista de la Universidad de México**, a la **Escuela Nacional de Estudios Superiores, Unidad Morelia**, a la **Dirección General para la Prevención y Mejora de la Gestión Institucional**, a la **Contraloría de la UNAM**, así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

Así lo resolvió 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, 20 y 53, fracción VI 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., 19 de agosto de 2022**



<b>Archivo</b>	09-ctunam-526-2022-docto-seg-2.pdf		
<b>Identificador único (hash)</b>	a00ee4c0a67a61c2ed9cc53aa6bbe78bd479032754f3d00cd0268e48f375c822		
<b>Fecha y hora de cierre</b>	19/08/2022 17:14:38	<b>Fecha y hora de emisión</b>	19/08/2022 17:15:48
<b>Número de páginas</b>	32	<b>Firmantes</b>	5



#### Firmantes

<b>Nombre</b>	Dr. Alfredo Sánchez Castañeda	<b>Fecha y hora de firma</b>	19/08/2022 17:14:38
Presidente del Comité de Transparencia			
<b>Hash Firma</b>	703be2ece91ffd054cef3b1984cbbafc0b5a6f1e19495deaf0cc39a0584c8cd8dd6ee5c2ab0cc7cb12f21da9425d0216		

<b>Nombre</b>	Dra. Guadalupe Barrera Nájera	<b>Fecha y hora de firma</b>	19/08/2022 16:00:35
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
<b>Hash Firma</b>	a4f86920e2691db68ae4e1579e0c2bf7a2b5ecaacf01afd87d1c84f21011f6fe792538b33b60b3a040a211c0b6f5c8d0		

<b>Nombre</b>	Ing. Ricardo Ramírez Ortiz	<b>Fecha y hora de firma</b>	19/08/2022 15:41:03
Director General de Servicios Generales y Movilidad			
<b>Hash Firma</b>	c41d0b86838de36bb258bc9e110f03a5037c5a514d3201273cba98bf761e922daabffeb0ee1b4947e8f9dfb87f35928b		

<b>Nombre</b>	JOSE MELJEM MOCTEZUMA	<b>Fecha y hora de firma</b>	19/08/2022 16:28:33
Titular de la Unidad de Transparencia			
<b>Hash Firma</b>	a37da27c6dee77a1342d07ad8cba7ebf2266e842a4bce737555205f518cdbc09c8637407658ccdc174d87f0b3c6aa397		

<b>Nombre</b>	Dra. Jacqueline Peschard Mariscal	<b>Fecha y hora de firma</b>	19/08/2022 16:19:05
Especialista			
<b>Hash Firma</b>	330a8226143d821f616117ce1d84ce19f1efaa35a0fbf6f8601c42c329207ad53becc8ad31584d38f47f22897d3433be		